



## DIGITAL MANUFACTURING PLATFORMS FOR CONNECTED SMART FACTORIES

### D3.10 QU4LITY SPT FRAMEWORK (final version)

Deliverable Id:	<b>D3.10</b>
Deliverable Name:	<b>QU4LITY SPT Framework (final version)</b>
Status:	<b>Work in Progress</b>
Dissemination Level:	<b>PU</b>
Due date of deliverable:	<b>31/03/2021</b>
Actual submission date:	<b>28/09/2021</b>
Work Package:	<b>WP3</b>
Organization name of lead contractor for this deliverable:	<b>ATOS</b>
Author(s):	<b>Jose Francisco Ruiz (ATOS)</b>
Partner(s) contributing:	<b>Xabier De Carlos (IKER) Jan Jürjens (FRA) Sebastian Scholze (ATB) Feryal Fulya Horozal (ATB) Cristocal Arellano (IKER) Guillermo Yuste (ATOS)</b>


**Abstract:** This deliverable presents the final version of the QU4LITY SPT Framework, which aims to provide different cybersecurity services to the manufacturing domain. In this document we present the changes to the architecture from the initial version and description of its cybersecurity solutions.



<b>QU4LITY</b>	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

## Contents

HISTORY .....	4
List of figures .....	5
List of Abbreviations .....	7
1. Executive Summary .....	8
2. Introduction.....	9
2.1 Scope and objectives of the updated SPT Framework .....	9
2.2 Methodology and workplan.....	9
2.3 Document structure .....	10
2.4 Update on state of the art .....	11
• 2.4.1 Authentication, Identity and Access Control.....	11
• 2.4.2 Cybersecurity monitoring .....	11
• 2.4.3 Data protection.....	12
• 2.4.4 Cybersecurity modeling .....	13
3. Updated SPT Framework Architecture .....	15
3.1 Description and Functionalities.....	15
3.2 Roles .....	18
3.3 Future enhancements.....	19
4. SPT Framework Solutions .....	20
4.1 Authentication & Authorization Solution .....	20
• 4.1.1 Description and Functionality.....	20
• 4.1.2 Usage and Results.....	28
• 4.1.3 Future Work .....	35
4.2 Data Anonymization Solution.....	35
• 4.2.1 Description and Functionality.....	35
• 4.2.2 Usage and Results.....	36
4.3 Monitoring Solution .....	38
• 4.3.1 Description and Functionality.....	38
• 4.3.2 Usage and Results.....	39
• 4.3.3 Future Work .....	41
4.4 Cybersecurity Modeling for Manufacturing Solution.....	41
• 4.4.1 Description and Functionality.....	41
• 4.4.2 Usage and Results.....	43
5. Conclusions .....	56

	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

Partners .....57

<b>QU4LITY</b>	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

## HISTORY

Version	Date	Modification reason	Modified by
0.1	01/03/2021	Initial version	Jose Francisco Ruiz (ATOS)
0.2	26/03/2021	Added auth solution	Xabier De Carlos (IKER)
0.3	28/03/2021	Added data protection solution	Feryal Fulya Horozal (ATB)
0.4	20/04/2021	Added monitoring solution	Jose Francisco Ruiz (ATOS)
0.5	22/04/2021	Added security-by-design solution	Jan Juerjens (FRA)
0.6	20/05/2021	Added SPT framework	Jose Francisco Ruiz (ATOS)
0.7	10/06/2021	Refined version of the deliverable	Jose Francisco Ruiz (ATOS)
0.8	20/07/2021	Updated design and feedback on tools	Jose Francisco Ruiz (ATOS)
0.9	20/09/2021	Added conclusions and reviewed document	Jose Francisco Ruiz (ATOS)
0.10	27/09/2021	Review	Irune Mato (SQS/INNO)
1.0	28/09/2021	Added modifications from reviewers	Jose Francisco Ruiz (ATOS)

<b>QU4LITY</b>	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

## List of figures

Figure 1: SPT enhancement methodology .....	10
Figure 2: QU4LITY Reference Architecture .....	15
Figure 3: SPT Reference Architecture .....	17
Figure 4: SPT roles .....	18
Figure 5: Profiling a user based on three dimensions: Who, what, where .....	22
Figure 6: Fingerprint evolution over time .....	23
Figure 7: Module composition.....	24
Figure 8: IK-SEC context-based module data model diagram .....	25
Figure 9: Registering a new device and session sequence diagram.....	26
Figure 10: Handling login with existent device sequence diagram .....	27
Figure 11: Unzipped Keycloak folder .....	28
Figure 12: Keycloak home page .....	29
Figure 13: Registering first admin user for Wildfly management .....	30
Figure 14: Keycloak Server Deployments Page .....	31
Figure 15: Deployment button.....	31
Figure 16: Module deployment process.....	32
Figure 17: Module correctly deployed .....	32
Figure 18: Adding an Event Listener in Keycloak.....	33
Figure 19: Configuring Keycloak themes.....	34
Figure 20: Adding a new authentication flow .....	34
Figure 21: Configuring the CBA flow.....	35
Figure 22: Binding the CBA flow .....	35
Figure 23: Sample Dataset in the ARX tool before data-anonymization.....	37
Figure 24: Monitoring Sensors schema .....	38
Figure 25: Example of an event log.....	39
Figure 26: General view of the SIEM .....	40
Figure 27: List of all events.....	40
Figure 28: List of all alarms. ....	41
Figure 29: Overview of the Cyber Security and Risk Analysis Approach and Workflow .....	42
Figure 30: International Data Spaces Structural Overview in a UML Class Diagram .....	45
Figure 31: Structural Overview of the Internal Data Exchange in a UML Class Diagram .....	46
Figure 32: Data Collection subprocess in a BPMN Diagram .....	47
Figure 33: Data Acquisition System and Data Management System of the Data Provider in a BPMN Diagram .....	47
Figure 34: Data Provisioning Process from the Internal Connector to the External Connector in a BPMN Diagram.....	48
Figure 35: High-level Overview of Invoke Data Exchange Process in a BPMN Diagram (Otto et al., 2019) .....	50
Figure 36: Data Exchange Process in a BPMN Diagram .....	50
Figure 37: Find Data Provider Subprocess in a BPMN Diagram.....	51
Figure 38: Query Data subprocess in a BPMN Diagram .....	52
Figure 39: Transaction Logging Subprocess in a BPMN Diagram .....	53



	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

Figure 39: QU4LITY Infrastructure in a class diagram with <<secure dependency>>  
UMLsec check .....54

<b>QU4LITY</b>	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

## List of Abbreviations

ABAC	Attribute-based access control
APP	Application
CBAC	Context-based access control
CBA	Context-based Authentication
EPL	Event Process Language
HIDS	Host Intruder Detection System
IAM	Identity Access Management
ICS	Industrial Control System
IDS	Intruder Detection System
IoT	Internet of Things
IT	Information Technology
MFA	Multi Factor Authentication
OT	Operational Technology
OTP	One Time Password
PAP	Policy Administration Point
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIP	Policy Information Point
RA	Reference Architecture
RBAC	Role-based access control
RPT	Requesting Party Token
SFA	Single Factor Authentication
SIEM	Security Incident and Event Management
SPI	Service Provider Interface
SPT	Security Privacy and Trust
UBAC	User-based access control
UMA	User-Managed Access
ZDM	Zero Defect Manufacturing

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

## 1. Executive Summary

This deliverable describes the current and final work of the SPT (cybersecurity, Privacy and Trust) QU4LITY Framework. Using as basis the work presented in D3.9 we continued working in refining and updating the different components of the SPT Framework and the architecture of the cybersecurity solution for industry. The work presented here was done specially in Task 3.5. There, each partner focused into one specific tool in order to provide a clear and unique functionality for the cybersecurity, trust and privacy approach of the project.

The SPT platform allows, from an architectural point of view, to integrate and use the result of all the solutions developed so far in QU4LITY but also to extend it with new and additional solutions. This way, because cybersecurity is a topic that is continuously evolving and changing, we had to design the SPT in a way that could be extended with solutions that can cover either new problems or technologies. Due to the special nature of the industry sector, as it evolves to continue being more digital and use actual solutions to improve its way of work, it has to be able to use and integrate solutions that can provide assurance for the companies and users.

The SPT has been planned to be used in the way of using specific tools in use cases in order to demonstrate their usability and integration. This is a work that was delayed due to the special situation of the COVID and will be reported in the work done with the use cases.

The solutions covered so far in the SPT are cybersecurity monitoring solutions, authentication, data protection and cybersecurity by design. Following we describe briefly each of these areas and why are they important for the industry sector. Also, we explain the updates and refined version of the SPT architecture, which would be used for a joint platform where the different cybersecurity tools would provide their information so end-users could have a joint and central solution for cybersecurity activities. Of course, and due to the nature of some of these solutions, not all of them could be integrated at all levels but we aim to support the maximum number of tools as much as possible. Example of this is the monitoring solution and the cybersecurity modelling tool. Both are important but cover, and provide, different output and results, which although are very important at different levels (design and run-time) is difficult for integrating into a common dashboard that provides a unified solution. Nonetheless, all the SPT solutions are covered under the same framework and we provided descriptions and documentation of each of them.



QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

## 2. Introduction

The Security, Privacy and Trust (SPT) Framework has continued evolving in parallel with the cybersecurity technologies and results of the QU4LITY project. This way, since the first iteration of the framework we worked in extending the capabilities of the tools and the SPT Framework from the design point of view, in order to have a unified platform where different cybersecurity tools/solutions could be integrated and used in the scope of Industry 4.0. This means the tools are specific for the constraints, requirements, usability and needs of the different industry scenarios, using as basis the ones of the QU4LITY project.

Therefore, this deliverable presents, on the one hand, the work of the SPT Framework from a design and usability point of view and, on the other hand, the development, updates, usage and functionality of the tools developed in the project.

### 2.1 Scope and objectives of the updated SPT Framework

The SPT Framework went through a couple of iterations in order to define better different aspects that were found in need of a more maturity. These aspects were the communication of the tools and user interface (so how they present the information to the user) together with deployment. Those aspects were very important because the integration of cybersecurity in the industry systems had to be as natural as possible and, on the other hand, the information had to be provided in a way that could be as useful as possible for the users. Finally, we created subcomponents for the different areas of application of cybersecurity because it is an area that is continuously evolving and, therefore, we need a way for having new tools that could provide support for new technologies or attacks that were not taken into account when designing the system.

### 2.2 Methodology and workplan

The methodology we followed in the SPT was divided into two different aspects: the design and work of the SPT and the refinement and development of the SPT solutions. For each one we had to follow different approaches given the specific objective of each of them and being at different layers of the life cycle.

Regarding the SPT, we performed two iterations in order to refine the functionality and services provided. The first iteration focused on the classification of the different tools in the life cycle and how the information could be provided. Here we focused mostly in the design of the tools and analysis of how they could be used in industry systems, together with the benefits and outputs they would provide.

On the second iteration we focused in refining the existing tools and their usability. This way, we described more in-depth use case and sequence diagrams for how the tools would work for the different roles that will have access to the platform.

