Collaborative Network for Industry, Manufacturing, Business and Logistics in Europe

D6.1

Security and Privacy Requirements

Project Acronym	NIMBLE	
Project Title	Collaboration Network for Industry, Manufacturing, Business and Logistics in Europe	
Project Number	723810	
Work Package	WP6	
Lead Beneficiary	SRFG	
Editor	Violeta Damjanovic-Behrendt	SRFG
Reviewers	Stefan Wellsandt	UB
	Wernher Behrendt	SRFG
Contributors		
Dissemination Level	PU	
Contractual Delivery Date	31/10/2017	
Actual Delivery Date	31/10/2017	
Version	V1.0	

Abstract

The NIMBLE project performs research leading to the design and the development of a cloud and IoT-based multisided platform, targeting supply chain relationships and logistics in the EU. Core platform functionality will enable firms to register, publish machine-readable catalogues of their products and services, search for suitable supply chain partners, negotiate contracts and supply logistics, and develop private and secure information exchange channels between firms.

The aim of the project is to support a federation of NIMBLE platform instances, all providing a set of core services, and each specifically being tailored to a different aspect (regional, sectorial, topical, etc.). The overall role of the NIMBLE multisided platform in digital automation is to increase speed to market, cost minimization, optimization of manufacturing and logistic processes. Such goals open several side effects related to cybersecurity, which could cause serious harm to the participating companies, e.g. losing customers, facing a host of legal and financial penalties, putting businesses at risk. Hence, our focus in Work Package WP6 of the NIMBLE project is to ***(i) meet baseline security and privacy standards, (ii) enforce policies and procedures to prevent infiltration, (iii) provide means to detect inappropriate access to connected products, and (iv) minimize any potential damage caused by unauthorized access.***

This document captures security and privacy requirements for the design and development of the NIMBLE platform. The report refers to and makes use of, several previously accomplished project tasks:

- ***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".*

This document defines and specifies ***use case-centric security and privacy requirements****,* ***platform-centric security and privacy requirements*** *and designs the* ***NIMBLE Privacy Requirements Framework*** *for addressing additional privacy related questions, including the General Data Protection Regulation (GDPR), which will apply from 25 May 2018. The mapping between GDPR requirements and the platform-centric security and privacy requirements is given in Appendix 1.*

The requirements evaluation is done through data flow analysis of the core processes running over the platform, following the STRIDE threat modelling principles. Here, we additionally presented mapping between use case-centric and platform-centric security requirements, which was performed in order to eliminate inconsistences between the requirements and to provide their final prioritization and specification before the security design and development for core services is accomplished in D6.2.

Note that this document refers only to technical security controls and methods, while various security capabilities, such as non-technical security controls, policy and procedures addressing business protection at the management level of the platform, etc. will be defined in a document ***"Plan for NIMBLE Platform Governance"****. Several relevant sections of the Plan for NIMBLE Platform Governance will later be made available from the project webpage.*

Document History

Version	Date	Comments
V0.1	30/05/2017	Initial version and assignments distribution
V0.2	31/07/2017	More detailed content of the document
V0.3	14/08/2017	Detailed analysis of use case requirements in order to capture security and privacy requirements
V0.4	04/09/2017	NIMBLE Privacy Requirements Framework; Adding contributions from use case partners
V0.5	18/09/2017	Platform-centric security and privacy requirements
V0.6	25/09/2017	Security and privacy requirements mapping
V0.7	09/10/2017	STRIDE-based requirements evaluation
V0.8	23/10/2017	Version ready for internal review
V0.9	29/10/2017	Final QA comments addressed GDPR addressed and mapped to security and privacy requirements captured in NIMBLE
V1.0	31/10/2017	Consolidated final version of D6.1

Table of Contents

List of Figures

List of Tables

Glossary

ISE/IEC 27000 series of Information Security Standard	*Known as the "ISMS Family of Standards" or "ISO27k" comprises Information Security standards published jointly by the ISE and the IEC. It covers privacy, confidentiality and IT/ technical/ cybersecurity issues.*
GDPR (General Data Protection Regulation)	*The new regulation by which the European Parliament, the Council of the EU and the European Commission intend to unify data protection for all individuals within the EU. It will come into force in May 2018.*
Confidentiality	*A set of rules that limits access or places restrictions on certain types of information.*
Integrity	*A set of rules ensuring that data cannot be modified in an unauthorized or undetected manner.*
Availability	*Security methods ensuring that services and data are functional and available when they are needed.*
Authenticity	*Security methods ensuring the proof of identity, which can be based on a password, a key card, or biometric methods like fingerprint, hand geometry scans, retinal scans, etc.*
Accountability	*Security methods generating "the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action" [NIST800-27].*
Non-repudiation	*Security methods must be used to prove that the message (sent or received) is not repudiated. Authenticity and data integrity are prerequisites for non-repudiation.*
Reliability	*The ability of the system to operate under designed operating conditions for a designed period of time or number of cycles [MODA93].*
Data provenance	*Security methods ensuring that data about access to the system is kept in audit logs. Data provenance matters in cybersecurity as a measure for preventing data manipulation.*
STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege)	*STRIDE is an approach to threat modelling and requirement evaluation, developed by Microsoft.*
Spoofing	*Pretending to be something or someone other than yourself.*
Tampering	*Modifying something on disk, on a network, or in memory,*

	by the user who is not supposed to modify it.
Repudiation	*The user is claiming that s/he didn't do something or s/he is not responsible, regardless of whether s/he did it or not.*
Information Disclosure	*Exposing information to people who are not authorized to see it.*
Denial of Service	*Absorbing resources needed to provide service (by crashing services, making them unusably slow, filling all available storage, etc.)*
Elevation of Privilege	*The user (or a software) is technically able (allowed) to perform something that they are not supposed (authorized) to do.*
Fair Information Practices (FIP) framework	*A privacy framework for formulating eight principles on personal data [OECD80][WPF08].*
Privacy by Design framework	*A privacy framework designed to help organizations to embed privacy into product design.*
Seven Laws of Identity framework	*A privacy framework that is useful for the consideration of "identity" [SHOS14].*
Data Minimization strategy	*It defines several constraints for minimizing risks of privacy breaches by putting sensitive data under the user's control [GÜTD11].*
Security Development Lifecycle (SDL)	*Microsoft Security Development Lifecycle (SDL) is a software development process used to reduce software maintenance costs and increase reliability of software concerning software security related bugs.*
Retention of data	*Security methods that define the policies of persistent data and records management for meeting legal and business data provenance requirements. The primary objective of data retention is traffic analysis and massive surveillance.*
SQL Injection	*A code injection technique used to attack data-driven applications.*
Data Integrity	*Security methods for assuring accuracy and consistency of data over its entire life-cycle. It is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.*
Data Flow Diagram (DFD)	A graphical model representing the "flow" of data through an information system, modelling its *process* aspects.

1 Introduction

The work presented in this report links to the results of several tasks, accomplished in the project and summarized in the following reports:

- **D1.1** "*Requirements and Collaboration Design for Manufacturing and Logistics in Four European Use Cases*" (published in March 2017);
- **D2.1** "*Platform Architecture Specification and Component Design*", (published in April 2017), and
- **D3.1** "*Core Platform Infrastructure*", (published in April 2017).

In addition to capturing security and privacy requirements related to known use cases in the project (e.g. use cases in furniture manufacturing (Micuna), textile sector (Piacenza), wooden house manufacturing (Lindbäcks) and white goods (Whirlpool)), we also studied some major predictable threats and vulnerabilities, in order to (1) to analyse risks and fully address security and privacy countermeasures, and (2) to adopt and integrate these measures in the platform. In this report, we focus on security and privacy requirements related to the core NIMBLE services, which will be refined and elaborated in the future, following the progress of the platform's further development.

1.1 Objectives

The objective of this report is to identify and specify security and privacy requirements leading to engineering and delivering secure platform solutions for a variety of users, e.g. suppliers, logistic operators, service providers, cloud providers, retailers and the future platform providers.

- **Our approach to security** follows the formulation of security as a property to prevent *unauthorized access to and modification of information and data, as well as unauthorized use of resources* [AMIN93].
- The **privacy consideration in NIMBLE** ensures the development of platform services that satisfy user's requirements related to privacy protection and disclosure of both personal and corporate information. Privacy is a common application of security technologies, with a significant intersection with data provenance that adds security controls for preserving both data integrity and confidentiality [MALN12][SUBS11].

Therefore, by engineering more reliable security- and privacy-centric services in NIMBLE, we ensure an adequate treatment of information stored and processed at the cloud service provider's system, as well as at the platform provider side.

1.2 Methodology

Our methodology for capturing security and privacy requirements includes the following steps:

1. **Use case-centric security and privacy requirements elicitation**, based on the collection of use case requirements extracted in task T1.1 (see D1.1). This is presented in Section 3. Summaries on use case-centric functional and non-functional security requirements, and use case-centric privacy requirements are given in subsection 3.5.
2. **Platform-centric security and privacy requirements elicitation**, based on the problem context of the platform system from task T2.1, which defined the NIMBLE platform architecture and component design (see D2.1).

3. **Mapping between use case-centric and platform-centric security and privacy requirements**, to eliminate possible inconsistencies and "normalize" these two subcategories of requirements.
4. **Threats and vulnerabilities identification**, based on analysis of assets of the platform that can be affected by threats and vulnerabilities. The threats will point to what the attacker can do to harm the platform, while vulnerabilities are weaknesses of the platform that could be exploited by the attacker. Here we will use the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) approach to threat modelling.
5. **Security and privacy requirements evaluation** through STRIDE analysis of data flows on the platform.

1.2.1 Requirements Attributes

For the management of security and privacy requirements and their attributes, we specify the following details in Table 1 and Table 2, respectively:

- the unique IDs of the security requirement (e.g. SEC_UC_xxx stands for use case-centric security requirements; PR_UC_xxx for use case-centric privacy requirements),
- the unique IDs of the use case requirements (as defined in D1.1),
- priority (must - should - could),
- name of the security requirement,
- description of the security requirement,
- stakeholder/ countermeasures (e.g. user identification & authentication methods; UC-14 (from D1.1)).

Table 1 presents a template for collecting security requirements attributes. Table 2 is a template for collecting privacy requirements attributes, and Table 3 separates functional and non-functional requirements.

Table 1: Template for security requirements attributes

Sec. Req. ID	UC Req. ID (from D1.1)	Priority	Name	Description	Stakeholder/ Countermeasures
SEC_UC_001	*REQ_MIC_xx*	*MUST or SHOULD or COULD*	*User authentication process*	*Authentication methods*	*User identification and authentication*

Table 2: Template for privacy requirements attributes

Req. ID	UC Req. ID (from D1.1)	Priority	Name	Description	Countermeasures
PR_UC_001	*REQ_MIC_xx*	*MUST or SHOULD or COULD*	*Normative and legislations*	*Establishing privacy awareness*	*Privacy awareness*

To differentiate between functional and non-functional security and privacy requirements and their attributes, we specify the following details in Table 3:

- the FINAL unique IDs of the security requirement (e.g. FUN_SEC_UC_xxx for use case-centric functional security requirements; NFUN_SEC_xxx for use case-centric non-functional security requirements, PRIV_UC_xxx for use case-centric privacy requirements, and PRIV_PLAT_xxx for platform-centric privacy requirements),
- name of the security requirement,
- the unique IDs of the security requirements,
- priority (must - should - could),
- description of the security requirement,
- stakeholder/ countermeasures.

Table 3: Functional and non-functional security requirements attributes

Sec. Req. ID	Name	Sec. Req. ID	Priority	Description	Stakeholder/ Countermeasures
FUN_SEC_UC_001	*Secure access to the platform*	*SEC_UC_01*	*MUST or SHOULD or COULD*	*Authentication methods*	*User identification and authentication*

1.2.2 Document Organization

Section 2 presents our approach to security and privacy requirements acquisition in the NIMBLE project. In Section 3, we specify and summarize use case-related requirements, while the NIMBLE system security architecture and related security system/ platform-centric requirements are given in Section 4. Section 5 provides mapping between captured security requirements, which are afterwards evaluated in Section 6. Section 7 concludes this document.

Note, **SECURITY CAPABILITIES** such as non-technical security controls, addressing policy and procedures for business protection at the management of the platform, will be defined in a document ***"Plan for NIMBLE Platform Governance"***. The plan will also cover the *Data Integrity and Data Quality Policy* (as explained in Table 28). Note that Table 28 specifically incorporates the GDPR requirements in the *NIMBLE Privacy Requirements Framework*.

The *Plan for NIMBLE Platform Governance* will be a part of D8.8 "*NIMBLE Platform SEED Programme: Manual and Materials Package*", and will be available in M15. The most important sections of the *Plan for NIMBLE Platform Governance* will also be made available from the project webpage.

2 NIMBLE Approach to Security and Privacy Requirements Elicitation Process

Adopting key security concepts and integrating security controls are two necessary steps for preventing financial loss and data breaches, damaging trust and the corporate reputation built over time. In the business world, information security needs to be balanced against costs. For example, the investments in cybersecurity can be measured using a mathematical economic model called the *Gordon-Loeb Model* [GOLO02], which compares metrics for quantifying expected financial loss without and with security investments. The model is grounded on the breach probability functions which consider two factors: the security level and the system's inherent vulnerability. Similarly, the selection of security controls to be integrated in business solutions can be based on *likelihood-weighted cost-benefit analysis*, which measures the likelihood of an unwanted event and the cost/ impact of its consequence [MALN12].

Our objective in T6.1 is to find a match of the most important security controls and measures to be integrated in the NIMBLE platform, through an analysis of functional and non-functional security and privacy requirements related to various platform stakeholders: use case partners, core platform/ system technical requirements, cloud providers, platform providers, actual European industry rules and laws. Therefore, the systematic security and privacy requirements elicitation process in NIMBLE introduces the following five perspectives:

- ***Use case-centric requirements*** featuring relationships and interaction between users of the platform, and between users and the platform (Section 3);
- ***Platform-/ system-centric requirements*** supporting the entire business interaction between the users and the platform/system, e.g. data sharing, searching, negotiation, creation of catalogues and offers, business process execution, etc. (Section 4);
- ***Cloud service provider requirements*** ensuring appropriate security protection and positive security implication on businesses when using cloud services (Section 4.4);
- ***Platform provider requirements*** ensuring that minimum baselines for Information Security are provided, e.g. strong access control measures, data protection, a *Vulnerability Management Program* is maintained, an *Information Security Policy* is in place, secure software development standard practices such as OWASP and OWASP *Mobile Security Project* will be considered too, etc. (Section 4.3);
- ***Industry-specific requirements*** enabling compliance of services and products with industry rules or law, e.g. in case of implementing payment methods via the NIMBLE platform.

Capturing functional and non-functional security requirements in NIMBLE puts a strong emphasis on an early integration of security with software development, which is ensured through the key concepts of Information Security, as defined in the **ISO/IEC 27000:2009 standard** [ISE/IEC09]. In addition to ISE/IEC 27000 series, we use several privacy requirements frameworks that will be tailored into the **NIMBLE Privacy Requirements Framework**.

Figure 1 illustrates our approach to capturing security and privacy requirements. We are using the ISE/IEC 27000 series of Information Security Standard for capturing security requirements related to use cases (presented in D1.1) and to the NIMBLE platform architecture and components design (presented in D2.1 and D3.1). In this way, we identify and specify use case-centric and platform-centric security requirements in the project. For privacy, we define the NIMBLE Privacy Requirements Framework, which incorporates elements from several privacy

frameworks and strategies, e.g. the Fair Information Practices, the Seven Laws of Identity, the Data minimization strategy, and looks at the new General Data Protection Regulation (GDPR) and its requirements. For the identification and specification of privacy requirements of the NIMBLE platform, we apply the NIMBLE Privacy Requirements Framework and the Microsoft Privacy Guidelines for Software Product and Services. The result of this step are platform-centric privacy requirements in NIMBLE. We map use case-centric and platform-centric security and privacy requirements in order to eliminate possible inconsistences and repetitions. Finally, we use the STRIDE-based methods for the evaluation of security requirements, and perform mapping of platform-centric security and privacy requirements with the GDPR requirements, in order to get NIMBLE GDPR compliant.

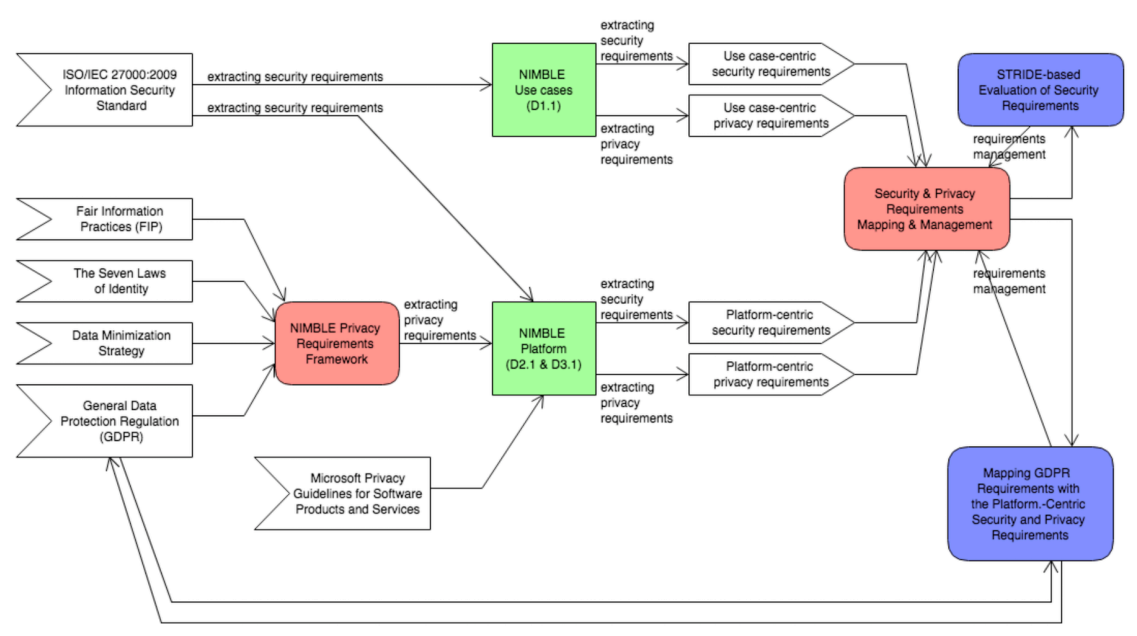

Figure 1: NIMBLE approach to capturing security and privacy requirements

2.1 ISO/IEC 27000:2009 Guidelines

The ISO/IEC 27000:2009 standard ensures that the information is neither violated nor compromised through possible critical situations, i.e. device malfunctions, threats (software attacks, ransomware, viruses and the like), identity theft, hazards, natural disasters. The standard contains the following seven elements, which are known as **defensive tactics** or the **desirable security properties** in cybersecurity:

- **Confidentiality** - "*...information is not made available or disclosed to unauthorized individuals, entities, or processes*" (excerpt from [ISO/IEC09]);
- **Integrity** - "*...data cannot be modified in an unauthorized or undetected manner*". Data accuracy and data completeness need to be adequately assured, using various security methods and mechanisms;
- **Availability** - security methods for services and data must be functional and available when they are needed;
- **Authenticity** - involves proof of identity and can be validated through authentication. The proof of identity can be based on a password, a key card, or biometric methods like fingerprint, hand geometry scans, retinal scans, etc.