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

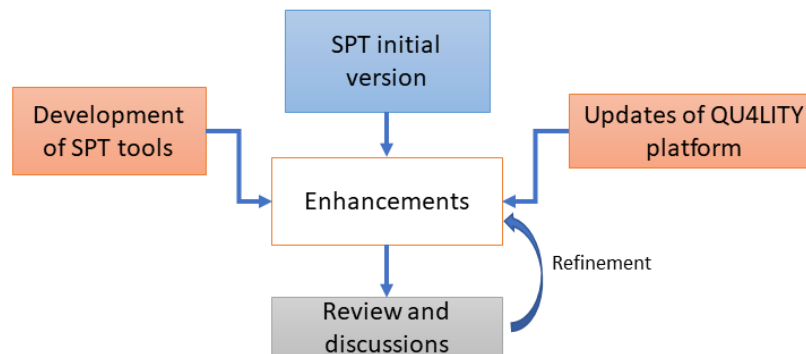


Figure 1: SPT enhancement methodology

Figure 1 shows the process we followed for this second version of the SPT and the sources we used. Additionally with the initial version of the SPT we used the information of the work done in the extensions of the tools of the SPT (which are described in the following sections) and the updates of the QU4LITY platform. More information about this integration can be found in D3.11.

Of course, for each iteration we had an analysis and review of the new functionalities by the partners of the task in order to have a good review of the changes. This was necessary to be in-line for the feasibility of the system, bearing in mind the specifics of the cybersecurity solutions and how they work.

## 2.3 Document structure

This deliverable is composed of the different sections:

- Section 1: here we provide the executive summary of the work presented in the whole deliverable together with the motivation and goals to be achieved by the SPT Framework
- Section 2: this section describes the composition of the document, the scope and objectives of the SPT Framework, the methodology followed for the development of the different components and architecture and finally an update on the state of the art of cybersecurity solutions for industry. This is an important aspect in order to align the scope of the SPT, the work done and what exist right now in the market.
- Section 3: this section describes the updates done in the SPT, motivation and needs for the changes, roles and possible extensions. This goes in line with the updates done in the different tools presented in D3.9.
- Section 4: here we describe the different cybersecurity, privacy and trust solutions developed in the project using as basis the work presented in D3.9, which focused more on the design aspect. We provide a more in-depth description of the tools, documentation, definition of the different functionalities offered and future work that we plan to continue in order to provide better performance and results in the industry area.

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

- Section 5: this section presents the conclusions and general future work of the SPT

## 2.4 Update on state of the art

As abovementioned cybersecurity is a topic that continuous evolving as new technologies, methods and products are developed. Therefore, we thought it would be very useful to provide an update of the state of the art of the different cybersecurity areas we are working with in the SPT. Thanks to this work we were able to work better in the advancements and innovations of the solutions.

### • 2.4.1 Authentication, Identity and Access Control

Nowadays, we are engaged in what is called “The 4.0 industry”. The changes that are shaping the digital world echo in all sectors, where industry makes no exception to this rule. The consequences do not necessarily imply entail negative aspects, given that most companies are now able to deal with increased amounts of data and, thus, enhance and empower their operations. However, while the industry 4.0 requires for more and more transactions to be digitally accomplished, this means that people taking part in them must be digitally identified and authorized.

The very first step in any transaction involves the identification of the individual. Companies need to take identification quite seriously, specially because digital identity is the basis for trust, security, and reliability amongst industries: it is essential for the accomplishment of every transaction.

Authentication becomes important if valuable assets are at stake. While it has been traditionally performed by means of the user/password combo, these is no longer enough in terms of satisfying security standards and now, 2FA is gaining momentum. Unfortunately, things such as biometry, tokens or even smart cards implantation varies significantly amongst industries. Several sectors, including government, healthcare or finance have already incorporated 2FA, but the path is far from being fully traveled, in terms of security. The specific nuisances of every field sometimes require a careful approach, to effective balance between security and usability. Examples of 2FA in the industry include the use of ATMs (require the card and the PIN) or the CAC (Common Access Card) that US Army employs. Other scenarios consider the Adaptative Multi-Factor Authentication or AMFA, where companies must decide which security factors can assist on protecting assets and systems.

At the same time, the Industry 4.0 is facing the risks of the IoT side, that is, a Pleiad of new, smart devices expected to deliver in various fields, where authentication may be an issue. Besides, the protection of the data sent and received by these devices is an extra risk that must be considered nowadays.

### • 2.4.2 Cybersecurity monitoring

Defense in depth (DID) is an essential part of any security architecture. There is a great deal of components that helps shaping security in various layers, while components such as Intrusion Detection Systems (IDS) and Intrusion Prevention

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

Systems (IPS) play a big role. At the same time, various critical systems such as Industrial Control Systems (ICS) and SCADA require higher level of protection, due to its sensitive nature. However, it may be paradoxical that, for some time, these critical components relied on unprotected, clear-text communications and made use of protocols lacking a minimum-security level.

Both IDS and IPS are common in today's cyberworld and are subject to be host-based or network-based. However, they offer different capabilities that can enhance security from distinct perspectives: on the one hand, IDS focus on detection, while IPS are more prevention oriented.

As part of its nature, ICS tend to slowly adopt new security features. The reason is simple: it is not always immediate to integrate new security devices with advanced features into systems that regulate, manage and control systems. Besides, false positives could possibly hinder the implementation of such devices in an industrial environment.

Fast development of security has shaped cloud IPS/IDS, solutions that are step-by-step being embraced by organizations in various sectors including government agencies, healthcare, financial, retail or even the very cloud security providers.


Not only IDS and IPS should be considered but also security must include a variety of components, devices, and systems to further develop the DID concept. Honeypots and honeynets are also capable of delivering security information through the collection and gathering on attackers' actions and methods. Honeypots are designed to serve as a trap to delude attackers. Given that ICS systems are continuously and increasingly being attacked<sup>1</sup>, currently honeypots are being considered to protect them and detect attack vectors. Due to the increased sophistication of some APTs (Advanced Persistent Threats), the information provided by honeypots could tip the balance towards an effective protection

### • 2.4.3 Data protection

Every company and business today demands and processes a great deal of information. With the rising of the Big Data, volumes of information exchanged, stored, and employed have increased dramatically. However, until recently, data was not subject of adequate levels of protection. The safeguard of the information comes with the objective of guaranteeing its confidentiality, integrity, and availability in its different states, including while in transit and at rest. In addition, the 4.0 industry is increasingly adopting a more decentralized approach, with more and more industrial systems becoming autonomous, something that impacts the way data should be protected.

In addition, the protection of data must ensure that sensitive information is protected when handled. To achieve this, the anonymization is one, if not the best, option. The advantages of anonymization include the possibility of sharing the data with third

<sup>1</sup> <https://www.vice.com/en/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report>

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU


parties without breaking the rules. Various processes can be applied to data, including:

- **Suppression:** the elimination of one part of the dataset can be effective to anonymize data, especially when the erased information is not a key part or whether a specific attribute can be considered dispensable. Some label suppression as a hard technique since data erased cannot be recovered from the original dataset. It could have different approaches: attribute suppression, record suppression...
- **Pseudonymization:** this refers to the process of replacing a sensitive and recognizable identifier with a less evident or non-discernible one. One example would be to change a personal, identifiable name by other such as "John Doe".
- **Generalization,** as the process of broadening information with the aim of hampering identification of certain aspects of data while lowering its accuracy. It requires some degree of expertise, given that identifiable aspects of information should be blurred while guaranteeing that accuracy of the dataset has not been affected by this.
- **Use of artificial, synthetic data:** this scenario implies the adoption of data produced by computers. The disadvantage is that, although this artificially engineered information allows for testing, it is not related to the original, sensitive information, that may be necessary in some cases. The key for a proper synthetic production of a dataset involves the use of patterns.
- **Shuffling:** this technique is known as "data swapping" and requires the permutation of values with the purpose of blurring the original location of sensitive data. It must be performed with special care, given that not all fields fit, once shuffled, into a destination category or field. For example, dates may not fit into certain fields.
- **Masking:** the process is quite straightforward compared to other anonymization techniques. Special characters including asterisk (\*) or similar could be used to replace figures or letters and, thus, contributing to make any attempt of reverse engineering almost impossible.
- **Perturbation:** the definition of noise in data refers to information that provides no value, that is, meaningless data. Including noise helps anonymizing but, at the same time, too much noise could potentially spoil the original dataset because of the disturbance provoked on it. So, it must be performed with a certain degree of expertise.

#### • 2.4.4 Cybersecurity modeling

Starting from the very general concept of modeling, the process helps illustrating features of both a system and its environment. From a cybersecurity perspective, modeling should include different aspects that take part in the whole picture of security, such as:


- What constraints affect the system?
- The possible limitations inherent to the system and/or industry.

	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

- The possibility of simplifying and reducing complexity in the process of addressing security.
- Assumptions affecting the system that could be made. For example, the number of states (limited or finite or not) a system could be in and how to shift from one to another.

Generally, the process of integrating security in the industrial sector could significantly differ in terms of complexity amongst the various sectors considered. For example, a dynamic system could potentially entail bigger risks, given its nature: consequences of actions are not seen in the short term, while real-time ones perform low or negligible processing of data, and are much-more bolstered by events. Therefore, if modeling security, the consideration of future effects should be taken into account. This is easier said than done. To make things a bit harder, the point of view (or simply the “view”) shapes the modeling process in different ways. For example, internal views of the system are more influenced by mechanics and provide more data about how the system performs. On the contrary, an external perspective should involve not only the system but also external factors. Therefore, depending on how the view is handled, the modeling may fluctuate accordingly. In addition, some authors consider a third view called the behavioral view, that impinges on how objects react *after* an event has taken place.

Obviously, all those factors play a role in the process of cybersecurity modeling. Sometimes the analyst must rely on previous experiences to reach a valid conclusion that can really help hardening and making the system more resilient.

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

### 3. Updated SPT Framework Architecture

This section describes the updates done in the SPT Framework architecture using as basis the initial version presented in the previous deliverable. The updates focused mostly on the design and functionality of the system, which went through a couple of iterations. The work done in the tools was parallel to the architecture and therefore contributed to the changes on how they would communicate with it.

Additionally, we worked with the components of the QU4LITY platform in order to identify how we would communicate and how the information obtained from the different SPT tools could be of use to the end-users of the systems being protected. Information about this was included in D3.11 and D3.14.

#### 3.1 Description and Functionalities

The objective of the SPT is to provide cybersecurity, privacy and trust functionalities to the QU4LITY platform and the different industry scenarios using it. This way, the SPT provides, on the one hand, a framework for integrating the information coming from the systems and, on the other hand, a set of tools that can be deployed or used in the target system in order to provide a cybersecurity characteristic or functionality. We can see the goal of the SPT in the QU4LITY reference architecture shown in Figure 2 together with the communication points.

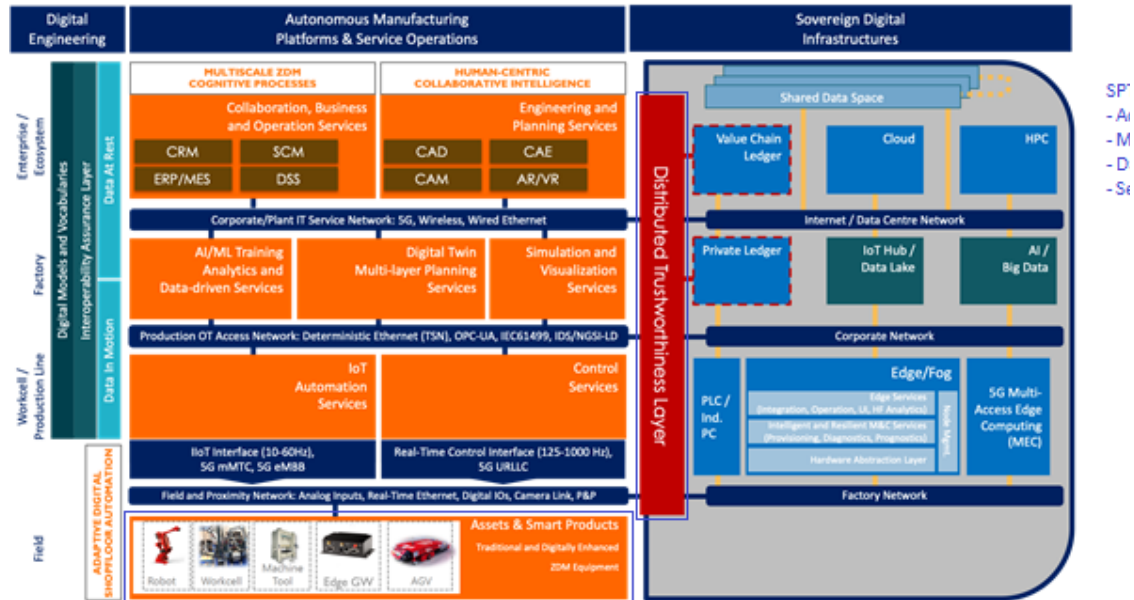


Figure 2: QU4LITY Reference Architecture

As we can see in the previous figure, the SPT provides functionality in the QU4LITY reference architecture in both the scenarios ("Assets & Smart Products") and the communication component between the systems and digital infrastructures ("Sovereign Digital Infrastructures"). The way it provides its services are in the following way, according to the functionality of the cybersecurity solutions:




<b>QU4LITY</b>	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

- Access control: the cybersecurity solution of access control integrated in the SPT allows for users to define and specify how and who can access the target system, specific resources, etc., being able to create specialized roles for accessing unique functionalities or the whole system. This way, it would be possible to create roles that can access only the needed parts of the system instead of having everyone with full access. Apart from being a good way of protecting the system against external malicious hackers it would also protect against internal attacks or leaking of user/password, as only specific and necessary users/roles would have access to critical aspects of the system.
- Monitoring: the cybersecurity monitoring solution is able to monitor, analyze and inform users about cyber incidents in the network of the systems, being the end-point with the assets or in the digital infrastructure (or both). This way, the monitoring solution could be deployed in the necessary system/network and provide information of cybersecurity status together with recommendations for reacting to cyberattacks. The information can be accessed via the user interface and integrated with the SPT access control solution, so the role management and access to the information is done by only the necessary or specific users/roles of the whole system. This solution requires an integration of an agent in order to compile the information of the system, which has to be deployed according to the specific technology of the system.
- Data protection: this SPT solution is a library/API that provides access to an anonymization functionality which can be used for both storing information or sending over an untrusted network. This can be used both by the end-systems (assets) for sending information or by the digital infrastructures for communication with external systems or storing the information in order to increase its security. The data protection component can be used easily in different scenarios for satisfying different constraints and deployed in any environment.
- Security-by-design: this tool covers the design phase of the SPT for the creation of security and privacy systems. The modeling solution can be used at the designing of the whole system or some parts of it. It includes a library of cybersecurity components in order to integrate them with the normal system so the development/testing phase can be done with security integrated naturally in the system. This way, the library of cybersecurity models can be extended in the future with more elements so it can cover more scenarios and environments as the digital industry domain grows or evolves. This solution can be used both by the end-users for the design of their system or at QU4LITY for providing cybersecurity-oriented design of the target system, in order to enhance it with functionality and components integrated from the beginning in the target system instead of being an addon used when the system is already created and running.

These tools explained previously (and which are described more in-detail in the following sections) are the initial ones we have developed in QU4LITY but, as abovementioned, can be extended in the SPT with more tools as necessary. This is a



	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

required characteristic as the industry 4.0 scenario will continue evolving digitally and the cybersecurity aspect has to continue growing at the same level.

Figure 3 below displays the architecture view of the SPT and the different tools that compose it.

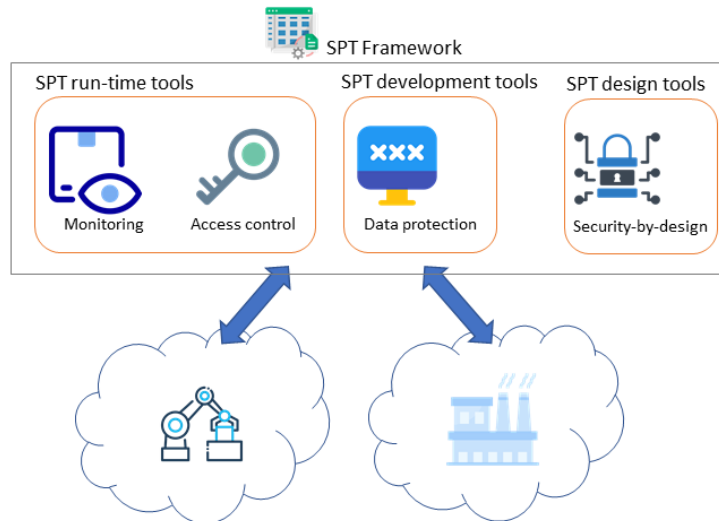


Figure 3: SPT Reference Architecture

As we can see in the figure of above, the SPT is composed of three different components that cover the different life cycle of digital components in order to provide cybersecurity. The objective of each one is:

- SPT run-time tools: solutions that aim to protect, monitor, analyze, react, etc. against cyberattacks for running systems. These solutions could range from a honeypot to a malware protection solution. These solutions can also be integrated between them in order to provide a more complex functionality.
- SPT development tools: these tools provide cybersecurity protection when developing industry systems. These solutions can provided different characteristics such as encryption, sanitization of data, key generation or storing, etc.
- SPT design tools: this component provides tools oriented at design time. These ones can support requirement elicitation, tracking and definition, system design, etc. This way the system would be created as secure by design, being able to integrate cybersecurity functionalities or characteristics in the target system naturally.

The three sub-components provided tools and solutions in their own, although they could be related for supporting specific functionalities. This way, the run-time solutions could monitor variables or scenarios that are defined as critical at the design time. Also, each tool provides its own data storage and user interface, if possible, so they can provide to the users the status of the system together with remediation actions.

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

The tools are deployed and used in the system according to their specification and way of working. This way, there is not a unique way of deploying the tools, configuring and using them but they follow special steps. As an example, the data protection (anonymization) solution is an API that can be downloaded and used when developing software while the monitoring solution requires to deploy the agent in the system to be monitored and a server for the analysis and interface. We provide more information about how these tools work in the following sections.

## 3.2 Roles

Due to the complexity and number of cybersecurity solutions of the SPT we have identified different roles that can take advantage of them. In this way, we can have a better overview of the expertise and needs required for the users that plan to use the tools of SPT. We thought it was necessary to provide an overview about this topic because cybersecurity is a complex area and in order to take full advantage of it, users should have a minimum level of expertise. Figure 4 shows the different roles we have identified.

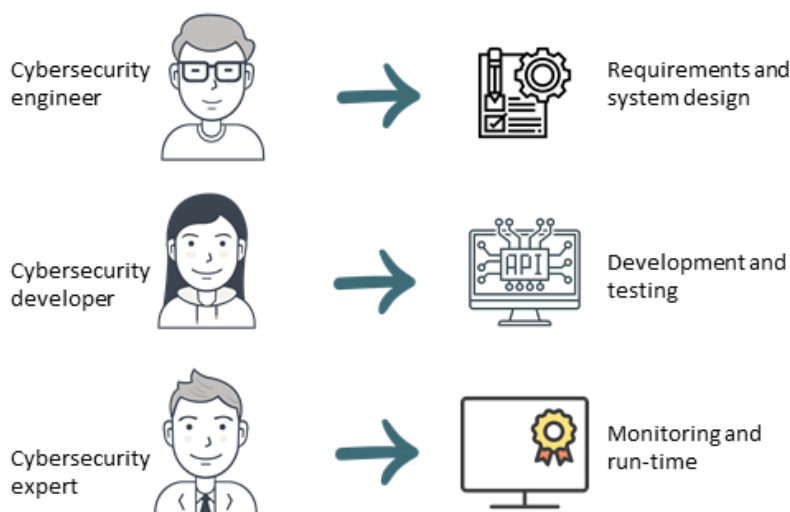


Figure 4: SPT roles

**Cybersecurity engineer:** this role focuses on the identification of cybersecurity requirements and needs in the target system, integration of cybersecurity at design time and understanding the impact of the cybersecurity solutions and components in the whole system. This is very important for identifying how cybersecurity solutions would impact in the system in order to add the necessary extra components or policies. This role would use the tools of the component "SPT design".

**Cybersecurity developer:** this role is the one working on the development of systems and any digital component of industry 4.0. The developer uses cybersecurity solutions for either integrating in the system or taking advantage of the provided functionalities (such as an API) for providing resilience or privacy characteristics to a system. This role works with the tools provided by the component "SPT development".

<b>QU4LITY</b>	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

Cybersecurity expert: this role is the one that can work and analyze the results of the run-time tools. This implies working in the deployment and configuration of the tools and understanding their results. This cybersecurity expert can be either a member of the organization or working in a third-party, providing cybersecurity services and informing the organization about the cybersecurity status of the company or any cyberattack that is detected. This role works with the tools provided by the component "SPT run-time".

### 3.3 Future enhancements

Regarding future enhancements for the SPT we have identified a couple of areas that could benefit from extra work and refinement in the platform. The enhancement focuses on this sub-section in the SPT platform as a whole, as the description of the tools in the following section focuses on their specific aspects.

One of the initial enhancements that could improve the SPT would be to have a joint data repository, analysis and interface for providing correlated data and have a better understanding of what is happening in the target system. This way, the tools of the run-time component would be able to store all their information in a common data repository and this would be used for further and joint analysis, being able to present to the end-user even more useful information of what is happening in their system. This could be extended with an information-specific user interface that would allow users with different roles in the organization to have different views of what is happening in the system. This would help either people with a high-level of knowledge of cybersecurity or managers, who could have a more precise and useful feedback.

Another possible enhancement for the SPT would be to extend the library of cybersecurity design in order to include more specific components for different domains of application. Being the concept of "Industry 4.0" so big, the more refined components for design would help to better fulfill the requirements and have a better understanding of the impact the cybersecurity solutions would have in the whole system. This could be offered in various ways to end-users, so they could extend the libraries with their own or just use the ones of a specific domain/organization for their own systems.