- **Accountability** - generates "the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action" [NIST800-27].
- **Non-repudiation** - security methods must be used to prove that the message (sent or received) is not repudiated. Authenticity and data integrity are prerequisites for non-repudiation; and
- **Reliability** of the system - "the ability of the system to operate under designed operating conditions for a designed period of time or number of cycles" [MODA93].

A failure to control the distribution of data and data integrity often leads to **data breaches**, loss of sensitive information and data manipulation, which should be prevented by using adequate **security controls**, e.g. authenticated users can access data in a controlled manner. **Provenance information** about access to the system needs to be kept in audit logs, while security controls for anomaly detection need to be regularly performed to capture unusual behaviour. Provenance information matters in cybersecurity as a measure for preventing **data manipulation** that can cause harmful changes of product specifications (e.g. power outages, data integrity attacks in smart cars and smart cities, data sabotage, etc.). In NIMBLE, we anticipate data manipulation actions related to comparison of products and suppliers, filtering and ordering information about products and suppliers in order to force unfair trade and monopolies. The **secure exchange of business information** through file sharing, email and messaging system for negotiation, is another big concern for business parties involved in any interaction via the NIMBLE platform.

2.2 STRIDE Threat Modelling and Requirements Evaluation

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) is an approach to threat modelling, developed by Microsoft [SHOS14]. STRIDE is designed to help capturing Information Security threats, for security requirements elicitation, defining appropriate security mitigation strategies and for the security requirements evaluation. The major elements of STRIDE are the following:

1. **Spoofing.** Pretending to be something or someone other than yourself.
2. **Tampering.** Modifying something on disk, on a network, or in memory, by the user who is not supposed to modify it.
3. **Repudiation.** The user is claiming that s/he didn't do something or s/he is not responsible, regardless of whether s/he did it or not.
4. **Information Disclosure.** Exposing information to people who are not authorized to see it.
5. **Denial of Service (DoS).** Absorbing resources needed to provide service (by crashing services, making them unusably slow, filling all available storage, etc.)
6. **Elevation of Privilege (EoP).** The user (or a software) is technically able (allowed) to perform something that they are not supposed (authorized) to do.

Each of the STRIDE threats can be matched with the desired security property (i.e. properties defined in the ISO/IEC 27000:2009 standard/ see Section 2.1), which is summarized in Table 4. Here we also add adequate mitigation strategies for each of the STRIDE threats.

Table 4: Threats - Desired security properties - Mitigation strategies

STRIDE Threat	Desirable properties	Mitigation strategies (Countermeasures)
Spoofing	Authentication	Identification and Authentication; Cryptographic Authentication
Tampering	Integrity	Cryptography; Anti-pattern (for network isolation)
Repudiation	Non-Repudiation	Maintaining protected log files
Information Disclosure	Confidentiality	Encryption; Cryptography; Carefully designed control
Denial of Service	Availability	Careful design of resources and resource management; Avoid multipliers (of CPU consumption in network)
Elevation of Privilege	Authorization	Separate data and code; Careful treatment of file bugs

In NIMBLE, we use STRIDE to evaluate captured security requirements. For privacy requirements, we combine several methods and strategies, that will be discussed in Section 2.3.

2.3 Privacy Requirements Frameworks and Strategies

The following privacy requirements frameworks are important because they are either influential with regulations or have been designed to provide practical advice for developers. The selection of appropriate privacy requirements frameworks depends on what is going to be built and for whom [SHOS14]. For example, the *Fair Information Practices* framework opens a list of privacy elements which are useful to be discussed in the system design phase, while the *Seven Laws of Identity* framework improves usable security topics (user-centric privacy).

2.3.1 Fair Information Practices (FIP)

The Fair Information Practices (FIP) framework was established in 1973, by setting forward the five fundamental principles for safeguarding privacy. These principles were extended in 1980 by the OECD (Organization for Economic Cooperation and Development) **Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data,** formulating the following eight principles on personal data [OECD80][WPF08]:

1. **Collection Limitation Principle**: Personal data need to be obtained fairly and lawfully, with consent given by the data subject.
2. **Data Quality Principle**: Personal data should be relevant to the purposes for which they are to be used; should be accurate, complete and kept up-to-date.
3. **Purpose Specification Principle**. The purposes for which personal data are collected should be specified at the time of data collection.
4. **Use Limitation Principle**. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified: a) with the consent of the data subject, or b) by the authority of law.

5. **Security Safeguards Principle**. Personal data should be protected by reasonable security safeguards against risks such as data loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **Openness Principle**. There should be a general policy of openness about developments, practices and policies with respect to personal data.
7. **Individual Participation Principle**. An individual should have certain rights related to his data, e.g. a) obtaining data from a data controller; b) being informed about data relating to him within a reasonable time, in an understandable form; c) having the data erased, rectified, completed or amended, when required.
8. **Accountability Principle**. A data controller should be accountable for complying with measures which give effect to the above principles.

The EU *Directive on the Protection of Personal Data* (1995) is based on FIP. From the developer's perspective, the above eight principles are useful for evaluating security and privacy issues at design time.

2.3.2 Privacy by Design (PbD)

The Privacy by Design framework includes seven principles, designed to help organizations to embed privacy into product design [CAVO12]:

1. **Proactive** - PbD approach is characterized by proactive rather than reactive measures. It is focused on identification and prevention of privacy invasive events.
2. **By Default** - It ensures that personal data are automatically protected in any system or business practice. User's privacy is built into the system, by default.
3. **Embedded** - It is embedded into the design and architecture of systems and business practices, and is integral to them.
4. **Positive Sum** - It demonstrates that it is possible to have both privacy and security, leading towards positive sum, instead of "zero sum" payoff.
5. **Life-Cycle Protection** - It ensures adoption of strong security measures that are essential to privacy, from start to finish. This ensures that all data are securely retained, and securely destroyed at the end of the process (secure lifecycle management of information).
6. **Visibility/ Transparency (Keep It Open Principle)** - It ensures all stakeholders operate according to the stated promises and objectives, in visible and transparent ways.
7. **Respect for Users (Keep It User-Centric Principle)** - It implements measures such as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Privacy by Design has been criticized as a "vague" instrument for engineering systems: the authors in [GÜTD11] emphasize the gap between policy makers and engineers on what it means to technically address privacy threats. For example, the PbD principle no. 6 (Visibility/ Transparency) does not mitigate the privacy risk arising from mass collection of data in databases, e.g. single point of failure, risk of public disclosure, "stealthy" abuses (secondary use).

2.3.3 The Seven Laws of Identity

The Seven Laws of Identity framework is not a true privacy requirements framework, but some elements of this framework are useful for the consideration of "identity" [SHOS14]. Table 5 presents these seven laws/ principles, and in parallel, our exercise to invert these laws into threats:

Table 5. Seven Laws of Identity and their inversion into Threats

Laws of Identity	Description of law	Inversion into **threats**
User Control and Consent.	The system reveals user information only with the user's consent.	*Does the system obtain consent before revealing information? Does the system reveal information without the user's consent?*
Minimal Disclosure for a Constrained Use.	The system discloses the least amount of identifiable information and with its limited use.	*Does the system disclose identifiable information that is not required for a transaction? Does the system disclose identifiable information for unlimited use?*
Justifiable Parties.	Disclosure of identifiable information is limited to parties with a necessary and justifiable place in a given identity relationship	*Does the system disclose identifiable information to parties which are not necessary in the system?*
Directed Identity.	The system must support both omni-directional identities (for public entities) and uni-directional identities (for use by private entities).	*Does the system support use by public entities? Does the system support use by private entities?*
Pluralism of Operators and Technologies.	The system must enable the interworking of multiple identity technologies run by multiple identity providers;	*Does the system support use by various identity providers? Does the system support the interworking of multiple identity technologies?*
Human Integration.	The human user must be a component of the distributed system, offering protection against identity attacks.	*Is the human user "integrated" into the system? Is there any protection against identity attacks?*
Consistent Experience Across Contexts.	The system must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple technologies.	*What is the user experience in using the system? Do different contexts bring different complexity to users?*

2.3.4 Data Minimization Strategy

The Data Minimization strategy is designed with the aim to reduce privacy risks and provide users with maximum control over their sensitive information. It defines several constraints for minimizing risks of privacy breaches and putting sensitive data under the user's control [GÜTD11]. Specifically designed mechanisms can be applied to validate the integrity of algorithms, demonstrate compliant handling of data, prove that data collectors and processors respect privacy policies, etc.

Here is an overview of data minimization principles:

- **Minimize Collections** of data in the system;
- **Minimize Disclosure** by constraining the flow of information to parties other than the entity to whom the data relates.
- **Minimize Replication** by limiting the amount of entities where data is stored or processed.
- **Minimize Centralization** by avoiding single point of failure in the system.
- **Minimize Linkability** by limiting the inferences that can be made by linking data.
- **Minimize Retention** of data in the system.

For the development of privacy preserving mechanisms in NIMBLE, we combine the FIP privacy framework and the above data minimization principles. Major privacy objectives in NIMBLE relate to minimizing the risks of privacy breaches and limiting the need for trust between users and/ or between users and devices.

2.3.5 Microsoft Privacy Guidelines for Software Products and Services

This set of guidelines is based on Microsoft's internal best practices, which have been integrated into the Security Development Lifecycle (SDL) and widely deployed in the company [PRIV-GUID08]. It offers guidelines for creating notice and consent experiences, providing sufficient data security, maintaining data integrity, supplying controls for developing software products, etc. One of the core principles of the guidelines refers on user's consent, which is related to what personal data will be collected, with whom it will be shared, and how it will be used.

The type of notice and consent depends on the type of data being collected and how it will be used. For example, a **privacy notice** can be:

- A prominent notice: designed to capture the user's attention, offering high-level details about the collected data;
- A discoverable notice: contained in a specifically designed privacy link that is accessible from a website, or a Help menu. This notice should be certified by a certification organization such as TRUSTe.
- A layered notice: containing several specific sections and summaries giving information about complex privacy statements, e.g. "User's Choices", "Uses of Information", "How to Contact Us", etc.

Consent can be obtained from the user through GUIs or a website, in a form of an agreement that need to be accepted during the registration process, or "just-in-time notice", just before collecting data, or "installation time notice" that appear during the installation of the product. Another privacy feature to be addressed in NIMBLE is related to **privacy controls**, e.g. user controls enabling users to delete any stored sensitive information, or administrator privacy controls enabling setting group data retention policies. Special consideration needs to be given to setting privacy guidance for cookies, pre-release products, transferring data, file and path names, changing the purpose of using previously collected data, etc.
Despite recent privacy issues with Windows 10 [WARR17][BOOM17], we consider *Microsoft Privacy Guidelines for Software Products and Services* as a good baseline for the NIMBLE Privacy Requirements Framework. Microsoft outlined their **commitment to the EU's General Data Protection Regulations (GDPR)**, which is documented in [MICR17], as well as in the blog post by Brendon Lynch, Microsoft's Chief Privacy Officer [LYNC17] and in the blog post by Rich Sauer, Microsoft's Corporate Vice President & Deputy General Counsel [SAUE17]. For more details on GDPR, see the following section.

2.3.6 General Data Protection Regulations (GDPR)

The GDPR (Directive 95/46/EC) is a new European privacy regulation about protecting and enabling the privacy rights of individuals (in relation to a natural person, or data subject) [GDPR95][ICO17a]. It establishes strict privacy requirements, governing the way of protecting personal data, respecting the user's individual choice. The GDPR is a complex regulation encompassing numerous elements, to name a few below: [MICR17]

- **Enhanced personal privacy rights** enabling the data owners the right to access to their personal data, to correct inaccuracies in their data, to erase the data, to object to processing of their personal data and to move it;
- **Increased duty for protecting personal data** by organizations that process personal data;
- **Mandatory personal data breach reporting** by organizations that control personal data, which are required to report personal data breaches, no later than 72 hours once they become aware of the breach.

The GDPR makes clear that **the concept of personal data** includes any information related to an *identified or identifiable natural person*, and *online identifiers* (e.g., IP addresses, mobile device IDs) and *location data*. **Sensitive personal data** under the GDPR includes: genetic data, biometric data, personal data revealing ethnic or racial origin, political opinions, religious or philosophical views, data concerning health, data concerning a person's sex life or sexual orientation. Sensitive data require user's explicit consent for data processing.

In [MICR17], the authors suggest the following steps for an organization in order assure their compliance with the GDPR:

- **Discover personal and sensitive data**: Identify all personal data and where it resides;
- **Manage personal and sensitive data**: Govern the usage of personal and sensitive data;
- **Protect personal and sensitive data**: Establish security controls to protect these data, and to respond to data breaches and vulnerabilities;
- **Report on data breaches and keep documentation** (including provenance data and log files).

The GDPR will become enforceable in May 2018 and will have significant implications on businesses in the EU. Hence in NIMBLE, in order to comply with the GDPR, we are already designing our privacy policies, including data protection controls and breach notification mechanisms, etc. The authors in [ICO17b] suggest the following 12 steps to be taken by the organizations in order to prepare for the GDPR implementation:

1. Awareness that the law in changing to the GDPR;
2. Document all personal and sensitive personal data that the organization is hold (where the data is stored, with whom is it shared, etc.);
3. Reviewing current privacy notices for communicating privacy information, and preparing for GDPR implementation;
4. Checking the security and privacy procedures in order to cover all GDPR requirements (including deletion of personal data, or personal data modification by the data owners/subject);
5. Checking the security and privacy procedures for supporting subject's access requests;
6. Identifying lawful basis for processing personal data, and updating privacy notices to explain it;
7. Checking the security and privacy procedures for seeking, recording and managing consent;
8. Checking the security and privacy procedures for verifying the subjects' ages;

9. Checking the security and privacy procedures for detecting, reporting and investigating personal data breaches;
10. Implementing the following guidelines: the ICO's code of practice on Privacy Impact Assessment and the guidance from the Article 29 Working Party;
11. Formally designate a Data Protection Officer;
12. Determine the Lead Data Protection Supervisory Authority (based on Article 29 Working Party).

2.3.7 NIMBLE Privacy Requirements Framework

By combining the above-presented privacy frameworks and their principles of interest for NIMBLE, we design the NIMBLE Privacy Requirements Framework (see Table 7).

> Practically, the *NIMBLE Privacy Requirements Framework* combines several principles from the *Fair Information Practices* framework, the *Laws of Identity* framework, the *Data minimization principles*, and finally it looks at the *GDPR requirements*.

For example, we found that the *Accountability Principle* of the *Fair Information Practices* framework, could be compensated by the user's trust mechanisms that will be developed in NIMBLE (task T6.3). Hence, we do not address the *Accountability Principle* in our framework. From the *Laws of Identity* framework, we decided not to address: (i) the *Directed Identity* principle, which is a matter-of-course in multi-sided platforms, and (ii) the *Consistent Experience Across Contexts*, which we consider to be closer to usability than privacy requirements. The NIMBLE Privacy Requirements Framework fully adopts the Data minimization principles, which has a central role in our privacy requirements elicitation approach. Finally, we check our privacy controls with respect to the GDPR requirements, based on the 12 recommended steps to be taken by the organizations in order to prepare for the GDPR implementation [ICO17b].

Table 6 combines selected privacy requirements frameworks, i.e. FIP, Laws of Identity, Data minimization and GDPR, and convert them into specific privacy requirements of the NIMBLE Privacy Requirements Framework. Table 7 illustrates the NIMBLE Privacy Requirements Framework and its use for addressing user-centric privacy and data-centric privacy in the project.