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

## 4. SPT Framework Solutions

As commented in the previous sections the SPT Framework is composed of different solutions that work in specific areas, providing cybersecurity characteristics at different levels of the life cycle of the systems. In this section we describe the solutions we have developed and extended in QU4LITY and which can be used by the use cases for providing cybersecurity services and functionality.

### 4.1 Authentication & Authorization Solution

Authentication is the act or process of confirming that someone (or something) is who they say they are. In this context, the purpose of IK-SEC context-based module is to provide agile, intelligent and secure authentication to the digital resources and services.

The objective of IK-SEC context-based module is to strengthen authentication, thus preventing hackers or intruders from accessing protected corporate resources, but without compromising the user experience. IK-SEC context-based module is integrated as a transparent layer of continuous authentication, based on the context and user behavior through geolocation mechanisms, browser and device detection, which allows real-time analysis of unusual characteristics, thus being able to detect cases of identity theft in time.

IK-SEC context-based module has been developed as an extensible module for the IAM Open-Source Keycloak server.

#### • 4.1.1 Description and Functionality

IK-SEC context-based module has been developed as an extensible module for the IAM Open-Source

Today's authentication systems are widely different. From very basic ones consisting of providing a username and a password, to more complex ones such as facial or fingerprint recognition. All these systems can be categorized depending on the challenge nature into one of the following factors:

- Something you know: These authentication systems rely on the person knowing a secret key to validate their authenticity. For example, knowing the Personal Identification Number Code, a password, or the answer to a question.
- Something you have: Owning something can also validate the identity of a person. For example, providing the right OTP code sent via SMS, or using a YubiKey.
- Something you are: The systems that use this factor of authentication rely on sensors to capture some personal biometric information such as their faces or their fingerprints.

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

- Somewhere you are: This type of authentication focuses on the user's location. It is rarely that a person living in the UK tries to access from China. The most common method to detect the localization of a specific user is by analyzing its IP address.

No authentication factor is perfect, and it may validate the authenticity of an intruder. This kind of scenarios are also called false positive authentications. The opposite scenario (a false negative authentication) can also happen when a real user tries to validate their authenticity but are rejected. For instance, if a person forgets the password.

Basic authentication flows are based on just one type of authentication also known as **single factor authentication** or **SFA**, but as stated before, no authentication system is 100 % accurate.

As seen previously, SFA systems are far from perfect and attackers may be able to bypass the challenge presented even if it takes a long time.

In order to have a robust authentication, a new system is used where users have to provide more than just one factor of authentication. The reason being that each factor diminishes the unlawful users being validated.


This kind of authentication systems are also known as **multiple factor authentication** or **MFA** and are being adopted by many applications today.

Even if MFAs are an improvement from SFA systems from the point of view of the security, it also has some downsides primarily focusing on the user experience. It will take longer to authenticate a user as they are presented with more challenges. It is as important the security aspect of an authentication systems as the user experience, and a balance between them should exist.

To help balancing the user experience and the security aspect of an MFA authentication system, a new method is proposed called **context-based authentication**.

This new method dynamically establishes multiple authentication challenges based on the context where the authentication is taking place.

The key aspect of this authentication system is correctly defining the context. From an abstract point of view, the context is composed by different dimensions. The proposed authentication module focuses on three different dimensions:

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

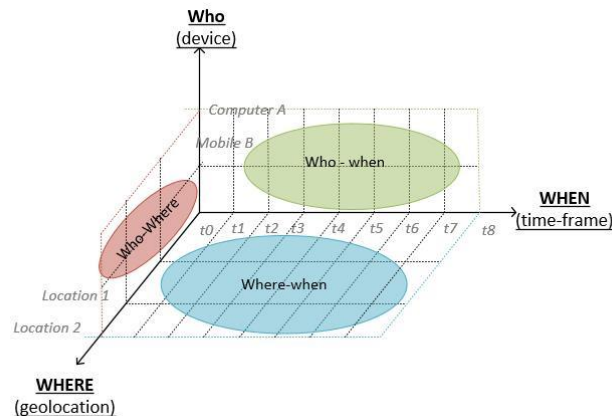


Figure 5: Profiling a user based on three dimensions: Who, what, where

- **WHO dimension:** This dimension registers the device with which the user connects. A user can access a system through different hardware devices: e.g. a computer, and a mobile device.

Currently there are device fingerprinting techniques that allow to identify the device unambiguously. The European Data Protection Committee, in its document "Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting" assumes the definition of RFC 69732 which defines fingerprint as "a set of information elements that identifies a device or an application instance". In other words, the device fingerprint is a set of data extracted from the user's terminal that makes it possible to uniquely identify that terminal.

But device fingerprints evolve over time. For example, the browser is updated to a newer version or a user installs a new plugin on their browser. A context-based authentication system should be able to track the evolution of a user device fingerprint.

Taking into consideration that users tend to use many devices to access the same application, it is also important to register many devices per user, as shown in **Error! Reference source not found..**

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

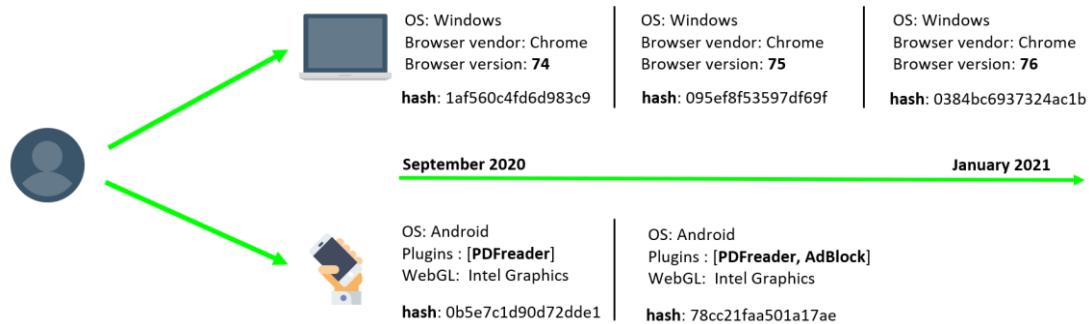


Figure 6: Fingerprint evolution over time

Since people do not usually share their equipment, whether it is a mobile, tablet, laptop or work computer, individualizing the terminal means individualizing the person using it. Thus, associating a device to the user (the WHO). This association is a 1 to N association (a user can have N devices, but a device belongs to only one user).

- **WHERE dimension:** This dimension records from where (geolocation) the user's device (the who) connects. For example, following the previous example, a user may connect from his workstation (location 1) using computer A. Additionally, he could connect from home (location 2) using his cell phone B.
- **WHEN dimension:** This dimension records when the user connects via one of their devices. It collects the patterns of activity/connection to the application. Each time the user logs in to the application, the start of activity is recorded, and when the user logs out, the application or the active session expires, the session is terminated. In this way, activity patterns can be traced. For example, user A accesses the application through mobile B in the time period between t5 and t7.

When the user accesses the system for the first time, the authentication server collects the first variables in the different dimensions: by executing JavaScript libraries it can capture (1) the WHO through the device fingerprint, (2) the WHERE through the public IP of the device connecting to the Internet, and (3) the WHEN through the time of connection and disconnection.

The context-based authentication system starts monitoring the user for a few days without taking any action, only monitoring and collecting the variables related to the different dimensions. After that time, it is considered that it has already delimited the user's context, and from that point on it can start detecting out-of-the-ordinary situations. For example, if the user usually connects only from the geographical points of his home and work, and eventually moves to another city from which he had not previously connected, the system will recognize this situation as anomalous.

<b>QU4LITY</b>	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

Therefore, the authentication server will either deny the user access, or will require an additional authentication factor to verify that it is indeed the legitimate user.

## Architecture

Keycloak runs as a subsystem on top of a WildFly server (also owned by RedHat). The default version of Keycloak is provided with an adapter to deploy the service within WildFly without any additional configuration or setup.

To extend the default version of keycloak with external modules, an interface is provided to implement new functionality called "Service Provider Interface" or SPI. There are many SPIs available depending on the functionality or extension being developed and deployed.

The IK-SEC context-based module uses two main SPIs, which are the authentication SPI and the JPA entity SPI. The session tracking module also uses the JPA entity SPI as well as the Keycloak event listener SPI.

The authentication SPI allows the creation of a new module responsible for authenticating users during login attempts. The JPA entity SPI allows a domain extension, i.e. adding new information to the database corresponding to the fingerprints. Finally, the event listener SPI allows new custom event listeners.

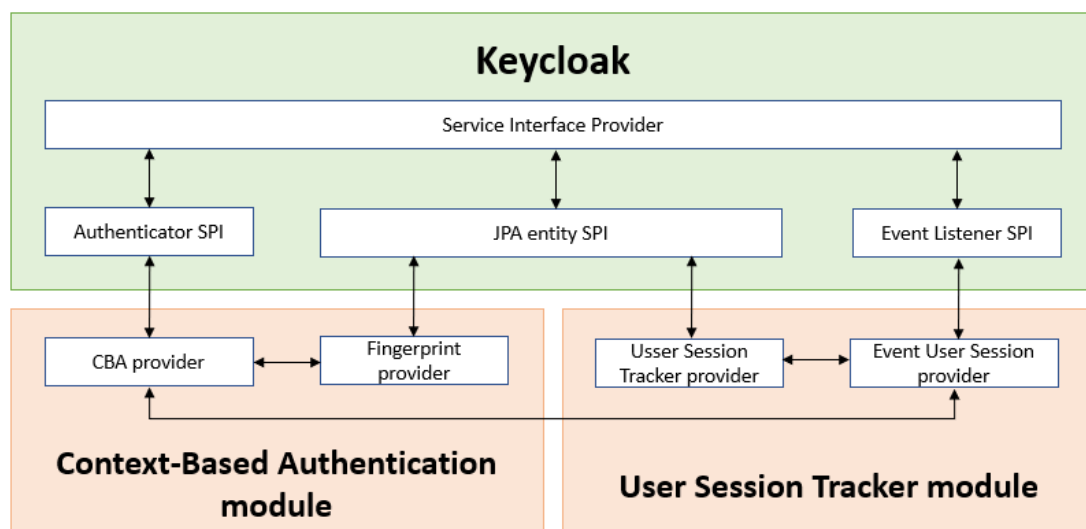



Figure 7: Module composition

The module has two sub-modules that will communicate using the available SPIs. The IK-SEC context-based module provider is responsible for executing and managing the authentication flow when the login is configured to use this module. It handles the logic of authenticating users by comparing their user/password credentials and validating the fingerprint. This module communicates directly with the Keycloak Authenticator SPI.



	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

The second sub-module called FingerprintProvider is responsible for storing new fingerprints and obtaining existing fingerprints by communicating with the Keycloak SPI JPA entity provider.

The second module is composed of two sub-modules, the first one called User Session Tracker provider, is in charge of creating the data model objects that persist in the database, while the second sub-module is in charge of listening for a specific event called while login in. When this event is triggered, the submodule communicates with the data model to create or update existing data.

Finally, some communication is required between the two developed modules. Each time a new login attempt is made, the IK-SEC context-based module provider submodule communicates with the event listener to determine if a user session exists.

### Data model

The module makes use of two defined entities which are: realm entity and user entity. A user always has at least one browser entity. The first one is attached when configuring OTP due to the lack of existing devices registered to that account.

During subsequent successful logins, a new fingerprint entity is registered using an existing browser ID. This is done to track possible feature updates.

If a fingerprint does not match, the user must complete an OTP form. Once submitted and validated, the new fingerprint entity is registered using a new browser entity ID, since it was previously determined that there was no device with that fingerprint.

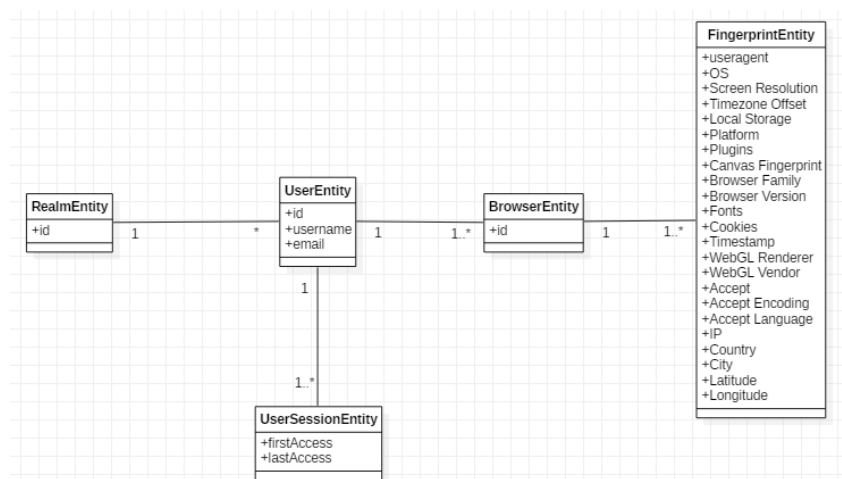



Figure 8: IK-SEC context-based module data model diagram

No fingerprint (having the same ID) can be present in two or more browser entities. This rule also applies to the browser entity. Even if a shared computer is used, the system would create or use different browser entity IDs.

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

Each user will have multiple user sessions (by default up to 10000). Once the system authenticates a user, a new user session is added. If the maximum number of entities is reached, the oldest user session is deleted in favor of the new one.

### Sequence diagram

Register new device (WHO) and user session (WHEN, WHERE)

As a first step, the user will need to provide his or her username and password. In addition, the fingerprint of the device (DIMENSION WHO) will also be calculated and sent when attempting to log in. Once the data is on the server, the authentication process begins.

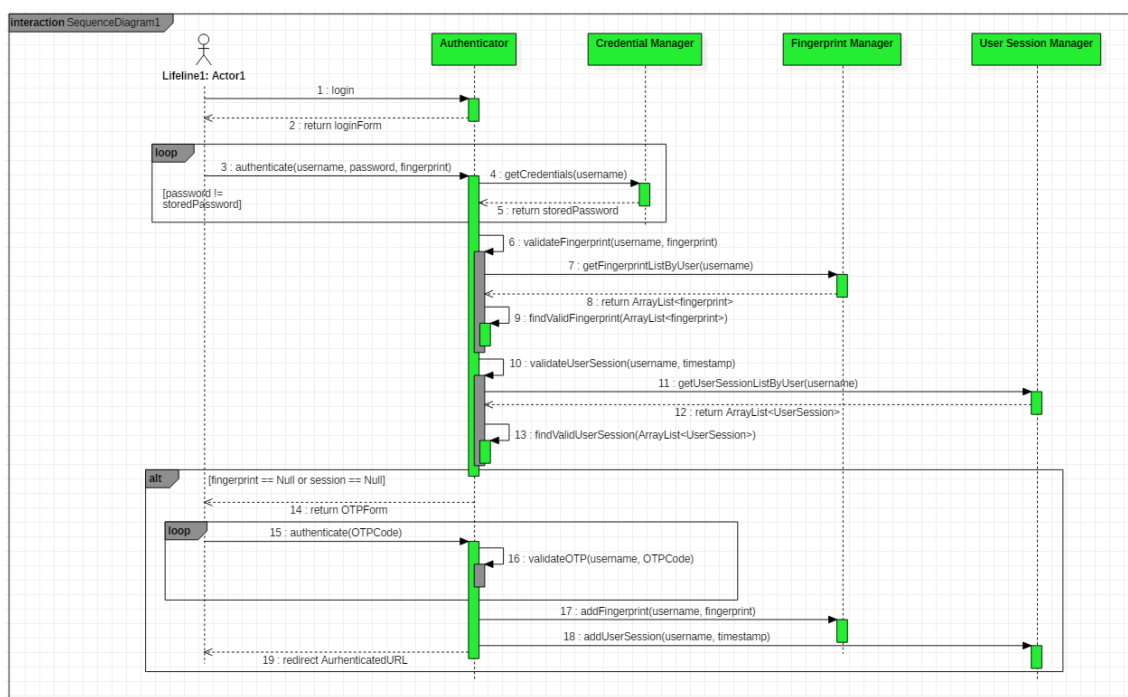



Figure 9: Registering a new device and session sequence diagram

First, it will find if a user exists with the provided username (or email); otherwise, the login form is displayed again showing that the username or password is incorrect (the exact error is not displayed, as it could alert potential attackers leading to an easier brute force attack).

Once the username is verified, the system will check if the provided password exists for that user. If there is no match between the password provided and the one stored in the database, the same error message is displayed. After verifying the username and password, the system will try to find a matching fingerprint stored for that particular user in the database using the rules described in the previous chapter. If there is no match with any stored fingerprint, the system will request a new authentication factor based on OTP.

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

The authentication flow also takes into account the time of day to validate the authenticity of the user (WHEN DIMENSION). The system looks for similar user sessions already stored to determine if the time of day is valid or not. If the system cannot find any matching sessions, the user will be prompted for the OTP form.

If the system cannot authenticate the user, it must provide the user with a valid OTP code. Once the code is validated, the previously collected fingerprint will be added and the new device used to log in will be registered, as well as the new session.

The authentication phase will finish by redirecting the user to the correct application providing the required JWT token.

#### Existing device (WHO) and user session (WHEN, WHERE)

The previous diagram explained the procedure performed by the authentication module to validate the user's identity when a new unregistered device is used to log in. In this section we will explain how the above is modified if there is a fingerprint match.

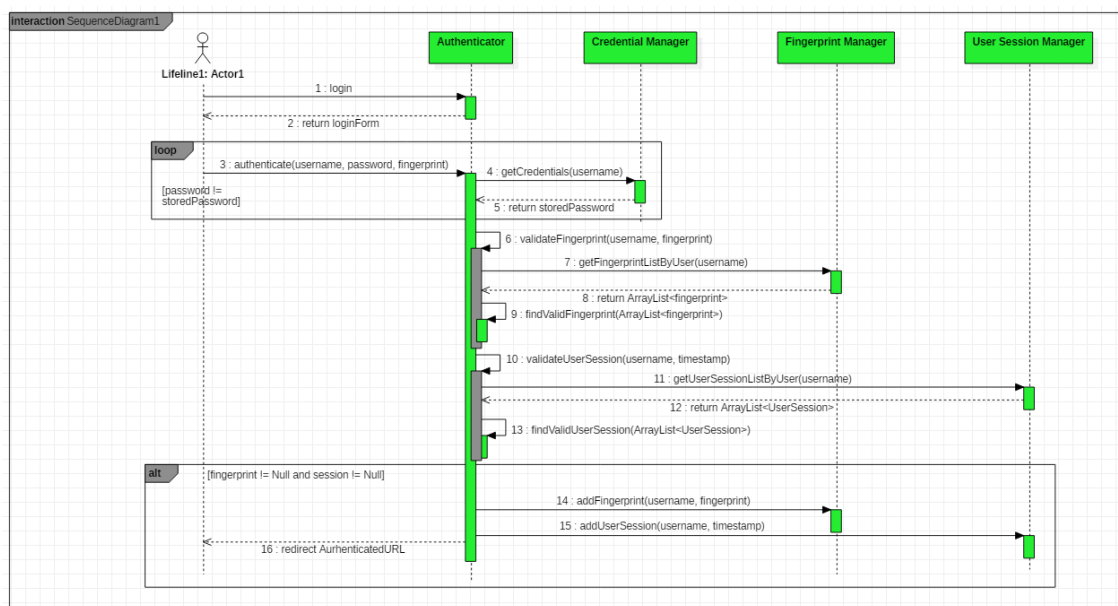



Figure 10: Handling login with existent device sequence diagram

When a fingerprint match is detected, the system will first calculate the geo-velocity of the two fingerprints and, if the value returned is less than the standard, the provided fingerprint is added to the database. The last fingerprint provided from each device is the most important, as it establishes the latest evolution of the fingerprint of the device used.

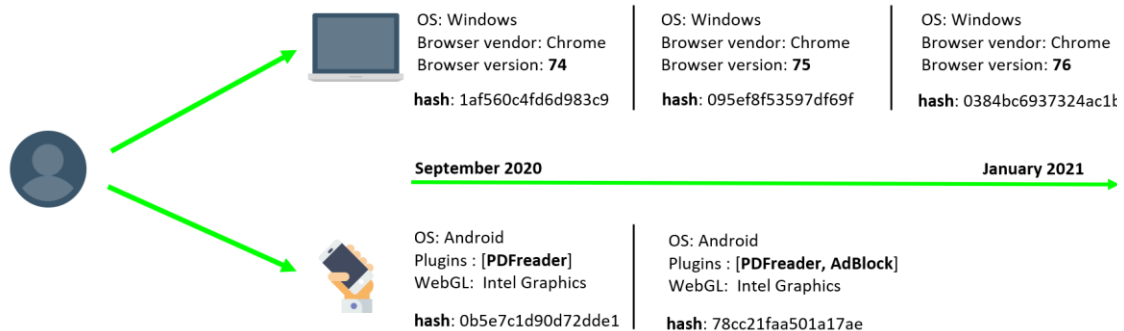
Essentially, we could describe a context-based authentication as a conditional authenticator. If the condition is met, i.e., having a matching fingerprint, the system will only display one authentication factor. If the condition is not met, i.e., no fingerprint and no matching user sessions, the system will display a second factor to ensure that the user attempting to log in is indeed the owner of that account.

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

#### • 4.1.2 Usage and Results

##### *Set up, deployment and configuration*

The developed software, IK-SEC context-based module, runs on a deployed Keycloak instance. The latest supported version of IK-SEC context-based module is Keycloak version 7.0.1.