Table 6: Adopting principles from the Fair Information Practices, the Laws of Identity, Data minimization and the GDPR to address privacy requirements in NIMBLE

Fair Information Practices	Laws of Identity	Data minimization	GDPR	Conversion into privacy requirement
Collection Limitation Principle	User Control and Consent		*GDPR requirement for implementing privacy procedures for seeking, recording and managing consent*	*Does the user give his consent for the collection and use of his sensitive data?*

Purpose Specification Principle			*GDPR requirement to document all personal and sensitive personal data that the organization is hold (where the data is stored, with whom is it shared, etc.)*	*Is the purpose of collecting sensitive data clearly defined? Are personal data and sensitive personal data adequately documented in the system?*
Data Quality Principle			*GDPR requirement for verifying the user's ages*	*Is sensitive data accurate, complete and up-to-date? Is the user's age verified?*
		Minimize collections of data in the system		*Is the amount of collected data minimal?*
Use Limitation Principle	Minimal Disclosure for a Constrained Use Justifiable Parties	Minimize disclosure		*Does the system disclose the least amount of sensitive data and with its limited use?*
		Minimize replication		*Is the amount of entities where data is stored or processed, minimal?*
		Minimize centralization		*Is the number of single point of failure in the system minimal? Is sensitive data minimally centralized in the system?*
		Minimize linkability		*Is the amount of linked sensitive data minimal?*
		Minimize retention of data in the system		*Is retention of data in the system minimal?*
Security Safeguards Principle				*Is sensitive data protected?*
Openness Principle	Pluralism of Operators and Technologies			*Does open developments, practices and policies respect sensitive data?*

				Does interworking technologies have privacy mechanisms taking into account respect for sensitive data?
Individual Participation Principle	Human integration		*GDPR requirement for deletion of personal data and/or personal data modification by the data subject;* *GDPR requirement for privacy procedures for supporting user's access requests*	*Does the user have rights to his sensitive data (e.g. obtaining data from a data controller, having the data erased, rectified, completed or amended, when required)?* *Does the user have the rights to access his data?* *Is there a way for the user to submit requests for access to his data?*
			GDPR requirement for reviewing existing privacy notices and keeping them up-to-date	*Are privacy notices updated?* *Are privacy notices clearly explained?* *Do privacy notices follow laws for processing personal data?*
			GDPR requirement for detecting, reporting and investigating a personal data breach	*Are the mechanisms for detecting personal data breaches established?* *Are the mechanisms for reporting personal data breaches defined?* *Do we have defined procedures for investigating a personal data breach?*
			GDPR requirement for implementing the ICO's code of practice on Privacy Impact Assessment	*Is the ICO's code of practice on Privacy Impact Assessment implemented?* *Are we using another method to assess privacy impact?*

	GDPR requirement to implement the guidance from the Article 29 Working Party	*Is the guidance from the Article 29 Working Party implemented?*

Table 7: NIMBLE Privacy Requirements Framework

Privacy Requirements Principles	**Conversion into privacy requirement**
User-centric approach	
User Consent w.r.t. Data Collection	*Does the user give his consent for the collection and use of his sensitive data?*
User Rights and Controls w.r.t. Data Collection	*Does the user have rights to his sensitive data (e.g. obtaining data from a data controller, having the data erased, rectified, completed or amended, when required)?* *Does the user have control over his sensitive data?* *Does the user have the rights to access his data?* *Is there a way for the user to submit request for access to his data?*
Data-centric approach	
Purpose Specification	*Is the purpose of collecting sensitive data clearly defined?*
Data Quality	*Is sensitive data accurate, complete and up-to-date?* *Is user's age verified?*
Minimize Data Collections	*Is the amount of collected data minimal?*
Minimize Disclosure	*Does the system disclose the least amount of sensitive data and with its limited use?*
Minimize Replication	*Is the amount of entities where data is stored or processed, minimal?*
Minimize Centralization	*Is the number of single point of failure in the system minimal? Is sensitive data minimally centralized in the system?*
Minimize Linkability of Data	*Is the amount of linked sensitive data minimal?*
Minimize Retention of Data	*Is retention of data in the system minimal?*
Security Safeguards	*Is sensitive data protected?*
Openness and Interworking of Providers and Technologies	*Does open developments, practices and policies respect sensitive data?* *Does interworking technologies have privacy mechanisms taking into account respect for sensitive data?*

GDPR requirements	
Reviewing existing privacy notices and keeping them up-to-date	*Are privacy notices updated?* *Are privacy notices clearly explained?* *Do privacy notices follow laws for processing personal data?*
Detecting, reporting and investigating a personal data breach	*Are the mechanisms for detecting personal data breaches established?* *Are the mechanisms for reporting personal data breaches defined?* *Do we have defined procedures for investigating a personal data breach?*
Assessing privacy impact	*Is the ICO's code of practice on Privacy Impact Assessment implemented?* *Are we using another method to assess privacy impact?*
Implementing the guidance from the Article 29 Working Party	*Is the guidance from the Article 29 Working Party implemented?*

3 Use Case-Centric Security and Privacy Requirements

An initial set of requirements of the four European use cases to be carried out on the NIMBLE platform is presented in D1.1. These requirements cover the following four business cases:

1. Micuna use case, with a focus on child care furniture manufacturing;
2. Piacenza use case, covering the textile sector;
3. Lindbäcks use case, for modularized buildings manufacturing;
4. Whirlpool use case, in the white goods sector.

The initial industrial use case-centric security requirements in NIMBLE are derived from a set of use case requirements, as elaborated in D1.1. Note that many articles on software engineering consider security and privacy requirements to be non-functional requirements per se, which is different in cybersecurity: here we differentiate between functional and non-functional security requirements. Hence, we split the requirements elicitation phase according to the requirements functionality criteria. The results are summarized as follows:

- Collections of ***use case-centric functional security*** requirements are summarized in Tables 8, 11, 14, and 17;
- Collections of ***use case- centric privacy requirements*** are summarized in Tables 9, 12, 15, and 18;
- Collections of ***use case-centric privacy requirements,*** captured based on the NIMBLE Privacy Requirements Framework (see Section 2.3.7) are given in Tables 10, 13, 16, and 19;
- Summary of the ***final functional security requirements*** is given in Table 20;
- Summary of the ***final non-functional security requirements*** is given in Table 21;
- Summary of privacy requirements is given in Table 22.

> We expect that the future evolution of the general use case requirements, which will be published in D1.3 “Consolidated Requirements” (month M21), will also lead to new security and privacy requirements.

3.1 Micuna

REQUIREMENTS DESCRIPTION. Micuna use case-centric requirements emphasize several situations in which the *Procurement Department* and the *Production Department* of Micuna perform the following actions, which are relevant to security matters (UC stands for Use Case):

- UC-1: Searching for new material suppliers and/or logistics operators,
- UC-2: Negotiate various business conditions,
- UC-3: Publish product catalogues,
- UC-4: Explore conditions for entering new markets, and
- UC-5: Manage the final stages of a product's existence (End-Of-Life (EOL) product).

NOTE: The field UC Req. ID in Table 8 corresponds/ links to the unique requirements identifications, as provided in D1.1.

Table 8 and Table 9 present security and privacy requirements for Micuna use case, which are completed based on D1.1. Table 10 adds an additional set of privacy requirements for Micuna, which are here completed based on the NIMBLE Privacy Requirements Framework. Note that

Micuna is asked to answer sections on user-centric and data-centric privacy requirements from the NIMBLE Privacy Requirements Framework, while GDPR requirements are not presented to Micuna. Note that Table 28 "Security Requirements: Data Integrity and Data Quality Management", Table 29 "Platform Service Provider Security Requirements" and Table 31 "Platform-Centric Privacy Requirements" describe security and privacy requirements with a view on GDPR. Mapping between the GDPR requirements, and security and privacy requirements captured in NIMBLE, is given in Appendix 1.

Table 8: Functional security requirements and their attributes for Micuna use case

Sec. Req. ID	UC Req. ID (D1.1)	Priority	Name	Description	Stakeholder/ Countermeasure
SEC_UC_01	*REQ_MIC_02, REQ_MIC_11, REQ_MIC_22, REQ_MIC_23*	*MUST*	*Secure access to the platform*	*Establishing secure connection between users and the platform, preventing unauthorized access to the platform.*	*Identification & authentication methods; UC-1/ UC-2/ UC-3/ UC-4/ UC-5*
SEC_UC_02	*REQ_MIC_01, REQ_MIC_07, REQ_MIC_05, REQ_MIC_20, REQ_MIC_21*	*MUST*	*Secure access to data to support search functionality*	*Establishing secure access to product data and provenance information*	*Authentication mechanisms for secure search services; Authorization & access control management; UC-1/ UC-5*
SEC_UC_03	*REQ_MIC_05*	*MUST*	*Secure data manipulation*	*Performing secure data manipulation*	*Authorization mechanisms enabling data manipulation; Access control management; UC-1/ UC-2/ UC-5*
SEC_UC_04	*REQ_MIC_06*	*SHOULD*	*Trust & reputation assessment*	*Trust and reputation of users must be automatically calculated and managed*	*Trust and reputation mechanisms (e.g. based on mutual evaluation of business actors)*
SEC_UC_05	*REQ_MIC_08, REQ_MIC_09, REQ_MIC_11*	*MUST*	*Secure access to data to support negotiation*	*Establishing secure access to product data (financial data, delivery data) and provenance information*	*Authentication mechanisms for performing negotiation; Authorization & management of users access rights; UC-2*

SEC_UC_06	*REQ_MIC_10, REQ_MIC_21, REQ_MIC_24*	*MUST*	*Secure information exchange*	*Establishing secure information exchange between platform's users and services*	*Identification & management of user's access rights; UC-2/ UC-5*
SEC_UC_07	*REQ_MIC_12, REQ_MIC_13, REQ_MIC_15*	*SHOULD*	*Secure access to Normative/ Legislation repositories*	*Establishing secure access to the normative and legislations materials in the destination country*	*Authentication controls for accessing a repository of normative and legislations materials; Authorization & access control management; UC-4*
SEC_UC_08	*REQ_MIC_16, REQ_MIC_17*	*MUST*	*Secure publishing of product catalogues*	*Establishing security controls for publishing product catalogues*	*Authorization & access control management; Product catalogues support different privacy settings, e.g. product visible to all or to the specific users; UC-3*
SEC_UC_09	*REQ_MIC_17*	*MUST*	*Secure maintaining of product catalogues*	*Establishing security controls for updating product catalogues*	*Authorization & access control management; UC-3*

Table 9: Privacy requirements for Micuna use case

Priv.Req. ID	UC Req. ID (D1.1)	Priority	Name	Description	Countermeasures
PR_UC_01	*REQ_MIC_12, REQ_MIC_13, REQ_MIC_14*	*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; UC-4*
PR_UC_02	*REQ_MIC_16, REQ_MIC_17, REQ_MIC_19*	*MUST*	*Privacy controls for product catalogues*	*Sharing corporate and product data with third parties; Insecure data transfer;*	*Privacy controls and penetration tests with a focus on privacy; UC-3*

Table 10: Privacy requirements based on NIMBLE Privacy Requirements Framework: Micuna use case

Privacy Requirements Principles	**Conversion into privacy requirement**	**Fill in your comment, or Y for "Yes, this is relevant" or N for "No, this is not relevant"**
User-centric approach		
User Consent w.r.t. data collection	*Does the user give his consent for the collection and use of his sensitive data?*	Y
User Control and Rights w.r.t. Data Collection	*Does the user have rights to his sensitive data (e.g. obtaining data from a data controller, having the data erased, rectified, completed or amended, when required)?* *Does the user have control over his sensitive data?* *Does the user have the rights to access his data?* *Is there a way for the user to submit request for access to his data?*	Y, these are all relevant privacy requirements for Micuna.
Data-centric approach		
Purpose Specification	*Is the purpose of collecting sensitive data clearly defined?* *Are personal data and sensitive personal data adequately documented in the system?*	Y, this is relevant and the purpose of collecting user sensitive data must be clearly defined and documented
Data Quality	*Is sensitive data accurate, complete and up-to-date?* *Is user's age verified?*	Y, the accuracy, completeness and updating of data rely on the data owners (users from companies). To determine whether the data meets these requirements is also a matter of the owner. However, other users may provide hints on this, e.g. Google is asking for the veracity of information about a given business.
Minimize Data Collections	*Is the amount of collected data minimal?*	Y, it should be minimal
Minimize Disclosure	*Does the system disclose the least amount of sensitive data and with its limited use?*	N (in MICUNA scenario the suggested approach is to let users decide about the level

		of data exposure.
Minimize Replication	*Is the amount of entities where data is stored or processed, minimal?*	Y, it should be minimal
Minimize Centralization	*Is the number of single point of failure in the system minimal? Is sensitive data minimally centralized in the system?*	Y, it should be minimal
Minimize Linkability of Data	*Is the amount of linked sensitive data minimal?*	Y, it should be minimal
Minimize Retention of Data	*Is retention of data in the system minimal?*	Y, it should be minimal
Security Safeguards	*Is sensitive data protected?*	Y, it should be protected
Openness and Interworking of Providers and Technologies	*Does open developments, practices and policies respect sensitive data?* *Does interworking technologies have privacy mechanisms taking into account respect for sensitive data?*	Y

3.2 Piacenza

REQUIREMENTS DESCRIPTION. Piacenza use case in the textile sector includes the following actions to be performed via the NIMBLE platform:

- UC-6: Collaborative textile design and production,
- UC-7: Real-time access to supplier's catalogues and inventories for fast design development,
- UC-8: Traceability of product manufacturing processes, including orders and deliveries,
- UC-9: Automatic creation of the *Textile Certificate of Origin* document, containing information regarding the environmental and ethical evidence of materials used in production, product's destination and country of export, etc.

Note: The field *UC Req. ID* in Table 11 corresponds to the unique requirement identifier, as defined in D1.1.

Table 11 and Table 12 present security and privacy requirements for Piacenza use case, which are completed based on D1.1. Table 13 adds an additional set of privacy requirements for Piacenza, which are here completed based on the NIMBLE Privacy Requirements Framework. Note that Piacenza is asked to answer sections on user-centric and data-centric privacy requirements from the NIMBLE Privacy Requirements Framework, while GDPR requirements are not presented to Piacenza.

Table 11: Functional security requirements and their attributes related to Piacenza use case

Sec. Req. ID	UC Req. ID (D1.1)	Priority	Name	Description	Stakeholder/ Countermeasure
SEC_UC_10	*REQ_PIA_01, REQ_PIA_09, REQ_PIA_12, REQ_PIA_17*	*MUST*	*Secure access to the platform and supplier's catalogues*	*Establishing secure connection between users and the platform, preventing unauthorized access to the platform.*	*User identification & authentication methods, e.g. the use of OTP (One-Time Password) that is valid for only one login session or transaction; UC-6/ UC-07/ UC-08*
SEC_UC_11	*REQ_PIA_05, REQ_PIA_08, REQ_PIA_18, REQ_PIA_19, REQ_PIA_20*	*MUST*	*Secure access to data to support search, data analysis & visualization*	*Establishing secure access to product data for search & analytics. Secure access to provenance information.*	*Authentication mechanisms for secure search services; Authorization & access control management; UC-6/ UC-07/ UC-08*
SEC_UC_12	*REQ_PIA_01, REQ_PIA_07 REQ_PIA_11, REQ_PIA_16*	*MUST*	*Secure information exchange*	*Establishing secure information exchange for collaborative design & production*	*Identification & access control management; UC-6/ UC-07/ UC-08/ UC_09*
SEC_UC_13	*REQ_PIA_02, REQ_PIA_11, REQ_PIA_17, REQ_PIA_20, REQ_PIA_25*	*MUST*	*Secure data manipulation*	*Performing secure data manipulation, e.g. textile design modifications.*	*Authorization mechanisms enabling data manipulation; Access control management; UC-6/ UC-07/ UC-09*
SEC_UC_14	*REQ_PIA_15, REQ_PIA_17*	*MUST*	*Secure comm. via the platform*	*Exchanging messages between the users*	*User identification & authentication; UC-7/ UC-08*
SEC_UC_15	*REQ_PIA_30*	*SHOULD*	*Trust & reputation*	*Trust and reputation must be calculated*	*Trust and reputation mechanisms; UC-08*
SEC_UC_16	*REQ_PIA_13, REQ_PIA_14*	*MUST*	*Secure publishing of product catalogues*	*Establishing services and privacy controls for publishing product catalogues*	*Only for authorized users (known customers or potential customers with OTPs); Authorization & access control management; UC-7*
SEC	*REQ_PIA_13,*	*MUST*	*Secure*	*Establishing*	*Only for authorized users;*

_UC_17	*REQ_PIA_14*		*maintaining of product catalogues*	*services and privacy controls for maintaining product catalogues*	*Authorization & access control management; UC-7*

Table 12; Privacy requirements for Piacenza use case

Priv.Req. ID	UC Req. ID (D1.1)	Priority	Name	Description	Countermeasures
PR_UC_03	*REQ_PIA_21, REQ_PIA_22, REQ_PIA_23, REQ_PIA_24*	*SHOULD*	Automatic Creation of the *Textile Certificate of Origin*	*The Textile Certificate of Origin can contain confidential information that may be "available to Customs upon request"; It must be signed by the legal entities; It includes legal information of the fabric producer, the yarn producer, the thread producer, the exporter ...*	*Privacy certification application for dealing with specific privacy and security requirements related to certification process. Managing certification process (pre-certification and post-certification). UC-08*
PR_UC_04	*REQ_PIA_03, REQ_PIA_06, REQ_PIA_09*	*MUST*	*Privacy controls for production data*	*Access controls for sharing production data; Insecure data transfer;*	*Privacy controls and tests with a focus on privacy; UC-6/ UC-7/ UC-9*

Table 13: Privacy requirements based on NIMBLE Privacy Requirements Framework: Piacenza use case

Privacy Requirements Principles	Conversion into privacy requirement	Fill in your comment, or Y for "Yes, this is relevant" or N for "No, this is not relevant"
User-centric approach		
User Consent w.r.t. data collection	*Does the user give his consent for the collection and use of his sensitive data via the NIMBLE platform?*	Yes, this is important for Piacenza

User Control and Rights w.r.t. Data Collection	*Does the user have rights to his sensitive data (e.g. obtaining data from a data controller, having the data erased, rectified, completed or amended, when required)?* *Does the user have control over his sensitive data?* *Does the user have the rights to access his data?* *Is there a way for the user to submit request for access to his data?*	Yes, this is important for Piacenza
Data-centric approach		
Purpose Specification	*Is the purpose of collecting sensitive data clearly defined?* *Are personal data and sensitive personal data adequately documented in the system?*	Yes, the purpose of collecting sensitive data should be clearly defined and documented.
Data Quality	*Is sensitive data accurate, complete and up-to-date?* *Is user's age verified?*	Yes, the data must be up-to-date and accurate. User's age should be verified during the registration process.
Minimize Data Collections	*Is the amount of collected data minimal?*	Yes, although the definition of "minimal" could vary in use cases
Minimize Disclosure	*Does the system disclose the least amount of sensitive data and with its limited use?*	This is not relevant for Piacenza
Minimize Replication	*Is the amount of entities where data is stored or processed, minimal?*	Yes, this is important for Piacenza
Minimize Centralization	*Is the number of single point of failure in the system minimal? Is sensitive data minimally centralized in the system?*	Yes, this is important for Piacenza
Minimize Linkability of Data	*Is the amount of linked sensitive data minimal?*	This is not relevant for Piacenza
Minimize Retention of Data	*Is retention of data in the system minimal?*	Yes, this is important for Piacenza
Security Safeguards	*Is sensitive data protected?*	Yes, this is very important for Piacenza
Openness and Interworking of Providers and Technologies	*Does open developments, practices and policies respect sensitive data?* *Does interworking technologies have privacy mechanisms taking into account respect for sensitive data?*	Yes, this is very important for Piacenza too.

3.3 Lindbäcks

REQUIREMENTS DESCRIPTION. Lindbäcks use case includes the following actions to be performed via the NIMBLE platform:

- UC-10: Product configurator,
- UC-11: IoT based measurements,
- UC-12: Tracing building components,
- UC-13: Quality control information.

Table 14 and Table 15 present security and privacy requirements for Lindbäcks use case, which are completed based on D1.1. Table 16 adds an additional set of privacy requirements for Lindbäcks, which are completed based on the NIMBLE Privacy Requirements Framework. Note that Lindbäcks is asked to answer sections on user-centric and data-centric privacy requirements from the NIMBLE Privacy Requirements Framework, while GDPR requirements are not presented to Lindbäcks.

Table 14: Functional security requirements and their attributes related to Lindbäcks use case

Sec. Req. ID	UC Req. ID (D1.1)	Priority	Name	Description	Stakeholder/ Countermeasures
SEC_UC_18	*REQ_LIN_01*	*MUST*	*Secure access to the platform and its product configurator*	*Establishing secure connection between users and the platform. Preventing unauthorized access to the platform and product configurator.*	*User identification & authentication methods; UC-10/ UC-11/ UC-12/ UC-13*
SEC_UC_19	*REQ_LIN_06, REQ_LIN_10 REQ_LIN_16, REQ_LIN_22*	*MUST*	*Secure data manipulation*	*Performing secure data modifications related to the product configuration.*	*Authorization methods for data manipulation; Access control management; UC-10*
SEC_UC_20	*REQ_LIN_03, REQ_LIN_05, REQ_LIN_01, REQ_LIN_10, REQ_LIN_14, REQ_LIN_15, REQ_LIN_19*	*MUST*	*Secure access to data for search and analytics*	*Establishing secure access to product data and provenance information.*	*Authentication methods for secure services; Authorization & access control management; UC-10/ UC-12*
SEC_UC_21	*REQ_LIN_07, REQ_LIN_15*	*MUST*	*Secure exchange of information & notifications*	*Exchanging messages & sending notifications*	*Identification & access control management;*

Table 15: Privacy requirements for Lindbäcks use case

Priv.Req. ID	UC Req. ID (D1.1)	Priority	Name	Description	Countermeasures
PR_UC_05	*REQ_LIN_03, REQ_LIN_05, REQ_LIN_08, REQ_LIN_19, REQ_LIN_20*	*MUST*	*Privacy compliance*	*Privacy compliance:* • *Specification of entities with the rights to access the data, including locally stored sensitive data, such as email or pictures.* • *User interface components with links to up-to-date information about privacy policies.* • *Contact links for users to send questions or concerns about their privacy.*	*Privacy tests, e.g. test for deletion requests, create, maintain and test incident response plan;* *UC-13*

Table 16: Privacy requirements based on NIMBLE Privacy Requirements Framework: Lindbäcks use case

Privacy Requirements Principles	Conversion into privacy requirement	Fill in your comment, or Y for "Yes, this is relevant" or N for "No, this is not relevant"
User-centric approach		
User Consent w.r.t. data collection	*Does the user give his consent for the collection and use of his sensitive data?*	Y (e.g. bathroom)
User Control and Rights w.r.t. Data Collection	*Does the user have rights to his sensitive data (e.g. obtaining data from a data controller, having the data erased, rectified, completed or amended, when required)?* *Does the user have control over his sensitive data?* *Does the user have the rights to access his data?*	Y (e.g. bathroom, configurator)

	Is there a way for the user to submit request for access to his data?	
Data-centric approach		
Purpose Specification	*Is the purpose of collecting sensitive data clearly defined?* *Are personal data and sensitive personal data adequately documented in the system?*	Y (platform and GDPR requirement)
Data Quality	*Is sensitive data accurate, complete and up-to-date?* *Is user's age verified?*	Y (platform and GDPR requirement)
Minimize Data Collections	*Is the amount of collected data minimal?*	Y (platform requirement)
Minimize Disclosure	*Does the system disclose the least amount of sensitive data and with its limited use?*	Y (platform requirement)
Minimize Replication	*Is the amount of entities where data is stored or processed, minimal?*	N (not relevant for the use case)
Minimize Centralization	*Is the number of single point of failure in the system minimal? Is sensitive data minimally centralized in the system?*	N (not relevant for the use case)
Minimize Linkability of Data	*Is the amount of linked sensitive data minimal?*	N (not relevant for the use case)
Minimize Retention of Data	*Is retention of data in the system minimal?*	N (not relevant for the use case)
Security Safeguards	*Is sensitive data protected?*	Y (platform requirement)
Openness and Interworking of Providers and Technologies	*Does open developments, practices and policies respect sensitive data?* *Does interworking technologies have privacy mechanisms taking into account respect for sensitive data?*	Y (platform requirement)

3.4 Whirlpool

REQUIREMENTS DESCRIPTION. Whirlpool white goods use case is focused on two tasks:

- UC-14: Regression analysis techniques used for forecasting, time series modelling and finding the causal effect relationship between the variables,
- UC-15: Product avatar.

Table 17 and Table 18 present security and privacy requirements for Whirlpool use case, which are completed based on D1.1. Table 19 adds an additional set of privacy requirements for Whirlpool, which are completed based on the NIMBLE Privacy Requirements Framework. Note that Whirlpool is asked to answer sections on user-centric and data-centric privacy

requirements from the NIMBLE Privacy Requirements Framework, while GDPR requirements are not presented to Whirlpool.

Table 17: Functional security requirements and their attributes related to Whirlpool use case

Sec. Req. ID	UC Req. ID (D1.1)	Priority	Name	Description	Stakeholder/ Countermeasures
SEC_UC_22	*REQ_WHR_06, REQ_WHR_16, REQ_WHR_18, REQ_WHR_19*	*MUST*	*Secure access to the platform*	*Establishing secure connection between users and the platform, preventing unauthorized access to the platform.*	*User identification & authentication methods; UC-14/ UC-15*
SEC_UC_23	*REQ_WHR_03, REQ_WHR_06, REQ_WHR_08, REQ_WHR_11, REQ_WHR_13*	*MUST*	*Secure access to data for search & analytics*	*Establishing secure access to product data and provenance information*	*Authentication methods for secure services; Authorization & access control management; UC-15*
SEC_UC_24	*REQ_WHR_04, REQ_WHR_05, REQ_WHR_07*	*MUST*	*Secure data manipulation, e.g. data correlation*	*Performing secure data modifications.*	*Authorization methods for data manipulation; Access control mngm.; UC-14*

Table 18: Privacy requirements for Whirlpool use case

Priv. Req. ID	UC Req. ID (D1.1)	Priority	Name	Description	Countermeasures
PR_UC_06	*REQ_WHR_22*	*MUST*	*Privacy controls for production data*	*Access controls for sharing production data with third parties; Insecure data transfer*	*Privacy controls and tests*

Table 19: Privacy requirements based on NIMBLE Privacy Requirements Framework: Whirlpool use case

Privacy Requirements Principles	Conversion into privacy requirement	Fill in your comment, or Y for "Yes, this is relevant" or N for "No, this is not relevant"
User-centric approach		
User Consent w.r.t.	*Does the user give his consent for the*	No, this is not relevant. We

data collection	*collection and use of his sensitive data?*	are not expecting users to provide any sensitive data.
User Control and Rights w.r.t. Data Collection	*Does the user have rights to his sensitive data (e.g. obtaining data from a data controller, having the data erased, rectified, completed or amended, when required)?* *Does the user have control over his sensitive data?* *Does the user have the rights to access his data?* *Is there a way for the user to submit request for access to his data?*	No, this is not relevant. We are not expecting users to provide any sensitive data.
Data-centric approach		
Purpose Specification	*Is the purpose of collecting sensitive data clearly defined?* *Are personal data and sensitive personal data adequately documented in the system?*	No sensitive data is expected to be used.
Data Quality	*Is sensitive data accurate, complete and up-to-date?* *Is user's age verified?*	No sensitive data is expected to be used.
Minimize Data Collections	*Is the amount of collected data minimal?*	This is not relevant for Whirlpool.
Minimize Disclosure	*Does the system disclose the least amount of sensitive data and with its limited use?*	This is not relevant for Whirlpool.
Minimize Replication	*Is the amount of entities where data is stored or processed, minimal?*	This is not relevant for Whirlpool.
Minimize Centralization	*Is the number of single point of failure in the system minimal? Is sensitive data minimally centralized in the system?*	No sensitive user data is expected.
Minimize Linkability of Data	*Is the amount of linked sensitive data minimal?*	This is not relevant for Whirlpool.
Minimize Retention of Data	*Is retention of data in the system minimal?*	This is not relevant for Whirlpool.
Security Safeguards	*Is sensitive data protected?*	This is not relevant for Whirlpool.
Openness and Interworking of Providers and Technologies	*Does open developments, practices and policies respect sensitive data?* *Does interworking technologies have privacy mechanisms taking into account respect for sensitive data?*	This is not relevant for Whirlpool.

3.5 Summary of Use Case-Centric Security and Privacy Requirements

3.5.1 Summary of Functional Security Requirements

Table 20: Summary of functional use case-centric security requirements (FUN_SEC_x)

Sec. Req. FINAL ID	Name	Sec. Req. ID	Priority	Description	Countermeasure
FUN_SEC_UC_01	*Secure access to the platform*	*SEC_UC_01, SEC_UC_10, SEC_UC_18, SEC_UC_22*	*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*	*SEC_UC_02, SEC_UC_11, SEC_UC_20, SEC_UC_23*	*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*	*SEC_UC_03, SEC_UC_13, SEC_UC_19, SEC_UC_24*	*MUST*	*Performing secure data manipulation, e.g. comparison of providers and products, filtering and ordering providers and products according to specific criteria, configuration if products, etc.*	*Authorization methods for data manipulation services; Access control management;*
FUN_SEC_UC_04	*Secure access to data to support negotiation*	*SEC_UC_05*	*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*	*SEC_UC_06, SEC_UC_12, SEC_UC_21*	*MUST*	*Establishing secure information exchange (file sharing, platform*	*Identification & access control management;*

				email exchange sys., notifications)	
FUN_SEC_UC_06	*Secure user communication via the platform*	*SEC_UC_14*	*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*	*SEC_UC_08, SEC_UC_09, SEC_UC_16, SEC_UC_17*	*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*	*SEC_UC_07*	*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;*

3.5.2 Summary of Non-Functional Security Requirements

Table 21: Summary of non-functional use case-centric security requirements (NFUN_SEC_x) and their attributes related to four use case

Sec. Req. ID	Name	UC Req. ID	Priority	Description	Countermeasures
NFUN_SEC_01	*Confidentiality*	*REQ_PIA_28, REQ_WHR_22*	*MUST*	*Information is not made available or disclosed to unauthorized individuals, entities, services.*	*Authorization and access control management*
NFUN_SEC_02	*Integrity*	*REQ_PIA_29, REQ_WHR_08*	*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*	*REQ_WHR_08*	*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*	*REQ_LIN_11, REQ_LIN_12, REQ_LIN_15, REQ_WHR_22, REQ_WHR_18, REQ_WHR_19*	*MUST*	*The proof of identity can be based on a password, a key card, or biometric method, e.g. fingerprint, hand geometry scans, retinal scans, etc.*	*User identification & authentication followed by the verification*
NFUN_SEC_05	*Reliability*	*REQ_MIC_27, REQ_MIC_28, REQ_PIA_29, REQ_WHR_09*	*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*	*REQ_MIC_06, REQ_MIC_30, REQ_PIA_30, REQ_WHR_22*	*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*	*REQ_MIC_25, REQ_PIA_27*	*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*	*REQ_MIC_31, REQ_PIA_31, REQ_WHR_23*	*SHOULD*	*The platform must be usable when security and privacy related methods are executed*	*Measuring efficiency of the platform, speed, learnability, memorability, user preference.*

3.5.3 Summary of Privacy Requirements

The following Table 22 summarizes privacy requirements in NIMBLE

Table 22: Summary of use-case centric privacy requirements in NIMBLE

Priv. Req. FINAL ID	Priv. Req. ID	Priority	Name	Description	Countermeasures
PRIV_UC_001	*PR_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	*PR_002,*	*MUST*	*Privacy*	*Sharing*	*Privacy controls and*

	PR_004, PR_006		*controls for product catalogues and production data*	*corporate and product data with third parties; Access controls for sharing production data; Insecure data transfer;*	*penetration tests with a focus on privacy;*
PRIV_UC_003	*PR_003*	*SHOULD*	Privacy methods related to the creation of the *Textile Certificate of Origin*	*The Textile Certificate of Origin can contain confidential information that may be "available to Customs upon request"; It must be signed by the legal entities; It includes legal information of the fabric producer, the yarn producer, the thread producer, the exporter ..*	*Privacy certification application for dealing with specific privacy and security requirements related to certification process. Managing certification process (pre-certification and post-certification).*
PRIV_UC_004	*PR_005*	*MUST*	*Privacy compliance (e.g. compliance to the GDPR requirements)*	*Privacy compliance: - Specification of entities with the rights to access the data, including locally stored sensitive data, such as email or pictures. - User interface components with links to up-to-date information about privacy policies. - Contact links for users to send questions or concerns about their privacy. - Data protection compliance.*	*Privacy tests, e.g. test for deletion requests, create, maintain and test incident response plan;*

4 Platform-Centric Security and Privacy Requirements

In addition to the security and privacy requirements elicitation phase, which is presented in Section 3 (informed by the four use cases in NIMBLE), in this section we discuss the platform-centric security and privacy requirements capturing. For that purpose, we firstly designed the ***NIMBLE Security Architecture***, which is fully aligned to the NIMBLE's architecture and platform infrastructure (see D2.1 *"Platform Architecture Specification and Component Design"* and D3.1 *"Core Platform Infrastructure"*).

4.1 NIMBLE Security Architecture Overview

Figure 2 illustrates the NIMBLE Security Architecture, which is based on the NIMBLE architecture specification (D2.1) [D2.1_17]. It addresses basic security controls and security best practices for each of the NIMBLE core components, i.e. FrontEnd, Open API, Data Store, Data Management, Services, Service Discovery, Service Registry, and Cloud Service Bus component. Basic security controls for each of those components are described in more details in Sections 4.2.1 - 4.2.5. Specifically, NIMBLE Security Architecture designs core Security and Privacy Controls for: Identity Management, Access Control Management, Authorization, Data Provenance Management, Trust and Reputation Management, and Data Quality Management (described in Section 4.3.). Platform-centric security and privacy requirements for each of the identified controls are further elaborated in Section 4.4. The NIMBLE platform runs in the cloud, which adds both the platform service provider and the cloud service provider requirements to the list of additional security controls. Section 4.6 summarizes platform-centric security and privacy requirements, in the form of checklists to guide decisions about basic security expectations in the project.

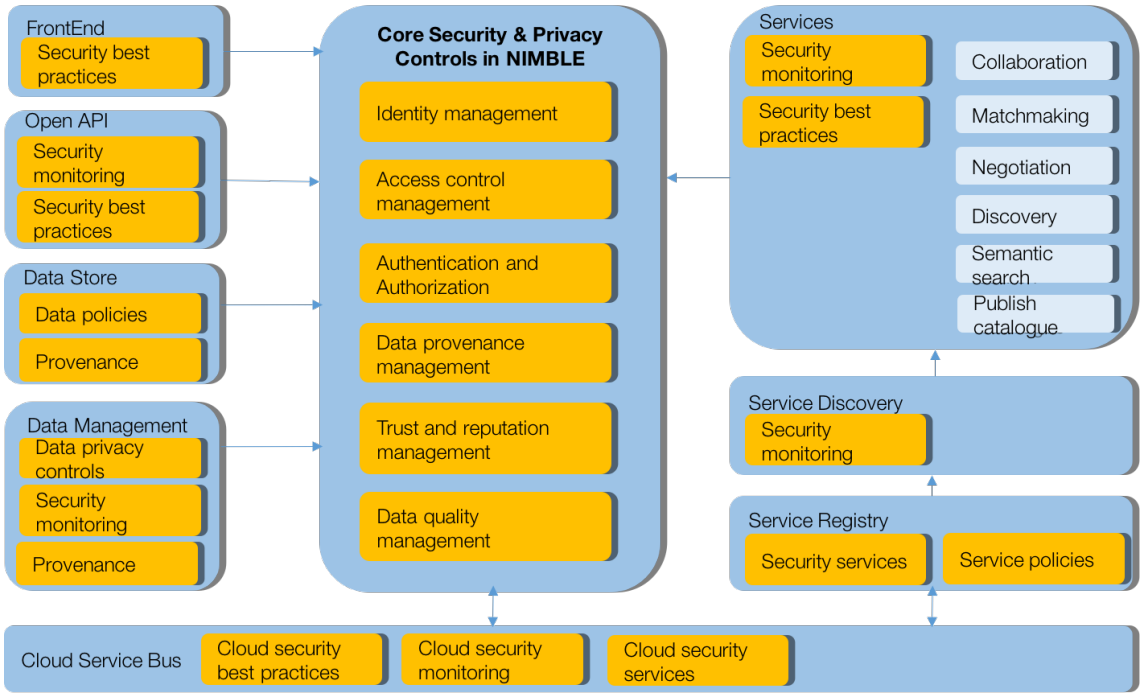

Figure 2: NIMBLE Security Architecture

4.2 Analysis of NIMBLE Security Controls

4.2.1 Front End Security Controls

The Front-end component of the NIMBLE platform provides a GUI for accessing the NIMBLE features and services. It controls user interaction requests and delegates them to the appropriate services (identity, search, publish, communication, negotiation, analytics – see D2.1). It is designed to ensure intuitive and easy-to-use interaction with the users, and to handle authentication, load balancing and related services. The adequate security controls need to ensure that **only authenticated users can access** the platform's services and data, according to policies set by platform administrators. In addition, security monitors must be in control of **provenance data**, revealing information about the platform's connection parameters (Information Disclosure, Tampering).

4.2.2 OpenAPI and its Security Controls

NIMBLE's Open API is dealing with a range of sensitive data and is calling for the following security control to be put in place:

- **Access control management**, defining how a software developer can access an API, what kind of security controls are in use, what set of security credentials must be acquired before a software developer can start working on an application that uses the API, etc.;
- **Security monitoring** applications, with the purpose to monitor unauthorized attempts to invoke an API, e.g. who is using the API and how;
- **Authorization methods**, regulating those applications and users who are authorized to use an API.