To install Keycloak on Windows 10 it is necessary to download the following file:  
<https://www.keycloak.org/archive/downloads-7.0.1.html>

Once downloaded, unzip it and access the unzipped folder:

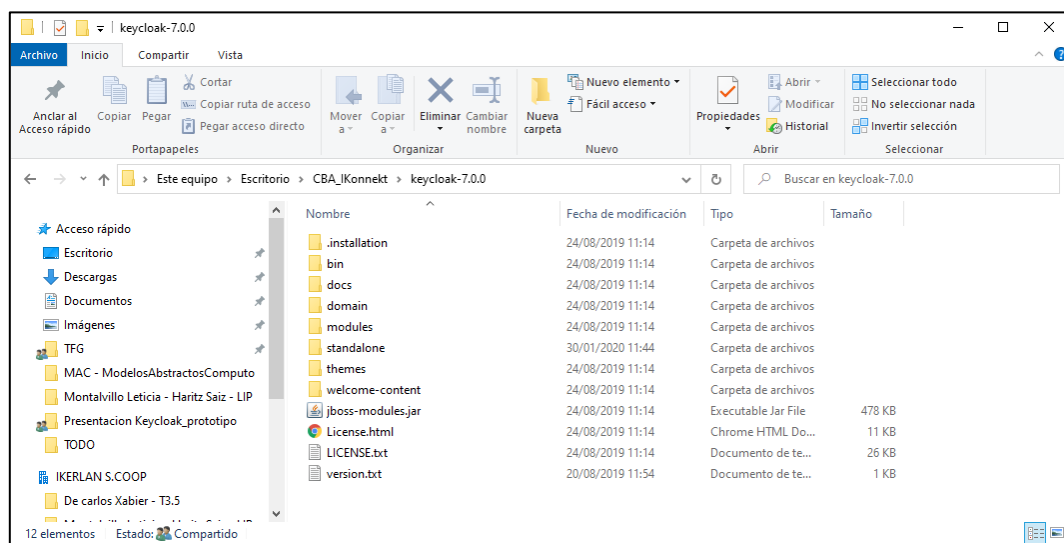



Figure 11: Unzipped Keycloak folder

To start the Keycloak service it is necessary to open a PowerShell terminal and execute the following command:

```
keycloak_dir> .\bin\standalone.bat
```

To access Keycloak navigate to the following address: <http://localhost:8080/auth/>

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

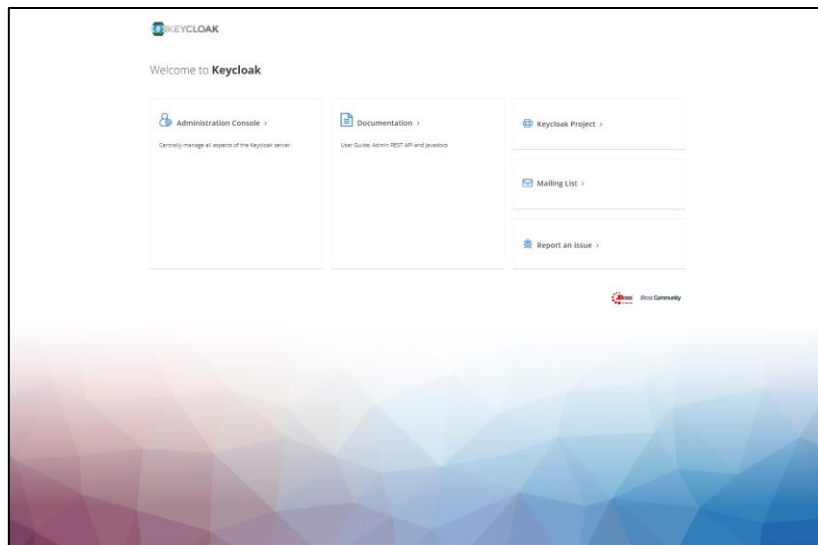


Figure 12: Keycloak home page

In order to be able to manage the Keycloak application it is necessary to register the administrator user. For the purpose of documenting the process to manage the deployment of the module in Keycloak, we will assume that the administrator user is admin.

Next, we go back to the Keycloak folder and reopen another PowerShell terminal on the same folder and execute the following command:

```
keycloak_dir> .\bin\add-user.bat
```

We will be asked different questions and we will respond as follows:

- What type of user do you wish to add? → a
- Username → admin
- User 'admin' already exists and is enabled, would you like to... → a
- Password → (admin's password)
- What groups do you want this user to belong to? (Please enter a comma separated list, or leave blank for none)[PowerUser,BillingAdmin,]: → (leave it blank)
- Is this new user going to be used for one AS process to connect to another AS process? → yes

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

```

-.\Desktop\CBA_Ikonnect\keycloak-8.0.1\bin> .\add-user.bat

What type of user do you wish to add?
a) Management User (mgmt-users.properties)
b) Application User (application-users.properties)
(a): a

Enter the details of the new user to add.
Using realm 'myrealm' as discovered from the existing property files.
Username: admin
User 'admin' already exists and is enabled, would you like to...
a) Update the existing user password and roles
b) Disable the existing user
c) Turn a new username
(a): a


Recommendations are listed below. To modify these restrictions edit the add-user.properties configuration file.
- The password should be different from the username
- The password should not be one of the following restricted values {root, admin, administrator}
- The password should contain at least 8 characters, 1 alphabetic character(s), 1 digit(s), 1 non-alphanumeric symbol(s)
Password:
wFLYDM0898: The password should be different from the username
Are you sure you want to use the password entered yes/no? yes
Re-enter Password:
What groups do you want this user to belong to? (Please enter a comma separated list, or leave blank for none){PowerUser,BillingAdmin,
Updated user 'admin' to file 'C:\Users\hsaiz\IKERLAN\Desktop\CBA_Ikonnect\keycloak-8.0.1\standalone\configuration\mgmt-users.properties'
Updated user 'admin' to file 'C:\Users\hsaiz\IKERLAN\Desktop\CBA_Ikonnect\keycloak-8.0.1\domain\configuration\mgmt-users.properties'
Updated user 'admin' with groups to file 'C:\Users\hsaiz\IKERLAN\Desktop\CBA_Ikonnect\keycloak-8.0.1\standalone\configuration\mgmt-groups.properties'
Updated user 'admin' with groups to file 'C:\Users\hsaiz\IKERLAN\Desktop\CBA_Ikonnect\keycloak-8.0.1\domain\configuration\mgmt-groups.properties'
Is this new user going to be used for one AS process to connect to another AS process?
e.g. host controller connecting to the master or for a Remoting connection for server to server EJB calls.
yes/no? yes
To register the user add the following to the server-identities definition <secret value="YWRtaW4=" />
Presione una tecla para continuar . . .
-.\Desktop\CBA_Ikonnect\keycloak-8.0.1\bin>

```

Figure 13: Registering first admin user for Wildfly management

In order to be able to manage the Keycloak application it is necessary to register the administrator user. For the purpose of documenting the process to manage the deployment of the module in Keycloak, we will assume that the administrator user is admin.

Once we have the Keycloak service active, we proceed to deploy the module developed in the following web: <http://localhost:9990/console/index.html>. Then access the Deployments tab.

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

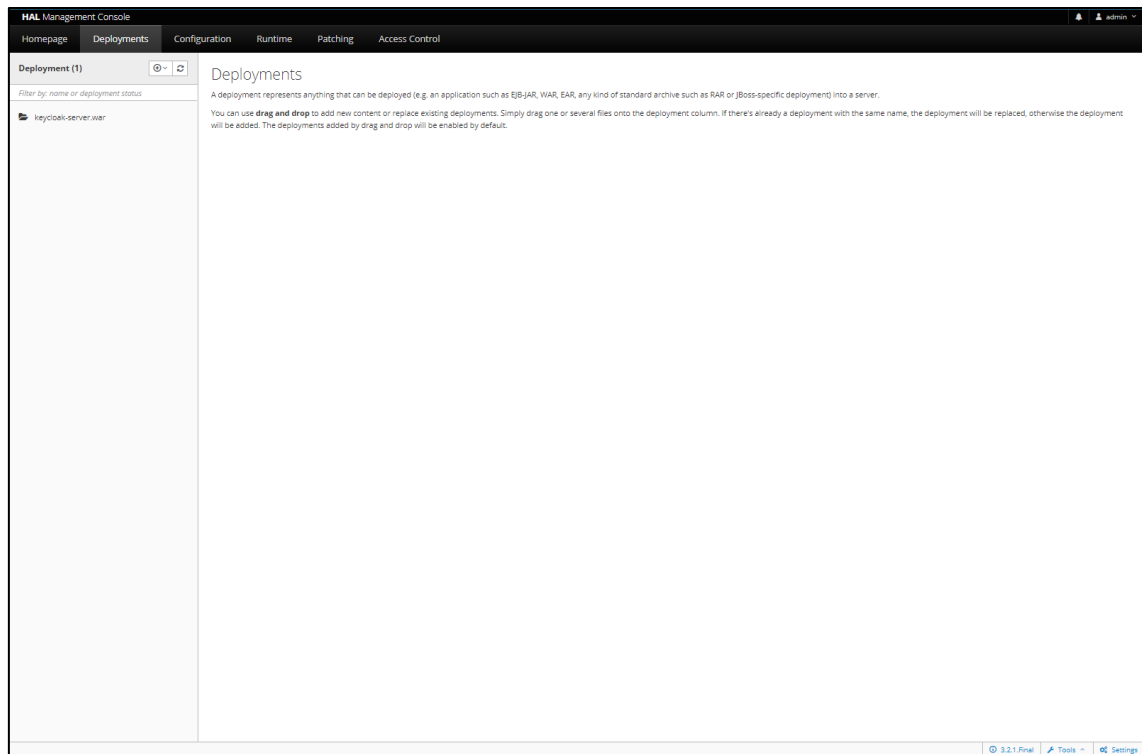



Figure 14: Keycloak Server Deployments Page

Click on the following button located at the top left:



Figure 15: Deployment button


Click on the upload a file button, and select the file Keycloak\_Session\_Tracker.ear

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

Add Deployment

Upload Deployment

Specify Names



Keycloak\_Session\_Tracker.ear

Cancel < Back Next >


Figure 16: Module deployment process

Once the file has been uploaded, click on the next button and then on finish. If the deployment process has worked correctly, the following message will appear:

Add Deployment

Upload Deployment

Specify Names



Upload successful

Keycloak\_Session\_Tracker.ear has been successfully uploaded to the content repository.


View Deployment

Cancel < Back Close

Figure 17: Module correctly deployed

And again, we click on the upload a file button, and select the other file Keycloak\_CBA.ear and follow the same steps.



	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

The installation process is now complete. Before continuing with the next steps, it is necessary to restart the Keycloak service. To do this, go back to the terminal used to start the application and press the keys ctrl + c. Once the application has finished running, launch the same command used previously.

We access again to the web address: <http://localhost:8080/auth/admin/>. Enter the credentials of the administrator user and access the Dashboard of the Keycloak application.