Additional security best practices which can make an impact on Open APIs are summarized below [BRAI16]:

- **Existing network security best practices**, e.g. firewalls, routers, management of TLS (Transport Layer Security) to protect assets, intrusion detection sensors;
- **Rate limiting mechanisms,** to control the amount of data that may be consumed from all users, including authorized users (for protecting the API against excessive traffic);
- **Verifying the identity** of both applications and users that consume the API;
- **Scanning incoming data for SQL injection**; scanning other malformed inputs designed to crash the system;
- **Putting traffic management features in place,** to control how much data each developer is allowed to access (e.g. to prevent against Insider attack).

4.2.3 Data Store, Data Management and Data Flow Security Controls

The Data Store in NIMBLE stores operational data, corporate data, product data (product catalogues), external data coming from sensors and applications, etc., which are all fed into the platform to support data processing, negotiation, sharing among partners, and more. Heterogeneous data is ingested into the platform via the Data Management component, which deals also with processing data for analytics and providing appropriate notifications.

Data generated from IoT devices are of interest for the NIMBLE project too, and could interact with other data, processes and applications running on the platform. Hence, the Data Store and Data Management in NIMBLE need to address data collection and fusion, and to enable

actionable insights out of the data streams and data oceans. The Data Management component must address data warehouse issues as well as real-time aspects (see D2.1).

In sum, securing heterogeneous data in NIMBLE requires appropriate security controls to be designed and implemented for various purposes:

- Security methods for **protecting against front end threats**,
- Security methods for **protecting against log threats (provenance data)**,
- Security methods **protecting against tampering and ensuring data integrity** (preventing against data breaches, loss of sensitive data, data manipulation and data sabotage),
- **Information disclosure from a data store or a data flow.** Data stores can leak the data, which could be caused by inappropriate use of security mechanisms. Hence, access controls and security groups need to be properly managed in the system. Data flows over a network or in a cloud are particularly susceptible to attacks, and should be monitored too.

Before designing the above-mentioned security controls, it is necessary to understand where sensitive data assets reside in the system, to determine their levels of data sensitivity by measuring related risks, to prioritize associated sensitive levels of data/ or risks, then remediate risks with data security controls (encryption, access controls), and continuously monitor data access [CHAN17].

4.2.4 Core Services, Service Registry and Service Discovery Security Controls

Another group of security controls in NIMBLE is designed to support the core services (product catalogue publishing, searching, negotiation, matchmaking), service registry and service discovery via the platform. For example, the Product Catalogue publishing process requires catalogue permission rules to be established, enforcing data confidentiality, integrity and authorization policies. These requirements call for the following security controls:

- **Controls for protecting published Product Catalogues against unauthorized access and distribution**:
    - catalogues encrypted to protect data,
    - catalogue access controls,
    - catalogue DRM (Digital Rights Management) defines: (i) when does product data /catalogue stop being available, (ii) decision to add dynamic watermarks that are displayed when the document is viewed,
    - setting limits for the access and visibility of data (for example, setting a number of times for viewing the content once first opened);
- **Controls for preventing Product Catalogues to be downloaded or saved locally on disk**;
- **SQL injection attack against Product Catalogues** and their data stored in databases, which lead to information disclosure and must be prevented.

Searching the content and performing any action that creates a query from user input, can lead to SQL injection attack. It happens when an attacker enters (untrusted) data (by accident or on purpose) that deviates the input (query) in a way that causes error leakage, damage to data, read data from the platform. This could be partially controlled by designing good client-side controls, although an attacker still can modify the code and bypass such validation controls. Fixing SQL injection requires input/ page validation to be performed, including strong input procedures that do not permit database manipulations.

4.2.5 Cloud Services Security Controls

Increased complexity in the connectivity and resource sharing via the cloud re-opens some traditional computer and network security issues, such as the need to provide data confidentiality, data integrity and system availability in the cloud. The potential of cloud to aggregate a large amount of sensitive data within its data centres, requires a high degree of confidence and data transparency in order for cloud providers to keep user's data isolated and protected [NIST-CC12] [NIST-SP15]. In this subsection, we investigate some common security monitoring services and best practices in the cloud, by looking at them from both cloud providers and cloud customers perspectives.
Note: A list of cloud provider security controls is presented in Table 28 (Section 4.5).

4.2.5.1 Threats coming from insiders at the cloud provider

Cloud providers can access all tenant's corporate data that is available via the cloud and is not protected [SHOS14]. Hence, the data in cloud should be protected either contractually (between the cloud provider and tenants) or cryptographically (encrypting the data and obfuscating the code before sending it to the cloud).

4.2.5.2 Threats coming from fellow tenants of the cloud system

There is also a set of threats to the cloud provider, which are performed by tenants to whom cloud providers give access to the system, e.g. tenants can attempt to hack the provider [SHOS14]. A fellow tenant can perform some action that shouldn't be allowed on the platform, e.g. tampering with other customers, or causing repudiation issues by using somebody's user data to sign in on the platform, or for spamming, running a botnet, piracy, etc. They can also direct attacks to other co-tenants.

4.2.6 Core Security and Privacy Controls in NIMBLE

Figure 2 illustrates core security and privacy controls of the NIMBLE Security Architecture, which includes the following functionalities:

- **Identity Management:** In multi-sided platforms, such as the NIMBLE platform, the concept of Identity Management extends from the users and services to their devices and sensors (IoT devices). It also extends from the core identities to identity of a group of users, objects and an identity based on specific features, e.g. quantity, ingredients, etc. In IoT-based multi-sided platforms, the authentication proof for devices can be obtained from identity relationships of devices with an owner, administrator, user or a group of stakeholders.
    - **Note:** A list of security requirements related to Identity Management, is given in Table 23.
- **Access Controls Management:** Although RBAC (*Role Based Access Control*) and GBAC (*Group Based Access Control*) can be used for handling system-wide policies in which certain roles or groups are allowed to perform certain operations, they cannot efficiently cover those use cases in which users allow other users to access their data without requiring a particular role to be defined by a system administrator. Hence, ABAC (*Attribute Based Access Control*) allows policies to be specified in terms of attributes that belong to a user, an object, an action performed by the user in an object or the environment [HU13].
    - **Note:** A list of security requirements related to Access Control Management, is given in Table 24.
- **Authentication and Authorization Management: Authentication** is an identity agreement between communicating parties and can be performed using various

authentication methods, e.g. passwords, two-factor authentication (password plus one-time unique code), biometric authentication (face recognition, voice recognition, fingerprint, etc.), gesture based authentication (keypad gestures, free form gestures, etc.). In multi-sided platforms (with various IoT aspects), there are some recommendations for complementing security tokens with stronger authentication methods, e.g. those with multiple factors, such as methods combining the context and the environment of the authentication process, use case specific factors, internal machine IDs, etc. (this is known as context-based authentication) [FRIE15]. **Authorization** is the response of the system that allows users/ devices to perform certain actions that include specific resources and services of the system.
    - Note: A list of relevant security requirements is given in Table 25.
- **Data Provenance Management:** Provenance has considerable value as a security measure, with the role to protect data integrity and confidentiality.
    - Note: A list of relevant security requirements is given in Table 26.
- **Trust and Reputation Management:** In [NIST-SP15], trust is defined as "the belief that an entity will behave in a predictable manner while performing specific functions, in specific environments and under specified conditions or circumstances." From an Information Security perspective, *trust is the belief that a security-relevant entity will behave in a predictable manner.* It is rather a subjective view on the complex interactions among entities (i.e., technical components, users), expressing its capability of operating within a defined risk tolerance, while preserving its confidentiality, integrity and availability of the information.
    - Note: A list of relevant security requirements is given in Table 27.
- **Data Integrity and Data Quality Management:** Data integrity guarantees that data are not modified in an unauthorized or undetected manner. Data quality guarantees data completeness and accuracy, allowing for data to be searched in an efficient manner. Both features are of considerable value for business entities and need to be secured in NIMBLE.
    - Note: A list of relevant security requirements is given in Table 28.

In the rest of this section, for each of the above-presented core security controls (functionalities), e.g. Identity Management, Access Controls Management, etc., we specify a set of core security requirements.

4.3 Core Security Requirements

4.3.1 Identity Management

Identity Management methods and techniques need to provide a simplified user experience for accessing various resources via the platform, greater control over sensitive corporate data, increased privacy controls and reduced risks and costs of data breaches. Identity Management in NIMBLE should be based on using the most appropriate security measures and best practices, e.g. password-based authentication, Single sign-on (SSO) mechanisms.

Some common identity management models include:

- **Isolated Identity Management:** It requires that each user possess an identifier for access to each isolated service, which is often difficult for users to manage;
- **Federated Identity Management:** A user of one service provider can access all services provided by another service provider in the group, with only a single identifier.

This is based on a set of agreements, which are defined among a group of service providers who recognise user identifiers from one another.

- **Centralized Identity Management:** In this model, the same identifier and credential are used by each service provider. This could be implemented by using a PKI: (i) a Certificate Authority (CA) issues certificates to users, or (ii) using the SSO model, which requires a user to login once and be authenticated automatically by all other service providers.

The increase in **identity theft** brought **two-factor authentication** methods for the identification of the user, in which the user needs a one-time password generated from a security token and sent via phone/ email, in addition to standard username/ password information. Identity management in multi-sided platforms requires generally stronger authentication, e.g. methods that includes **biometric information** (face recognition, fingerprints, iris scans) stored in a form of user's digital identities. In addition, methods for **preventing password guessing** and disabling an account after **a limited number of unsuccessful log-ins** can be used too, as well as methods for **timing-out idle logged-on sessions**.

Recently, a new approach to managing identities, based on the distributed trust models, came into focus. Here, the distributed trust model is empowered by **blockchain technology** for controlling user's identities. The two fundamental principles of such trusted identity management approach are:

- **The self-sovereign identity (user-centric identity) principle** empowers users to take full ownership and control of their identity information. This principle is based on two elements: consent and control [IBM17]. **Consent** is the agreement between the user and institutions, defining what personal information can be collected and used by whom and how. **Control** ensures that users have complete ownership of their personal data. The self-sovereign identity model puts privacy control in the hands of the users or intermediary identity broker, which consequently reduces the liability arising from identity breaches and fraud for businesses.
- **Distributed trust model:** Since identity is decentralized by default, it's critical to establish trust among users, identity providers and relying parties. By using blockchain-based distributed trust models, all parties can use an agreed-upon set of identity attributes to authenticate, verify and authorize individuals in order to perform business or social transactions.

In NIMBLE, the **distributed trust identity model based on blockchain technology** is seen as an identity model with the potential to overcome the paradox of user's control over data, to ease interoperability and to fully scale across participants in the business networks of the ConnectedFactories project (see: http://www.effra.eu/connectedfactories), through which NIMBLE has agreed to collaborate with another 9 FoF (Factories of the Future) projects (FoF-11-2016 research and innovation projects).

Table 23: Security requirements: Identity Management of Users, Devices and Services

Sec. Req. ID	Control name	Type	Priority	Description
SEC_IDM_01	***Identification Policy and Procedures***	*NFR*	*MUST*	*NIMBLE must follow defined Identification Policy and Procedures*

SEC_IDM02	***Federated Identity Management and SSO***	*FR*	*MUST*	*NIMBLE must provide Identity Management and SSO methods for the identification of users, devices and services*
SEC_IDM_02_1	*Federated Identity Management for **network access to privileged accounts***	*FR*	*MUST*	*Network access to privileged accounts must be addressed*
SEC_IDM_02_2	*Federated Identity Management for **network access to non-privileged accounts***	*FR*	*MUST*	*Network access to non-privileged accounts must be addressed*
SEC_IDM_02_3	*Federated Identity Management for **local access to privileged accounts***	*FR*	*MUST*	*Local access to privileged accounts must be addressed*
SEC_IDM_02_4	*Federated Identity Management for **local access to non-privileged accounts***	*FR*	*MUST*	*Local access to non-privileged accounts must be addressed*

4.3.2 Access Control Management

Table 24: Security requirements: Access Control Management

Sec. Req. ID	Control name	Type	Priority	Description
SEC_ACM_01	***Access Control Policy and Procedures***	*NFR*	*MUST*	*NIMBLE must follow defined Access Control Policy and Procedures*
SEC_ACM02	***Access Enforcement mechanisms***	*FR*	*MUST*	*NIMBLE must provide various Access Enforcement controls*
SEC_ACM02_1	***Mandatory** access controls*	*FR*	*MUST*	*Mandatory access controls must be provided*
SEC_ACM02_2	***Discretionary** access controls*	*FR*	*MUST*	*Discretionary access controls must be provided*
SEC_ACM02_3	***Role-based** access controls*	*FR*	*MUST*	*Role-based access controls must be provided*
SEC_ACM02_4	***Access to privileged functions***	*FR*	*MUST*	*Only to authorized users or services*
SEC_ACM02_5	***Dual authorization***	*FR*	*SHOULD*	*Only for selected users*

SEC_ACM02_6	***Review of user privileges***	*FR*	*SHOULD*	*Only for selected users*
SEC_ACM02_7	***Control of user privileges***	*FR*	*SHOULD*	*E.g. prohibit non-privileged users from accessing privileged content*
SEC_ACM_03	***Information Flow Enforcement mechanisms***	*FR*	*MUST*	*NIMBLE must provide Information Flow Enforcement mechanisms*
SEC_ACM_03_1	***Domain authentication***	*FR*	*MUST*	*E.g. different user authentication for different domains*
SEC_ACM_03_2	***Validation of metadata***	*FR*	*MUST*	*E.g. validation of accuracy and completeness of metadata*
SEC_ACM_03_3	***Security policy filters***	*FR*	*SHOULD*	*E.g. enable/ disable information flow, introduce constraints, re-configure filters*
SEC_ACM_04	***Account Management***	*FR*	*MUST*	*NIMBLE must support various Account Management controls*
SEC_ACM_04_1	***Dynamic account creation***	*FR*	*MUST*	*Must provide adequate services*
SEC_ACM_04_2	***Dynamic privilege management***	*FR*	*MUST*	*Must provide adequate services*
SEC_ACM_04_3	***Account monitoring***	*FR*	*MUST*	*Including successful and unsuccessful login attempts*
SEC_ACM_04_4	***Account maintenance***	*FR*	*MUST*	*Removing inactive accounts, high-risk user accounts, temporary accounts*
SEC_ACM_05	***Access Control for Mobile Devices***	*FR*	*MUST*	*E.g. container based encryption*
SEC_ACM_06	*Access Control for* ***Security Attributes Management***	*FR*	*COULD*	*Only for authorized users*
SEC_ACM06_1	***Security value changes***	*FR*	*COULD*	*Only for authorized users*
SEC_ACM06_2	***Security value maintenance and configuration***	*FR*	*COULD*	*Only for authorized users*
SEC_ACM07	***Access Controls for Information Sharing***	*FR*	*MUST*	*Only for authorized users*
SEC_ACM07_1	***Information Search***	*FR*	*MUST*	*Must provide adequate services*

	and Retrieval			
SEC_ACM07_2	***Decision Support***	*FR*	*MUST*	*Must provide adequate services*

4.3.3 Requirements Related to Authentication and Authorization Management

Table 25: Platform-related security requirements: Authentication and Authorization Management

Sec. Req. ID	Control name	Type	Priority	Description
SEC_AAM_01	***Authentication Policy and Procedures***	*NFR*	*MUST*	*NIMBLE must follow defined Authentication Policy*
SEC_AAM_02	***Authentication of Users, Devices and Services***	*FR*	*MUST*	*NIMBLE must provide various authentication mechanisms*
SEC_AAM_02_1	*User Authentication for* ***network access to privileged accounts***	*FR*	*MUST*	*Authentication must be provided for network access to privileged accounts*
SEC_AAM_02_2	*User Authentication for* ***network access to non-privileged accounts***	*FR*	*MUST*	*Authentication must be provided for network access to non- privileged accounts*
SEC_AAM_02_3	*User Authentication for* ***local access to privileged accounts***	*FR*	*MUST*	*Authentication must be provided for local access to privileged accounts*
SEC_AAM_02_4	*User Authentication for* ***local access to non-privileged accounts***	*FR*	*MUST*	*Authentication must be provided for local access to non-privileged accounts*
SEC_AAM_02_5	***Group Authentication***	*FR*	*MUST*	*Must provide adequate services*
SEC_AAM_02-6	***Cryptographic bidirectional network authentication*** *of devices*	*FR*	*SHOULD*	*Should provide adequate services and algorithms*
SEC_AAM_03	***Authentication Management***	*FR*	*MUST*	*Authentication Management services must be provided*
SEC_AAM_03_1	***Password based authentication***	*FR*	*MUST*	*Adequate services must be provided*
SEC_AAM_03_2	***Cross-organization credential management***	*FR*	*MUST*	*Adequate services must be provided*
SEC_AAM_03_3	***Expiration of cached authentication***	*FR*	*SHOULD*	*Monitoring services must be provided*

SEC_AAM_03_4	***Authentication feedback***	*FR*	*SHOULD*	*Monitoring services must be provided*
SEC_AAM_03_5	***Re-Authentication support***	*FR*	*SHOULD*	*Adequate services must be provided, e.g. limited number of repeated re-authentication services*

4.3.4 Data Provenance Management

Table 26: Security requirements: Data Provenance Management

Sec. Req. ID	Control name	Type	Priority	Description
SEC_PROV_01	***Recording information on data origin***	*FR*	*MUST*	*E.g. when and where is data coming from*
SEC_PROV_02	***Recording information on data modification***	*FR*	*MUST*	*E.g. who modified data; when is the data modified*

4.3.5 Trust and Reputation Management

The NIMBLE platform is designed to be one of the building blocks of the EU Digital Single Market strategy. In that context, it is necessary for NIMBLE to comply with the major EU regulations, offering legal frameworks for people, business entities and public administration for performing cross-border electronic transactions in a safe way. In the EU, the **Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)** has been created in 2014 and fully adopted in September 2015 [EUR-LEX14]. With respect to electronic Trust Services (eTS), this Regulation aims at fostering the security assessment (certification and validation) of qualified signature and seal devices, technical specification and formats of trusted lists and services, to encourage users in using electronic services. Hence, trusted services in NIMBLE are recognized as one of important (soft-)security requirements (see Table 27 below).

Table 27: Security requirements: Trust and Reputation Management

Sec. Req. ID	Control name	Type	Priority	Description
SEC_TRM01	***Electronic Trust Services (eTS) regulation***	*NFR*	*SHOULD*	*NIMBLE should comply with the eTS regulation [EUR-LEX14]*
SEC_TRM02	***Reputation of users and services*** *must be automatically estimated*	*FR*	*MUST*	*This requirement will be elaborated in more details in task T6.3 "Trust and Reputation Management"*

4.3.6 Data and Data Quality Management

Table 28: Security requirements: Data Integrity and Data Quality Management

Sec. Req. ID	Control name	Type	Priority	Description with a view to GDPR
SEC_DIDQ_01	***Data Integrity and Data Quality Policy***	*NFR*	*MUST*	*NIMBLE must follow the **Data Integrity and Data Quality Policy**, which is based on the NIMBLE Privacy Requirements Framework and the anticipated GDPR implications on NIMBLE. The Data Integrity and Data Quality Policy will be specified in the **Plan for the NIMBLE governance**.*
SEC_DIDQ_02	***Data input validation***	*FR*	*MUST*	*Controls over various factors: predictable behaviour, manual override, timing, etc. This requirement corresponds to the Data Quality Principle and the **GDPR requirement for verifying if sensitive data is accurate, complete and up-to-date**. This is also about verifying the subject's age requirement.*
SEC_DIDQ_03	***Data and metadata protection***	*FR*	*MUST*	*Protection against unauthorized access and manipulation; Automated restricted access; Cryptographic protection;* ***GDPR requirement for deletion of personal data and/or personal data modification*** *by the data subject;* ***GDPR requirement for supporting subject's access*** *requests to personal and sensitive data;*
SEC_DIDQ_03_1	***Data protection at rest***	*FR*	*MUST*	*Cryptographic protection, off-line storage;* ***GDPR requirement for deletion of personal data and/or personal data modification*** *by the data subject;*
SEC_DIDQ_03_2	***Data protection in shared resources***	*FR*	*MUST*	*Cryptographic protection;* ***GDPR requirement for deletion of personal data and/or personal data modification*** *by the data subject;*
SEC_DIDQ_04	***Notification of data integrity violations***	*FR*	*SHOULD*	*Monitoring services must be provided;* ***GDPR requirement for detecting, reporting and investigating personal data breaches****;* ***GDPR requirement for reviewing existing privacy notices and keeping them up-to-date****;*

SEC_DIDQ_05	***Informed consent by Design***	*NFR*	*MUST*	*User must issue their informed consent on the data usage, which prevents the use of data in a way that is not according to the user wish;* ***GDPR requirement for implementing privacy procedures for seeking, recording, and managing user's consent.***

4.4 Platform Provider Security Requirements

Table 29 captures platform service provider security requirements, which are here characterized as non-functional security (NFS) requirements, as they do not directly influence the design and functionality of the NIMBLE system. Rather, these requirements look at the security features that should be provided by the future NIMBLE platform service providers.

Table 29: Platform Service Provider Security Requirements

Sec. Req. ID	Control name	Type	Priority	Description with a view to GDPR
SEC_PLAT_01	***Security Monitoring***	*NFR*	*MUST*	*Continuous monitoring for: Insider threat, Anomalous system behaviour, Inbound and outbound comm. traffic Monitoring for Information Disclosure;* ***GDPR requirement for detecting, reporting and investigating personal data breaches****;*
SEC_PLAT_02	***Security Assessment***	*NFR*	*SHOULD*	*Penetration testing; Continuous Threat analysis;* ***GDPR requirement for assessing security and privacy impact****;*
SEC_PLAT_03	***Risk Assessment***	*NFR*	*SHOULD*	*Review of historic audit logs; Trend analyses, Penetration testing*
SEC_PLAT_04	***Security Planning***	*NFR*	*MUST*	*Information Security Architecture and Design;* ***GDPR requirement to incorporate the guidance from the Article 29 Working Party***
SEC_PLAT_05	***Audit Event Controls***	*NFR*	*SHOULD*	*Adequate services must be provided*
SEC_PLAT_05_1	*Audit* ***recording and storing***	*NFR*	*SHOULD*	*Content of audit; Transfer to alternative storage;*
SEC_PLAT_05_2	*Audit* ***review and analyses***	*NFR*	*SHOULD*	*Review of the content of audit; Analyses of the content of audit*

SEC_PLAT_05_3	*Audit **correlations with other sources***	*NFR*	*COULD*	*E.g. with nontechnical sources*
SEC_PLAT_05_4	***Protection of audit information***	*NFR*	*SHOULD*	*E.g. read- only access; cryptographic protection*
SEC_PLAT_06	***Contingency Plan***	*NFR*	*MUST*	*It must identify critical assets and define contingency procedures*
SEC_PLAT_06_1	*Information **system backup and recovery mechanisms***	*NFR*	*MUST*	*Restore within time period; Transaction recovery, etc.*
SEC_PLAT_06_2	***Incident response***	*NFR*	*SHOULD*	*Monitoring, Reporting, Incident response plan;*
SEC_PLAT_07	***Malicious code protection***	*NFR*	*SHOULD*	*E.g. non-privileged users, automatic updates, detection of unauthorized instructions, etc.*
SEC_PLAT_08	***Spam protection***	*NFR*	*SHOULD*	*Unauthorized services; Blacklisting*

4.5 Cloud Provider Security Requirements

One of the top security requirements in NIMBLE, related to its communication and resource sharing via cloud, is about implementing a security perimeter answering questions such as - who and what is allowed to access user's data and platform services, who has ability to monitor and/ or modify data and services in the cloud, etc. Key management of the user cryptographic keys inside a cloud is still an open issue, because the keys may be permanently stored in the VM for recovery purposes, or already migrated to different hardware [NIST-CC12].
Table 30 summarizes cloud service provider security requirements in NIMBLE, which are also characterized as non-functional requirements (NFR) with security features that should be guaranteed by the cloud service provider.

Table 30: Cloud Service Provider Security Requirements

Sec. Req. ID	Control name	Type	Priority	Description
SEC_CC_01	***Data protection***	*NFR*	*MUST*	*Protecting the confidentiality and integrity of data; Ensuring data availability (CIA)*
SEC_CC_01_1	*Avoid unintended **distribution of sensitive data***	*NFR*	*MUST*	*Monitoring services must be provided*
SEC_CC_01_2	*Avoid insecure or incomplete **data deletion***	*NFR*	*MUST*	*Monitoring services must be provided*
SEC_CC_01_3	***Encrypted data transfer** and application*	*NFR*	*SHOULD*	*Data transfer and application interaction within a cloud should*

	interaction			*use encryption*
SEC_CC_02	***System integrity check of cloud-hosted applications***	*NFR*	*SHOULD*	*It can prevent intentional sabotage or subversion of the functionality of the cloud.*
SEC_CC_03	***Key management***	*NFR*	*SHOULD*	*Key management to protect user's cryptographic keys*
SEC_CC_04	***Handling of security incidents***	*NFR*	*SHOULD*	*E.g. detecting and reporting security breaches*

4.6 Core Privacy Requirements

Protecting privacy of users (business entities) in NIMBLE is one of the critically important requirement. To address privacy requirement, we follow the Microsoft's Privacy Guidelines for Developing Software Products and Services [PRIV-GUID08].

Table 31: Platform-centric privacy requirements

Privacy Req. ID	Control name	Priority	Description with a view to GDPR
PRIV_PLAT_01	***Data privacy***	*MUST*	*NIMBLE must ensure privacy of collected data (including audit data). It must ensure the integrity of privacy data, which is required for auditing purposes;* ***GDPR requirement for detecting, reporting and investigating personal data breaches***
PRIV_PLAT_02	***Platform code and services privacy***	*MUST*	*NIMBLE must ensure that no code, services or platform features are released unless they meet privacy standards that are appropriate for public releases;* ***GDPR requirement to incorporate the guidance from the Article 29 Working Party***
PRIV_PLAT_03	***Preventing unauthorized access***	*MUST*	*NIMBLE must provide appropriate security mechanisms to prevent unauthorized access, e.g. file permissions and/ or encryption;* ***GDPR requirement for supporting subject's access*** *requests to personal and sensitive data*
PRIV_PLAT_04	***Informed Consent***	*MUST*	*NIMBLE must provide users with notice and get consent prior to storage of sensitive data;* ***GDPR requirement for implementing privacy procedures for seeking, recording, and managing user's consent.***

PRIV_PLAT_05	***Data minimization principle***	*MUST*	*NIMBLE must ensure that only minimum amount of data is stored for business purpose; Obfuscate or remove IP address if not essential*
PRIV_PLAT_06	***Prohibiting interaction with children or non-business entities***	*MUST*	*NIMBLE must ensure that children or non-business entities are not interacting via the platform.* ***GDPR requirement for verifying if sensitive data is accurate, complete and up-to-date, and for verifying the subjects' ages.***

4.7 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.

4.7.1 Core Security and Privacy Requirements: Priority MUST

Table 32: Core Security and Privacy Requirement: Priority - MUST

Sec. Req. ID	Control name	Type	Priority	Security functionality	Implem. plan
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_IDM02	***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*

4.7.2 Core Security and Privacy Requirements: Priority SHOULD

Table 33: Core Security and Privacy Requirement: Priority - SHOULD

Sec. Req. ID	Control name	Type	Priority	Security functionality	Implem. plan

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*

4.7.3 Core Security and Privacy Requirements: Priority COULD

Table 34: Core Security and Privacy Requirement: Priority - COULD

Sec. Req. ID	Control name	Type	Priority	Security functionality	Implem. plan
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*

4.7.4 Platform Service Provider Security Requirements: Priority MUST

The following is a checklist of security considerations to be implemented at the platform provider side. Note that NIMBLE doesn't build a specific *Implementation Plan for Security Functionalities of the Platform Providers.*

Table 35: Platform Service Provider Security Requirement: Priority - MUST

Sec. Req. ID	Control 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*

4.7.5 Platform Service Provider Security Requirements: Priority SHOULD

Table 36: Platform Service Provider Security Requirement: Priority - SHOULD

Sec. Req. ID	Control 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*

4.7.6 Cloud Service Provider Security Requirements: Priority MUST

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

Table 37: Cloud Service Provider Security Requirement: Priority - MUST

Sec. Req. ID	Control 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*

4.7.7 Cloud Service Provider Security Requirements: Priority SHOULD

Table 38: Cloud Service Provider Security Requirement: Priority - SHOULD

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

5 Security and Privacy Requirements Mapping and Management

To identify possible inconsistences and conflicts between use case-centric and platform-centric security requirements and to control the complexity of (use case) domains, the complexity of regulatory environment and the actual platform development (see D2.1 and D3.1), we perform the following mappings between security and privacy requirements:

- Mapping between use case-centric functional and non-functional security requirements and use case requirements for Micuna, presented in Figure 3.
- Mapping between use case-centric functional and non-functional security requirements and use case requirements for Piacenza, presented in Figure 4.
- Mapping between use case-centric functional and non-functional security requirements and use case requirements for Lindbäck, presented in Figure 5.
- Mapping between use case-centric functional and non-functional security requirements and use case requirements for Whirlpool, presented in Figure 6.

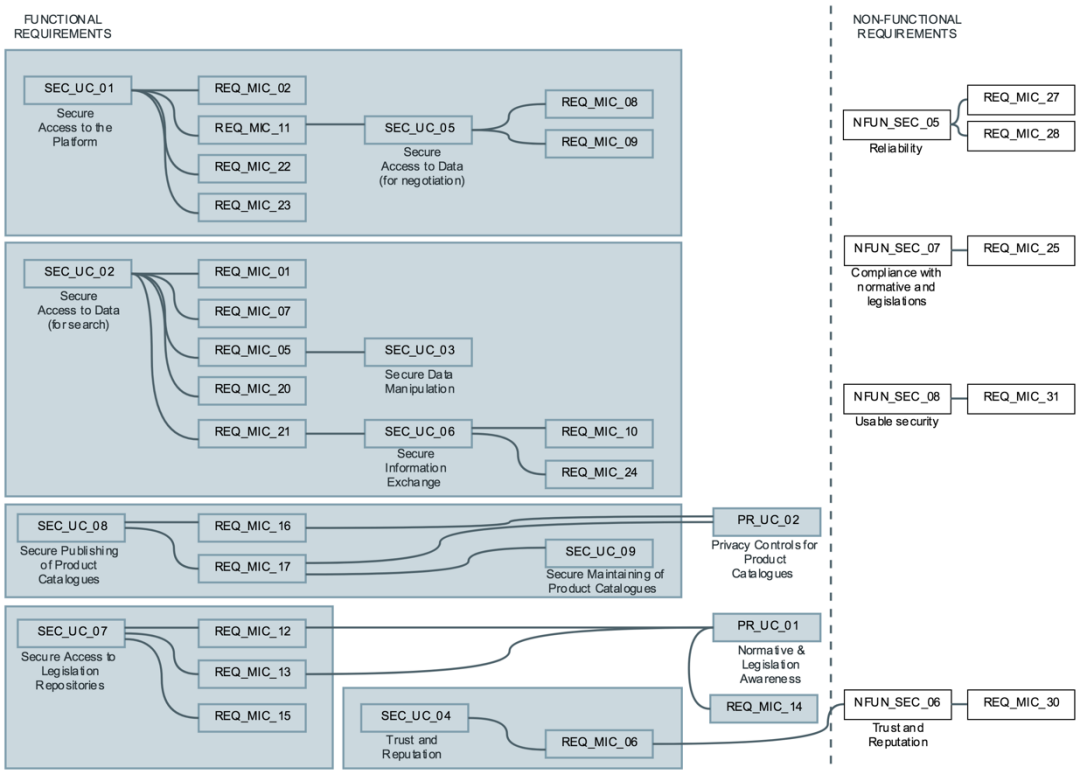

Figure 3: Mapping between use case-centric functional and non-functional security requirements and use case requirements for Micuna

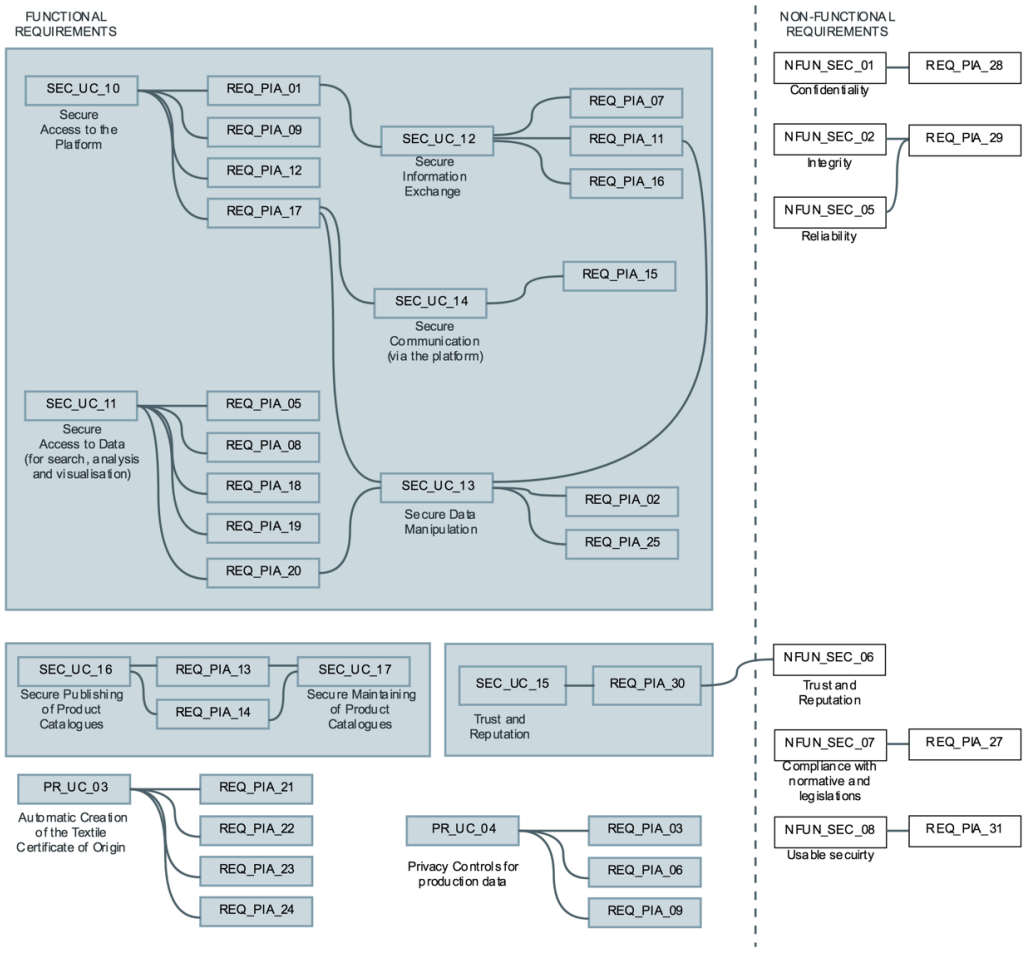

Figure 4: Mapping between use case-centric functional and non-functional security requirements and use case requirements for Piacenza

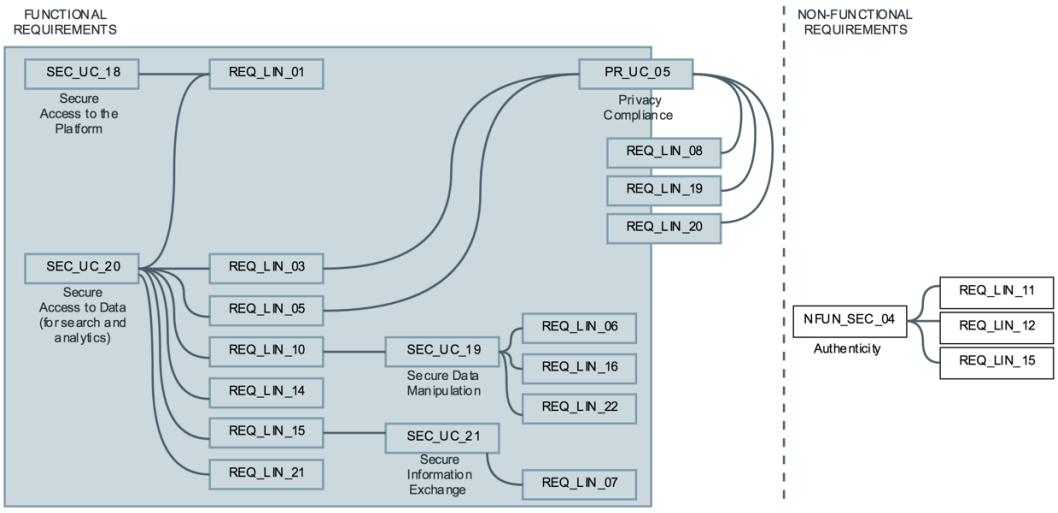

Figure 5: Mapping between use case-centric functional and non-functional security requirements and use case requirements for Lindbäcks