When accessing the Keycloak Dashboard for the first time, it will be necessary to apply a series of steps to configure the deployed modules. The first step is to configure the events module. To do this we go to the tab: Events > config and add the new "Event Listener":

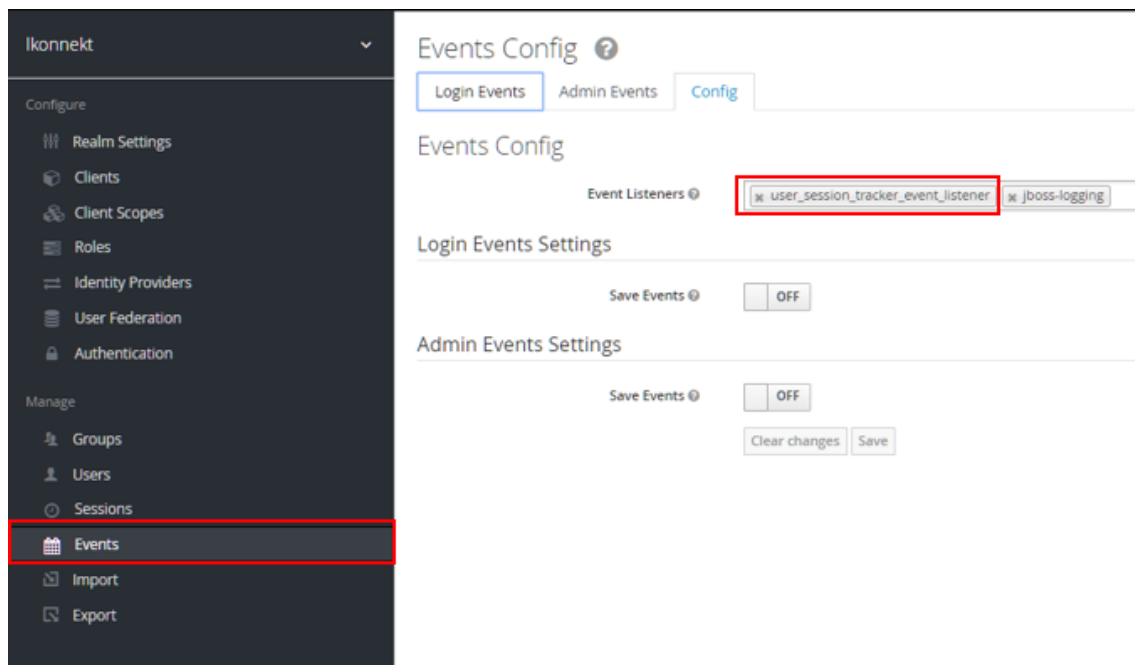



Figure 18: Adding an Event Listener in Keycloak

Once the previous step is configured, navigate to the following tabs: *Realm settings* > *Themes* and change the Login theme to *Ikerlan*.

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

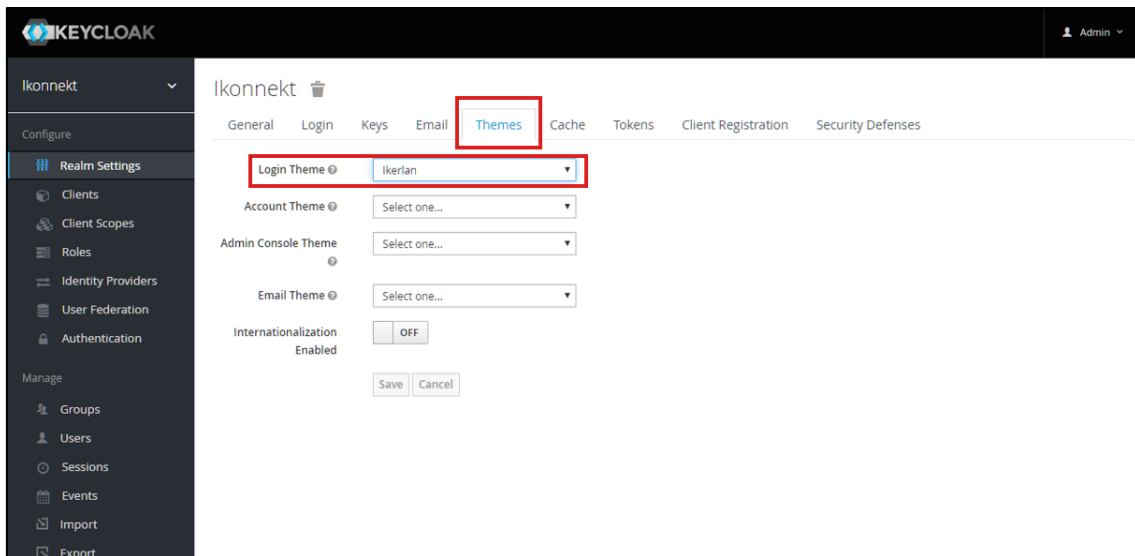


Figure 19: Configuring Keycloak themes

The next step is to create a new authentication flow. To do this we navigate to another tab located at *Authentication > Flows > New*:

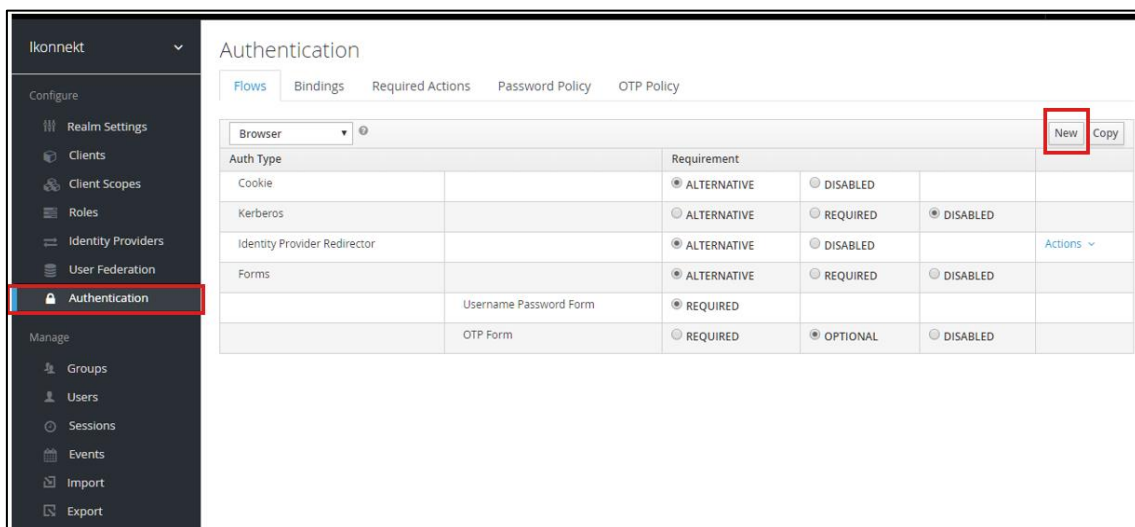



Figure 20: Adding a new authentication flow

We will call this flow CBA and we will add an "execution" by selecting the option called Context Base Authentication. It is important to check the Requirement box with the required option:

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

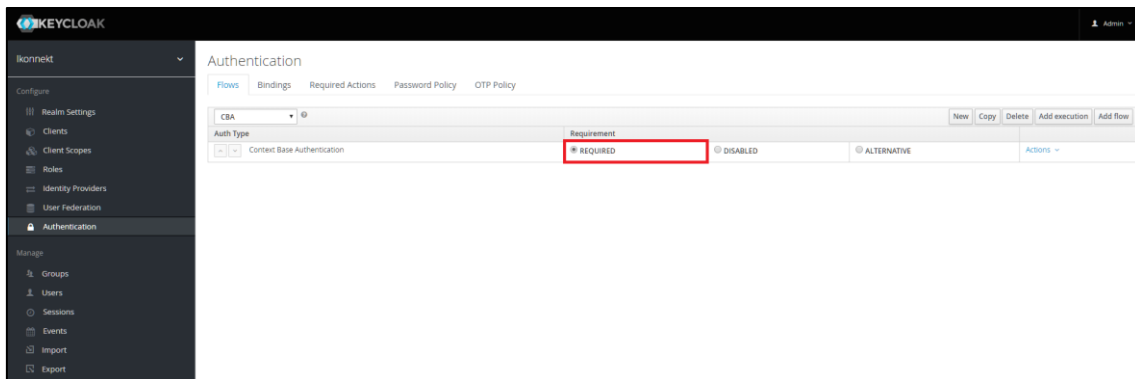


Figure 21: Configuring the CBA flow

Finally, we navigate to the Bindings tab and select the CBA option for Browser Flow.

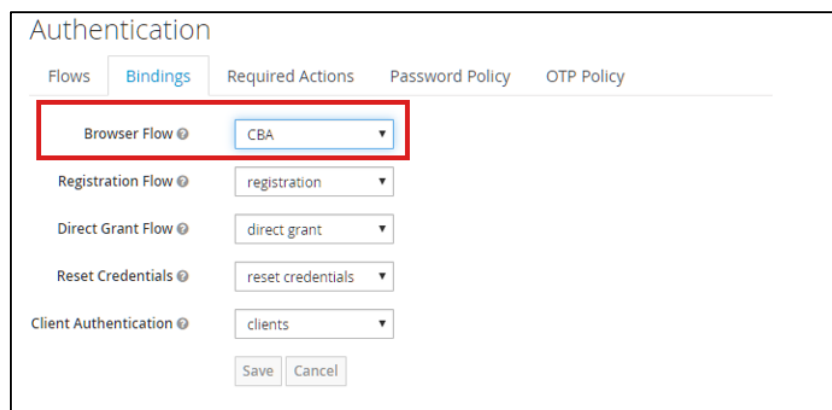


Figure 22: Binding the CBA flow

This concludes the installation, deployment and configuration guide of the IK-SEC context-based module in Keycloak.


### • 4.1.3 Future Work

The IK-SEC context-based module is integrated within the IK-SEC+ solution of IKERLAN, that is being integrated within the digital platform of the Fagor Arrasate machine pilot (pilot #13) in WP7 of QU4LITY. This way, the platform will use keycloak and the context-based keycloak module to provide access and authorization to the different users of the platform. The context data will be used to limit the access to the data and resources to the users, depending on their permissions.

## 4.2 Data Anonymization Solution

### • 4.2.1 Description and Functionality

Data anonymization, also called de-identification, is a vital building block for protecting privacy in applications that may use personal data from individuals. It is the process of protecting private and sensitive information by removing or encrypting identifiers, such as names, social security numbers and addresses that connect the

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

stored data to an individual. It is part of holistic security and privacy solution to protect personal data on premises, in the cloud and in hybrid environments.

The General Data Protection Regulation (GDPR) outlines a set of rules to protect the personal data of all European Union residents and visitors in order to establish personal data protection rights for individuals to access, correct, erase or port their personal data. GDPR's definition of personal data includes any information that can identify a specific person directly or indirectly. Based on that definition, examples of personal data can include biometric data, health data or other types of data such as online identifiers, personal identifying information such as name, social security number, email address, photos or messages.


In data anonymization the following methods are used:

- **Data masking:** The approach used is hiding of data with altered values, where characters that make up a data element are shuffled, encrypted or substituted by other words or characters. Depending on the kind of data masking approach is used, it may be possible to reverse-engineer or detect the original data.
- **Pseudonymization:** This is a data de-identification method that uses fake identifiers or pseudonyms to replace private identifiers and sensitive data. For instance, to replace the first and last name of an individual, "Bob Smith" with a fake one. The modified data can still be used for data analytics purposes while protecting data privacy.
- **Generalization:** This method is the removal of some of the data with the purpose of making it less likely to be identified. Typical approaches used are modifying data into a set of ranges or a broader category. For instance, the age of a person, "22" can be replaced with an interval of numbers, "[20-25]", that contains it.
- **Data swapping:** This method uses shuffling or permutation to rearrange the values in a dataset so that they do not match their original attributes (columns). For instance, swapping identifier values such as date of birth.
- **Data perturbation:** Dataset is modified by rounding number and adding random noise.
- **Synthetic data:** Data is simulated or manufactured algorithmically to create artificial datasets using statistical models such as standard deviations, medians or other statistical techniques.