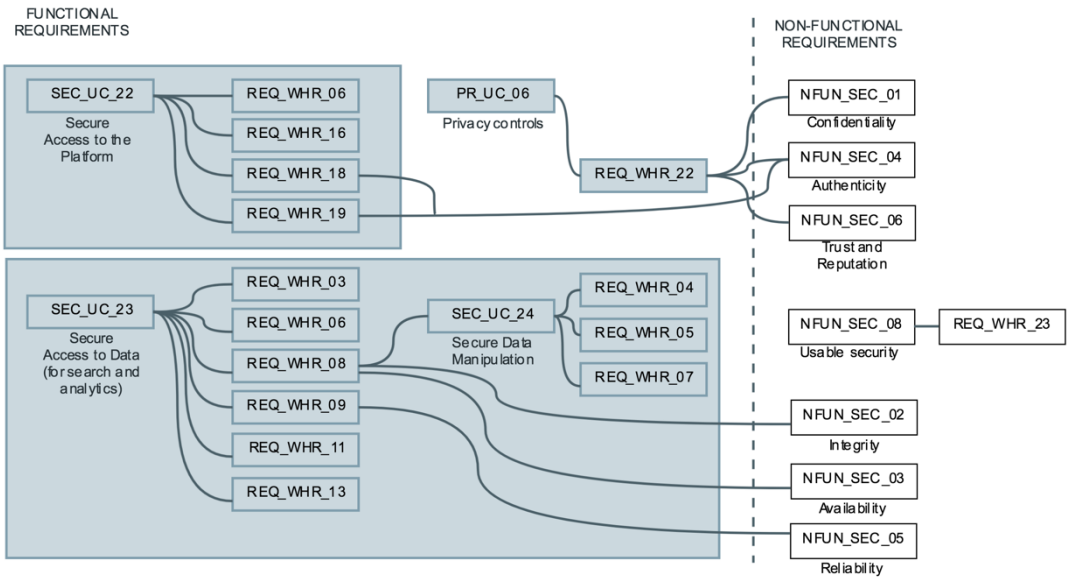

Figure 6: Mapping between use case-centric functional and non-functional security requirements and use case requirements for Whirlpool

To eliminate functional dependencies between requirements, which occur during requirements decomposition and could be either technology driven (e.g. dependencies between business rules, UI design and backend system (data storage) or end-user driven, we map core platform-centric and use case-centric functional and non-functional security requirements, which is presented in Figure 7.

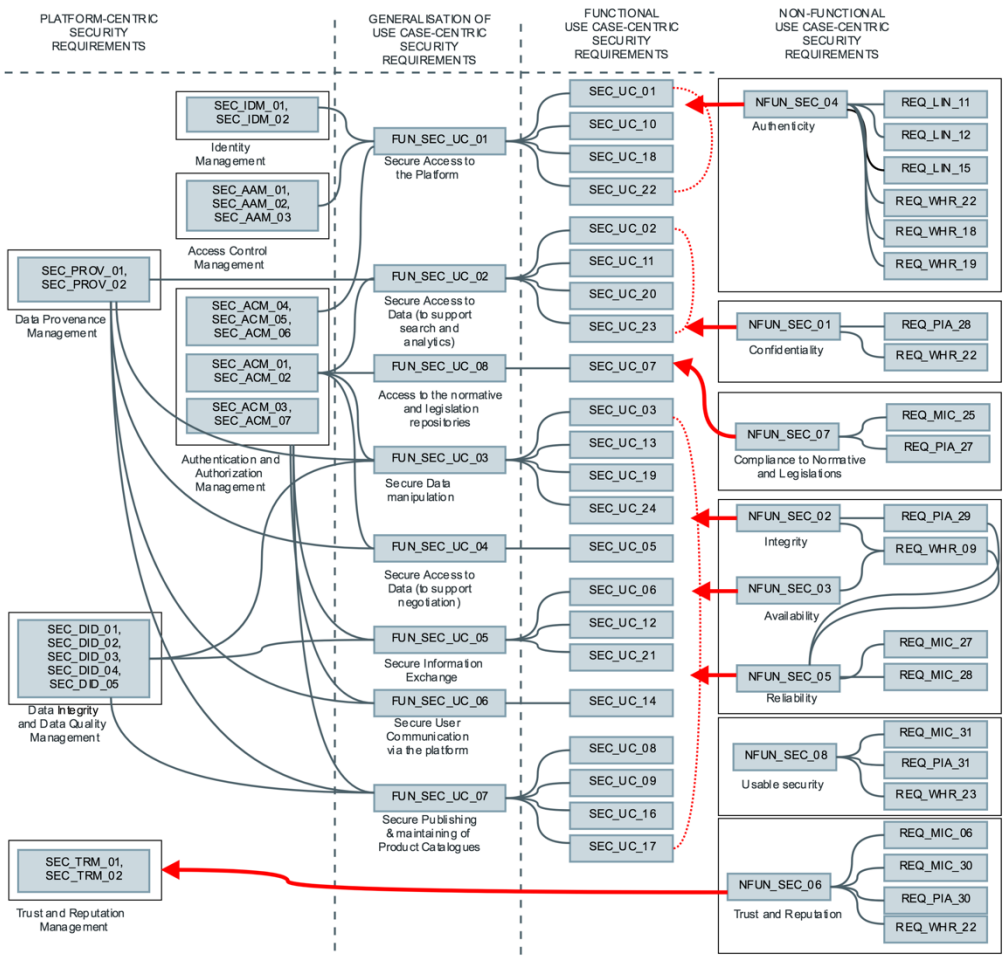

Figure 7: Mapping between core platform-centric and use case-centric functional and non-functional security requirements

Finally, for the management and traceability of security and privacy requirements in NIMBLE, we created an online collaborative spreadsheet, which is available from the project website.

6 Evaluation of Security Requirements Using STRIDE Threats and Vulnerabilities Analysis

The evaluation of security requirements in NIMBLE is based on the STRIDE analysis (see Section 2.2 for more details).

6.1 Data Flow Diagrams (DFDs) of Core Services In NIMBLE

We use Data Flow Diagrams (DFDs) to describe the following core services in NIMBLE:

- **User registration** on the platform (Figure 8)
- **User login** (Figure 9)
- **Search** for product (searching through Product Catalogue) (Figure 10)
- **Publish** new Product Catalogue (Figure 11)
- **Negotiate features for** product (Figure 12)

6.1.1 User registration DFD

A member of the public who wants to become a new registered user of the NIMBLE platform, fills the registration details in the required registration form. The registration parameters are checked for their validity, e.g. in case of user registration, we check for user's date of birth (note that this presents one aspect of our GDPR compliance). If the validity is correct, the registration procedure is moving on and the user account is generated. The username/ user account is stored with default password in *Account DB*. The registration process is confirmed by sending the registration confirmation message to the user (see Figure 8).

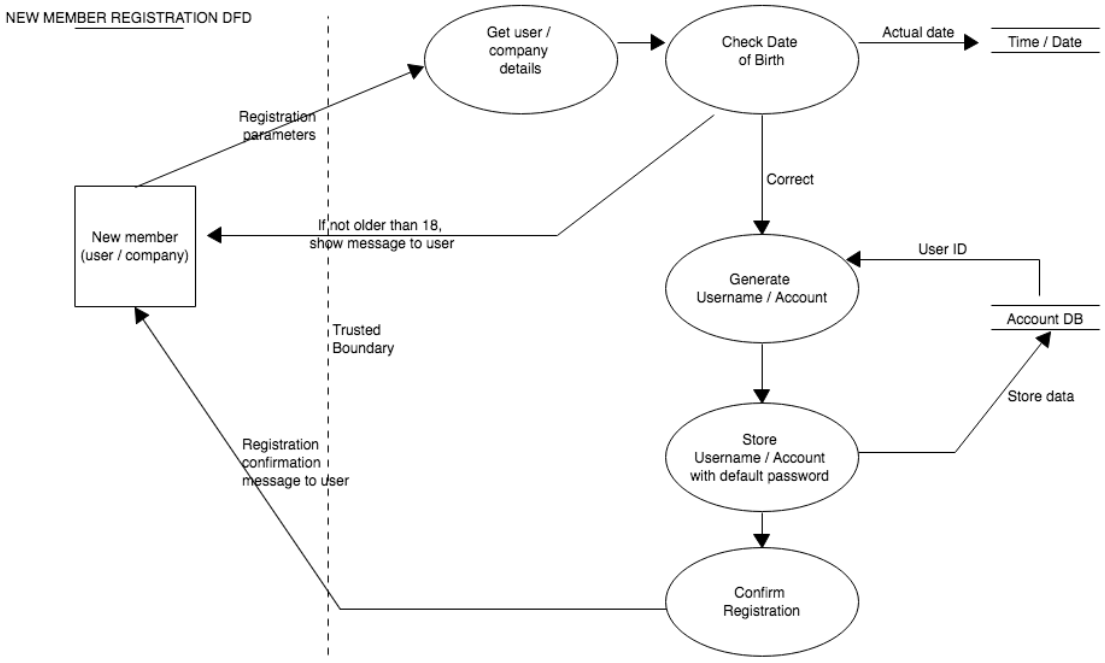

Figure 8: New member registration DFD

6.1.2 User login DFD

The user enters the login parameters in the login form. Login procedure starts with the authentication step, in which the user's account parameters are firstly checked in *Account DB* (checking if the user is registered on the platform), and secondly, the user identity is checked in *Log record DB*. If the user account is found in *Account DB* and the user identity exists in *Log record DB*, the authorization step is successfully finished. The final identity request is sent to *Login Processing service*, which performs the login of the user (see Figure 9).

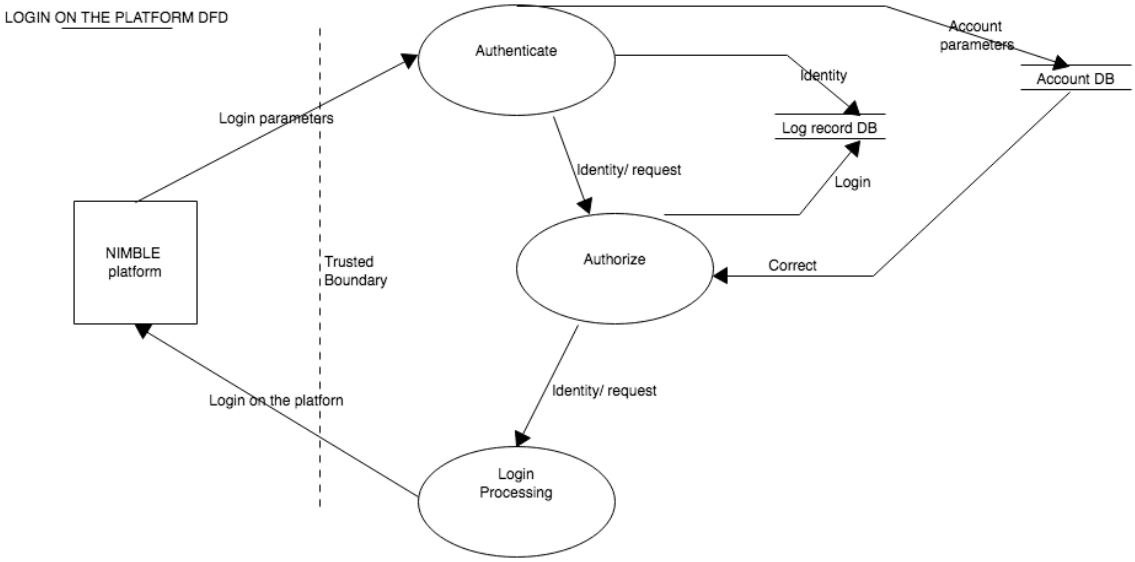

Figure 9: Login DFD

6.1.3 Searching for product DFD

After checking for the user's identity through authentication and authorization of the user to perform searching services on the platform, the search request proceeds to *Product Catalogue DB*, and the search results are returned to the user.

Note that searching process includes two trusted boundaries: the first one in positioned between the user and the platform security controls (Authentication, Authorization), and the second one is in between of the security controls and the platform's *Product Catalogue* (see Figure 10).

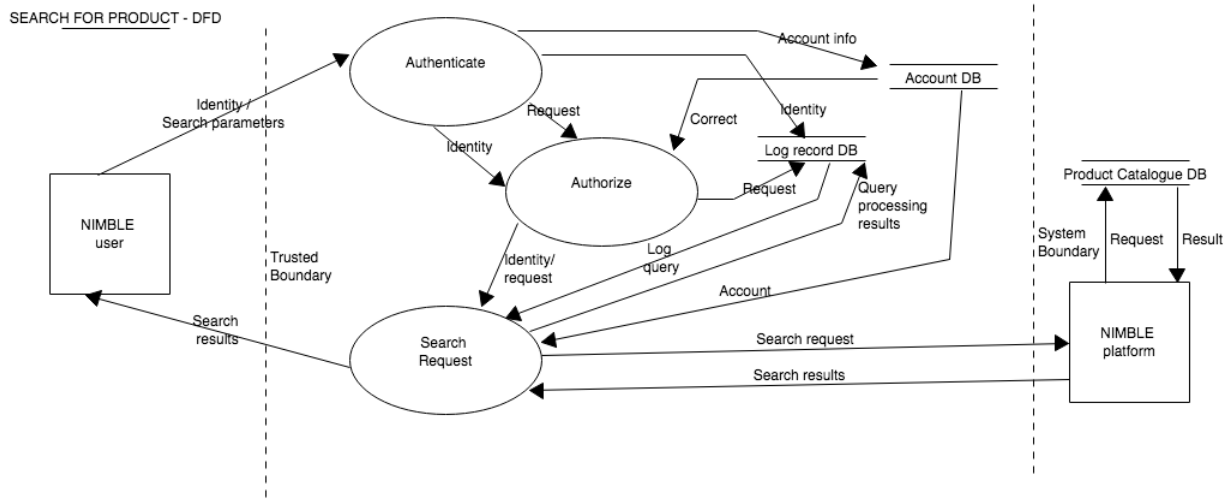

Figure 10: Searching for product DFD

6.1.4 Publishing Product Catalogue DFD

After checking for the user's identity through authentication and authorization of the user to publish new Product Catalogue on the platform, the *Publish Product Catalogue Request* is sent to *Product Catalogue DB*. The results of the publishing process are returned to the user (see Figure 11).

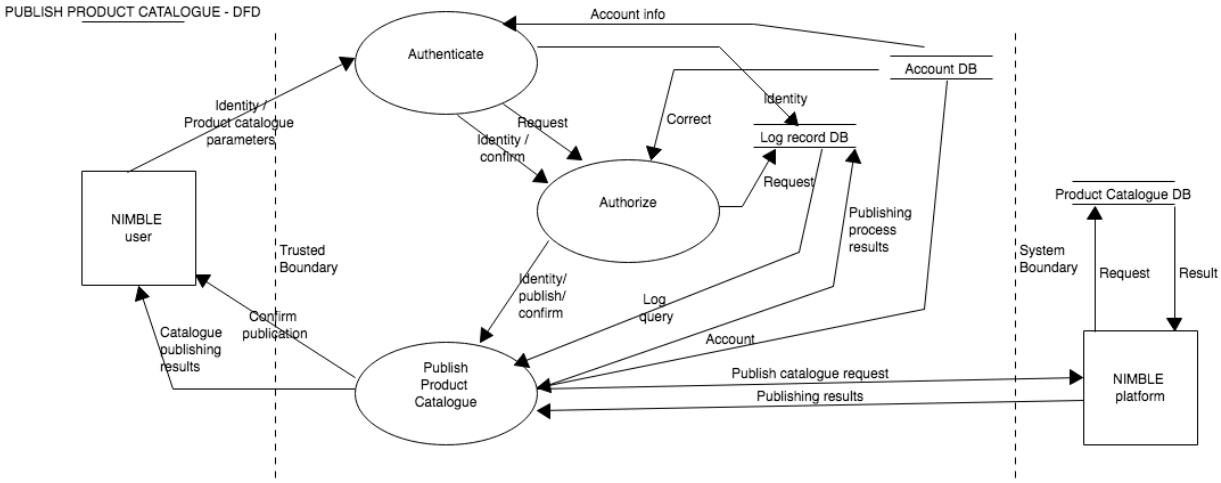

Figure 11: Publishing Product Catalogue DFD

6.1.5 Negotiating Features of Products DFD

This DFD involves two or more negotiation sides. After checking the identity of each of the users participating in the negotiation process, and after checking for each of the users if they are authorized to negotiate product features and create new negotiation contracts, *Negotiation Contract Request* is sent to *Negotiation Contract DB*. The confirmation message and the results of the negotiation process are forwarded to the user (see Figure 12).

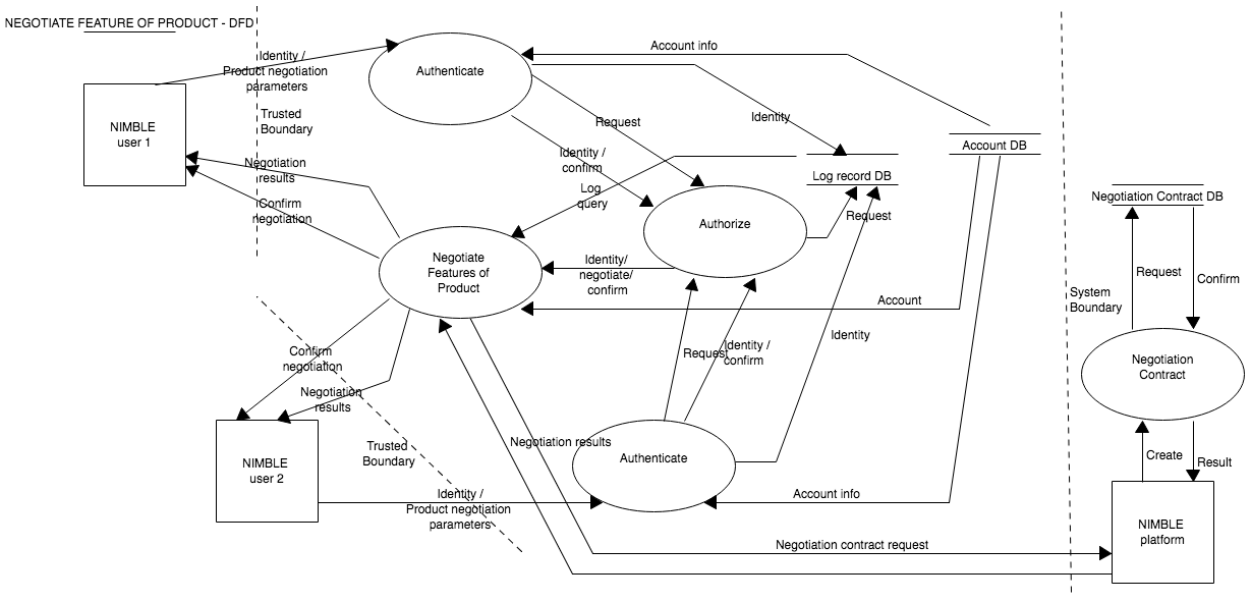

Figure 12: Negotiating Features of Product DFD

6.2 STRIDE-based Evaluation of Security Requirements in NIMBLE

For each of six STRIDE threats categories (i.e. S=Spoofing, T=Tampering, R=Repudiation, I=Information Disclosure, D=Denial of Service, and E=Elevation of Privilege), we played the Evaluation of Privilege (EOP) game, in order to identify potential threats in the system. The EOP game is played based on DFDs of core services in NIMBLE (see Figures 8-12) and the results of the game are recorded in Table 39.

In EOP, the analysis is performed for both the external and the internal interactors identified in DFDs, e.g. NIMBLE user is an external interactor, while the core NIMBLE platform and its services are internal interactors. For playing the EOP game, we used the evocative approach to form the hint sentences, e.g. "An attacker can…". The hint sentences are "played" for each of DFDs in order to make observations and identify threats in DFDs (threats in the system), related to hint sentences (threats in the cards). Practically, the EOP game is based on the following interaction:

Threats in the cards →--- finding ---→ Threats in the system

For example, the hint sentences for spoofing could be constructed in the following way (see Table 39 for formulated hint sentences):

1. An attacker (can) ... [**Pretend to be someone else**] (SE1) by using [**fake credentials**] (SE1.1.2) which are [**illegally obtained**] (SE1.1).
2. An attacker (can) … [**Simulate fake activities via the platform**] (SE2) through [**Malware simulating keyboard actions**] (SE2.1).

Table 39: STRIDE Analysis in NIMBLE

	External interactors	*Internal interactors*
Threat	NIMBLE user (user 1, user 2…) "An Attacker (can) ..."/ SE1.../ TE1… etc.	NIMBLE platform "NIMBLE platform can …"/SI1
S=Spoofing *(pretending to be something or someone other than yourself)*	**SE1. Pretend to be someone else** **SE1.1. Illegally obtained credentials** SE1.1.1. Legal credentials obtained by the attacker SE1.1.2. Fake credentials SE1.1.3. Credentials stolen from insecure storage **SE1.2. Weak password security** SE1.2.1. Password cracked and insecure SE1.2.2. Default password insecure SE1.2.3. Password stored in an insecure storage **SE1.3. Weak authentication** SE1.3.1. Lack of authentication mechanisms SE1.3.2. Vulnerable authentication mechanisms **SE1.4. Exposure to brute force attack** SE1.4.1. Lack of mechanisms to prevent brute force attack SE1.4.2. Weak mechanisms to block brute force attack **SE1.5. Weak session mechanisms** SE1.5.1. Lack of session timeout/ validity time mechanisms SE1.5.2. Lack of mechanisms for checking validity of session communication (e.g. Token Relay) **SE2. Simulate fake activities via the platform** SE2.1. Malware simulating keyboard actions SE2.2. Malware simulating user's actions	**SI1. Be a fraud site** SI1.1. Domain spoofing SI1.2. Content spoofing SI1.3. ARP spoofing **SI2. Be a fake site** **SI2.1. Illegally obtained credentials** SI2.1.1. Legal credentials obtained by the attacker SI2.1.2. Fake credentials **SI2.2. Weak authentication** SI2.2.1. Not sufficient authentication mechanisms (plus the platform doesn't force a better authentication) SI2.2.2. Vulnerable authentication mechanisms **SI3. Simulate fake activities** SI3.1. Malware simulating fake platform actions (e.g. platform is sending messages, spamming)
T=Tampering ***(****modifying something on disk, on a network, or in memory, by the user who is not supposed to*	**TE1. Take control over data** TE1.1. Integrity controls are not build using standard crypto TE1.2. Access to data is not defined in a security kernel to prevent unauthorized access and enable reference monitoring (e.g. access controls not defined using Access Management	**TI1. Embed malware** **TI1.1. Malware taking control over data** **TI1.2. Malware taking control over network** TI1.2.1. Attacker/ malware can modify keyboard input

modify it)	tools) TE1.3. Weak access controls to state data **TE2. Take control over network** TE2.1. Attacker/ malware can bypass weak permissions TE2.2. Attacker/ malware can modify messages sent or received over platform **TE3. Take control over memory** TE3.1. Attacker/ malware modify browser memory	**TI1.3. Malware taking control over memory**
R=Repudiation ***(****the user is claiming that he didn't do something, regardless of whether he did it or not****)***	**RE1. Access and manipulate data** RE1.1. Weak authentication RE1.2. Lack of provenance mechanisms RE1.3. Lack of access control validation mechanisms RE1.4. Lack of integrity controls **RE2. Perform unauthenticated activities and transactions** RE2.1. Bypass weak authentication RE2.2. Lack of transaction signature mechanisms (e.g. Token Relay in microservice architecture) RE2.3. Lack of provenance mechanisms RE2.4. Lack of transaction validation	**RI1. Denial of having carried out activities and transactions** RI1.1. No log records RI1.2. No signatures and records about performed activities
I=Information Disclosure *(exposing information to people who are not authorized to see it)*	**IE1. Access security sensitive content** IE1.1. Use of non-standard encryption algorithms IE1.2. Lack of authentication for endpoints of a network connection IE1.3. Malware stealing user credentials via keyboard record, screenshots, etc. **IE2. Weak security controls** IE2.1. Lack of message security controls IE2.2. Lack of channel security controls	**II1. Expose sensitive information to public** II1.1. Vulnerable search algorithms II1.2. Vulnerable logging mechanisms **II2. Information leakage** II2.1. Encryption key stored on the platform II2.2. Temporary files not deleted **II3. Cheating user input** II3.1. Fishing
D=Denial of Service *(absorbing resources needed to provide service)*	**DOSE1. Blocking of a client** DOSE1.1. Client unavailable DOSE1.2. Weak authentication **DOSE2. Blocking of a server** DOSE2.1. Server unavailable (crash) **DOSE3. Channel overload** DOSE3.1. Network blocked by large network	**DOSI1. Fake platform instance sending abnormal parameters to the system** DOSI1.1. Network blocked by large network packages DOSI1.2. Network blocked by concurrent operations DOSI1.3. Logging

	packages DOSE3.2. Network blocked by concurrent operations	mechanisms stopped working
E=Elevation of Privilege *(the user (or a software) is technically able (allowed) to perform something that they are not supposed (authorized) to do)*	**EOPE1. Client security vulnerability** EOPE1.1. Weak validation mechanisms EOPE1.2. Weak authorization EOPE1.3. Cross-site scripting vulnerabilities **EOPE2. Server security vulnerability** EOPE2.1. Cross-site scripting vulnerabilities	**EOPI1. Fake platform instance injecting a malicious command**

At the end, we compare the results of the STRIDE analysis (possible threats and vulnerabilities) with security requirements captured in Sections 3 and 4. Through such comparison, we check for those situations that have not been previously covered by the security requirements, evaluate newly perceived threats and vulnerabilities, and iteratively perform the security requirements elicitation process and enhance the captured requirements.

We also created a *STRIDE per element* diagram, which analyses the exposure of each of the NIMBLE components to the specific type of threat. In other words, this diagram observes which threats are more prevalent with certain components of the NIMBLE architecture/ system. This is shown in Table 40.

Table 40: STRIDE per element diagram in NIMBLE

NIMBLE Components	S	T	R	I	D	E
FrontEnd Services	x	x		x	x	
OpenAPI	x	x	x	x	x	x
Data Store		x		x	x	
Data Management		x	x	x	x	x
Data Flow	x	x	x	x	x	
Core Services	x	x	x	x		x
Service Discovery	x			x		
Service Registry	x		x		x	x
Cloud Services	x	x	x	x	x	x

7 Conclusion

The process of identifying, specifying, adopting and integrating security and privacy requirements leads to more secure software systems. In NIMBLE, the key security requirements relate to the user's identification, authentication, authorization and access controls management. From the perspective of privacy, the biggest concern of the users is about privacy of business data and transactions, and their possible manipulation via NIMBLE services. Hence, we created the *NIMBLE Privacy Requirements Framework* with the role to observe user privacy, data privacy and business privacy.

The iterative STRIDE-based requirements evaluation enhanced the requirements elicitation process and helped to better observe and categorize possible risks in NIMBLE. For example, we focus more on covering those situations that can cause attacks via *privileged access* and *unauthorized access*, than on *Denial of Service (DoS) attacks*. Still, DoS is on our radar as a potential risk to watch (see Table 41 that our observations on various risks in the context of the NIMBLE platform).
Note: Table 41 is based on the security questionnaire for the collaboration on the FoF (Factories of the Future) projects (FoF-11-2016).

Table 41: Potential risks associated with the NIMBLE platform

Privileged access	10
Unauthorized Access	9
Denial of Service	2
Data Leakage	7
Data Integrity	8
Integration	6
Availability	3
Reliability	11
Resilience	12
(Industrial) Espionage	5
Incident Management	1
Web Application Security	4

The future evolution of use case-centric requirements and platform-centric requirements, especially when the platform reaches more maturity and the massive adoption in various industry sectors, will further the evolution of security and privacy requirements in NIMBLE, too. The traceability of these requirements will be maintained using the online collaborative spreadsheet.

Appendix 1: Mapping between the GDPR Requirements and the Platform-Centric Security and Privacy Requirements in NIMBLE

GDPR Requirements	Security and Privacy Requirements IDs (in NIMBLE)	Security and Privacy Requirements Names (in NIMBLE)
GDPR requirement for implementing privacy procedures for seeking, recording, and managing user's consent	*SEC_DIDQ_05,* *PRIV_PLAT_04*	*Informed consent by Design;* *Informed Consent*
GDPR requirement to document all personal and sensitive personal data that the organization is hold	*SEC_DIDQ_01*	*Data Integrity and Data Quality Policy*
GDPR requirement for verifying if sensitive data is accurate, complete and up-to-date, and for verifying the subject's age	*SEC_DIDQ_02,* *PRIV_PLAT_06*	*Data input validation;* *Prohibiting interaction with children or non-business entities*
GDPR requirement for deletion of personal data and/or personal data modification by the data subject	*SEC_DIDQ_03,* *SEC_DIDQ_03_1,* *SEC_DIDQ_03_2*	*Data and metadata protection*
GDPR requirement for supporting subject's access requests to personal and sensitive data	*SEC_DIDQ_03,* *PRIV_PLAT_03*	*Data and metadata protection;* *Preventing unauthorized access*
GDPR requirement for reviewing existing privacy notices and keeping them up-to-date	*SEC_DIDQ_04*	*Notification of data integrity violations*
GDPR requirement for detecting, reporting and investigating personal data breaches	*SEC_DIDQ_04,* *SEC_PLAT_01,* *PRIV_PLAT_01*	*Notification of data integrity violations;* *Security Monitoring;* *Data privacy*
GDPR requirement for assessing security and privacy impact	*SEC_PLAT_02*	*Security Assessment*
GDPR requirement to incorporate the guidance from the Article 29 Working Party	*SEC_PLAT_04* *PRIV_PLAT_02*	*Security Planning;* *Platform code and services privacy access*

8 References

[AMIN93] M. Amini (1993). Formal Methods for Information Security. Online available: http://ce.sharif.edu/courses/92-93/2/ce873-1/resources/root/FMS-Amini-V0_4.pdf

[BOOM17] Boomi, D. (2017), How Windows 10 data collection trades privacy for security. Online: https://www.infoworld.com/article/3146523/microsoft-windows/how-windows-10-data-collection-trades-privacy-for-security.html Last access: October 2017.

[BRAI16] G. Brail, 2016. APIs for Data Security and Privacy: Part One. APIGee. Online available: https://apigee.com/about/blog/digital-business/apis-data-security-and-privacy-part-one-0 Last access: September 2017.

[CAVO12] A. Cavoukian (2012). Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices. Online: http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf Last access: September 2017.

[CHAN17] P. Chandramohan, 2017. Importance of Data Security in Master Data Management. Informatica blog. Online available: http://infa.media/2xxfnZM

[D2.1_17] B. Mandler (2017). D2.1 "Platform Architecture Specification and Component Design". Online available: https://www.nimble-project.org/deliverables/

[EUR-LEX14] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (23 July 2014). Online available: http://eur-lex.europa.eu/eli/reg/2014/910/oj

[FRIE15] I. Frese, J. Heuer, N. Kong, 2015. Challenges from the Identities of Things. Introduction of the Identities of Things Discussion Group within Kantara Initiative. Security and Privacy in Internet of Things (IoTs): Models, Algorithms and Implementations. Ed. Fei Hu. CRC Press, 2015.

[GDPR95] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Online available: https://www.cdt.org/files/privacy/eudirective/EU_Directive_.html Last access: October 2017

[GOLO02] L. Gordon and M. Loeb: "The Economics of Information Security Investment". ACM Transactions on Information and System Security. 5(4):438–457 (2002).

[GÜTD11] S. Gürses, C. Tronsoco, C. Diaz (2011). Engineering Privacy by Design. COSIC 2011. Online available from: https://www.esat.kuleuven.be/cosic/publications/article-2589.pdf Last access: September 2017.

[HU13] Hu, Vincent, et al. "Guide to Attribute Based Access Control (ABAC) Definition and Considerations." NIST Special Publication 800-162 DRAFT (2013)

[IBM17] Trust Me: Digital Identity on Blockchain. ExpertInsights@IBV. 2017. Online available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03823USEN& Last access: September 2017

[ICO17a] Overview of the General Data Protection Regulation (GDPR). Online available: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ Last access: October 2017

[ICO17b] Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now. V2.0 20170525. Online available: https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf Last access: October 2017

[ISO/IEC09] ISO/IEC 27000:2009 (E). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC. (2009)

[LYNC17] Brendon Lynch (2017). Get GDPR Compliant with the Microsoft Cloud. Online: https://blogs.microsoft.com/on-the-issues/2017/02/15/get-gdpr-compliant-with-the-microsoft-cloud/#hv52B68OZTwhUj2c.99- Last access: October 2017

[MALN12] A. Martin, J. Lyle, C. Namilkuo (2012). Provenance as a Security Control. In Proceedings of the 4th USENIX Conference on Theory and Practice of Provenance, USA. Online available: http://dl.acm.org/citation.cfm?id=2342878

[MICR17] Microsoft whitepaper (2017). Beginning your General Data Protection Regulations (GDPR) Journey for Windows 10. Online available: https://docs.microsoft.com/en-us/windows/configuration/gdpr-win10-whitepaper#windows-10-security-and-privacy Last access: October 2017.

[MODA93] M. Modarres (1993). What every enginer should know about reliability and risk analysis. Marcel Dekker Inc.

[NIST-CC12] L. Badger, T. Grance, R. Patt-Corner, J. Voas (2012). Cloud Computing Synopsis and Recommendations. Online available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf Last access: October 2017.

[NIST-SP15] NIST Special Publication (SP) 800-53 "Security and Privacy Controls For Federal Information Systems and Organizations". (Includes updates as of 01-22-2015) Online available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf Last access: October 2017.

[NIST800-27] NIST 800-27. G. Stoneburner, C. Hayden, A. Feringa. Engineering Principles for Information Technology Security (A Baseline for Achieving Security). Online available: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

[OECD80] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). Online available: http://bit.ly/2xfYFv3 Last access: September 2017

[PARI14] M.N. Parikshit, 2014. Identity Management Framework for Internet of Things. PhD dissertation. Aalborg Universitet. Online available: http://vbn.aau.dk/files/188530864/Thesis_Parikship_Mahalle.pdf Last access: March 2017.

[PRIV-GUID08] Privacy Guidelines for Developing Software Products and Services (2008). Version 3.1. Online available: http://splus.tjscott.net/3.sw.dev/ms.privacy.guidelines.pdf Last access: October 2017

[SAGI09] A. Sarma & J. Girão, (2009). "Identities in the Future Internet of Things," Wireless Personal Comm.

[SAUE17] Rich Sauer (2017). Earning your trust with contractual commitments to the General Data Protection Regulation. Online available: https://blogs.microsoft.com/on-the-issues/2017/04/17/earning-trust-contractual-commitments-general-data-protection-regulation/#6QbqoGWXCLavGM63.99 Last access: October 2017

[SHOS14] A. Shostack (2014). Threat Modeling. Designing for Security. John Wiley & Sons, Inc.

[SUBS11] S. Sultana, E. Bertino, M. Shehab (2011). A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks. In Distributed Computing Systems Workshops (ICDCSW) 2011, pp. 332 –338.

[WARR17] Warren, T. (2017), Microsoft finally reveals what data Windows 10 really collects. Online available from: https://www.theverge.com/2017/4/5/15188636/microsoft-windows-10-data-collection-documents-privacy-concerns Last access: October 2017.

[WPF08] World Privacy Forum (2008). A Brief Introduction to Fair Information Practices. Online available: http://bit.ly/2xmslsb Last access: September 2017.