#### • 4.2.2 Usage and Results

Implementing formal methods of data anonymization requires a complex interplay of methods for measuring privacy risks, transforming data, and also for making sure that the usefulness of data is not overly impacted. To put these approaches into practice requires tool support. One such tool is ARX<sup>2</sup>, which was initially presented at AMIA 2014.

<sup>2</sup> <https://arx.deidentifier.org>

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

Using ARX data can be transformed semi-automatically to anonymize data according to the GDPR compliance. ARX supports a wide range of formal mathematical and statistical methods for data transformation, risk assessment and utility evaluation.

**Privacy Models** When using anonymization methods, an important aspect is how risks and degrees of protection are being quantified. ARX supports several privacy models for quantifying and protecting privacy. These include well-known models, such as k-anonymity and l-diversity, t-closeness, b-likeness, but also statistical models based on population estimates and state-of the art models such as game-theoretic approaches and differential privacy.

**Transformation models** After deciding on a method for quantifying risks it is important to transform data in such a way that risk thresholds and required protection levels are met. ARX supports different methods for transforming data including various ways of data generalization, top and bottom coding, suppression sampling and the aggregation of numeric variables.

**Utility Models** Anonymization is an optimization process, where reduction of risks is traded off against reduction of the utility of data. To be able to perform this in a semi-automated manner, ARX supports several different models for quantifying the utility of data during the anonymization process, including general-purpose methods reflecting data fidelity or changes to value distributions as well as application specific models, such as for creating privacy preserving machine learning models.

**Graphical User Interface** ARX offers a comprehensive and highly scalable graphical user interface. It provides compatibility with SQL databases, MS Excel and CSV files.

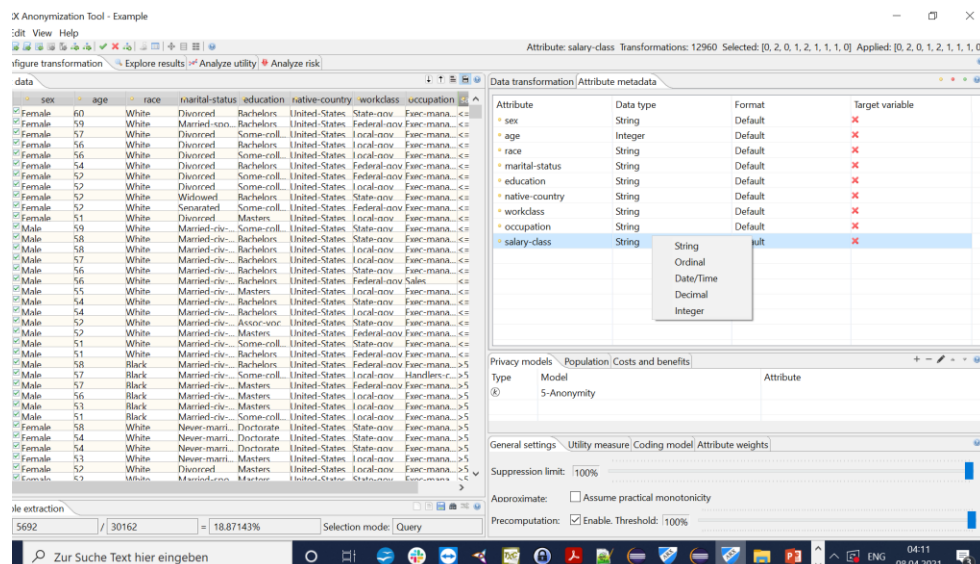


Figure 23: Sample Dataset in the ARX tool before data-anonymization

Supported data types are string, ordinal, date/time, decimal and integer. Attributes can be categorized as quasi-identifiers, identifiers, sensitive or insensitive attributes. For each attribute in the dataset, it is possible to create and edit generalization

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

hierarchies, specify the privacy criteria, such as k-anonymity, for the type of the attribute and configure the anonymization process. For example, the attribute sex is a categorical attribute. A generalization hierarchy for the attribute sex can be created by using a wizard based on ordering, creating an ordered list of the values male and female of the attribute, and combining these values into a common group. Another example is the attribute age, which is a numeric attribute. For numeric attributes, one can use a wizard based on intervals and define the range, the length of the interval. New intervals can be defined by merging intervals from lower levels.

## 4.3 Monitoring Solution

This section describes the monitoring solution used in QU4LITY in the SPT and its functionality, focused on the aspects more specific for the constraints and needs of industry.

### • 4.3.1 Description and Functionality

Is very important to spot the errors and service failures before they make any impact. System and network monitoring in QU4LITY will help us in resolving any issues before it leads to a significant break in the system. It will also be very useful when investigating the cause of an attack.

The monitoring sensor provides a real-time view of computing system internals and network packets. This info is stored and used by the SIEM to generate security alerts and allow the user to have a complete view of the risks and evolution of the system.

The sensors are structured in the form of the client-server schema, with multiple sensors pointing each agent, which in turn send information to a server.

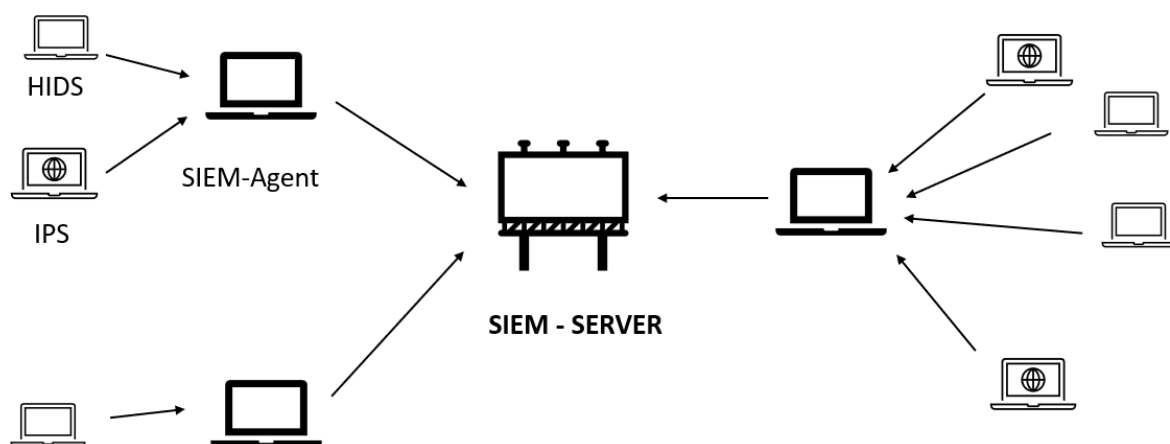


Figure 24: Monitoring Sensors schema

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

The sensors can detect a wide number of threats like the following:

- Network packets directed to the host.
- Rootkit detection.
- Intrusion detection.
- Periodical integrity checking for most operating system.

Once the event is detected, the agent filter through irrelevant information to find essential events and send it to the server. Finally, on the server side, the SIEM read all event logs and identify which sequences of events would be an indication of anomalies. Using previously configured correlation rules, the topology creates the corresponding alarms and assigns them a degree of criticality. The server has a graphical interface to have a quick view of the events and alarms and a database to store it.

#### • 4.3.2 Usage and Results

All the monitoring sensors can be easily deployed as Docker containers. As a backend component, the monitoring sensor are constantly working without user intervention.

```

** Alert 1631739391.21576033: - pam,syslog,authentication_failed,
2021 Sep 15 20:56:31 qu4lity->/var/log/auth.log
Rule: 5503 (level 5) -> 'User login failed.'
Src IP: 45.42.13.123
User: root
Sep 15 20:56:31 qu4lity sshd[465609]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=45.42.13.123 user=root

** Alert 1631739393.21576375: - syslog,sshd,authentication_failed,
2021 Sep 15 20:56:33 qu4lity->/var/log/auth.log
Rule: 5716 (level 5) -> 'SSH authentication failed.'
Src IP: 45.42.13.123
User: root
Sep 15 20:56:33 qu4lity sshd[465609]: Failed password for root from 45.42.13.123 port 45232 ssh2

```

Figure 25: Example of an event log.

The user will be able to see all the relevant information through the SIEM graphical interface in the following web address. Mostly of the SIEM configuration are configurable as well.

<https://37.48.101.251:8080>

Right in the frontpage of the SIEM, the user can take a quick look at all the evolution in time of all the monitoring sensors relevant events:


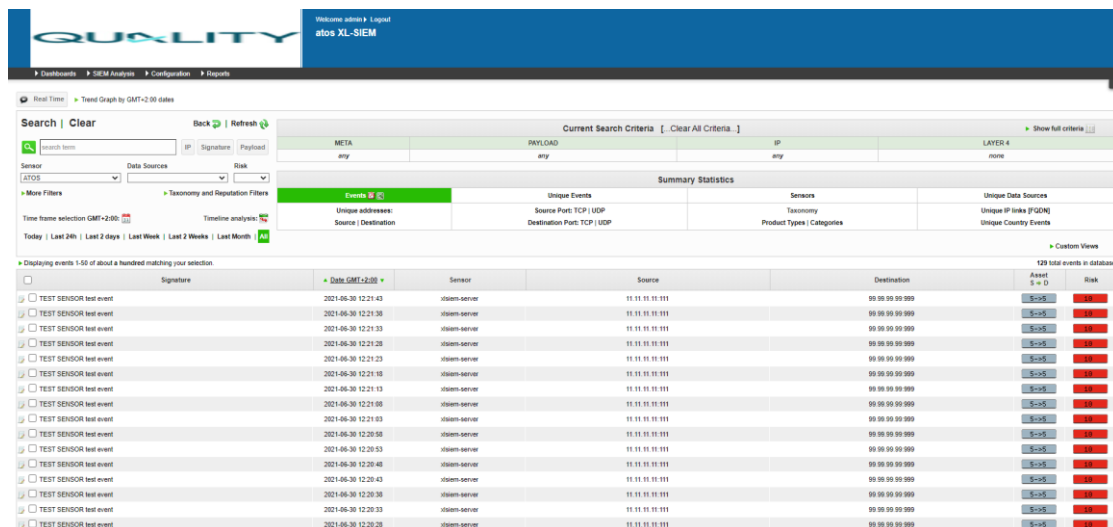
	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU



Figure 26: General view of the SIEM

A list of all events and alarms are also displayed:




Signature	Date GMT+2:00	Sensor	Source	Destination	Asset S+O	Risk
TEST SENSOR test event	2021-06-30 12:21:43	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:21:38	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:21:33	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:21:28	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:21:23	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:21:18	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:21:13	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:21:08	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:21:03	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:20:58	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:20:53	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:20:48	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:20:43	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:20:38	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:20:33	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High
TEST SENSOR test event	2021-06-30 12:20:28	alarm-server	11.11.11.111	99.99.99.999	S-C-S	High

Figure 27: List of all events





	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

More details on this analysis can be found in the corresponding technical report to be found at <https://cloud.uni-koblenz.de/s/zz5yEKej8qjLGm3> . The following figure gives an overview of the content of that report.

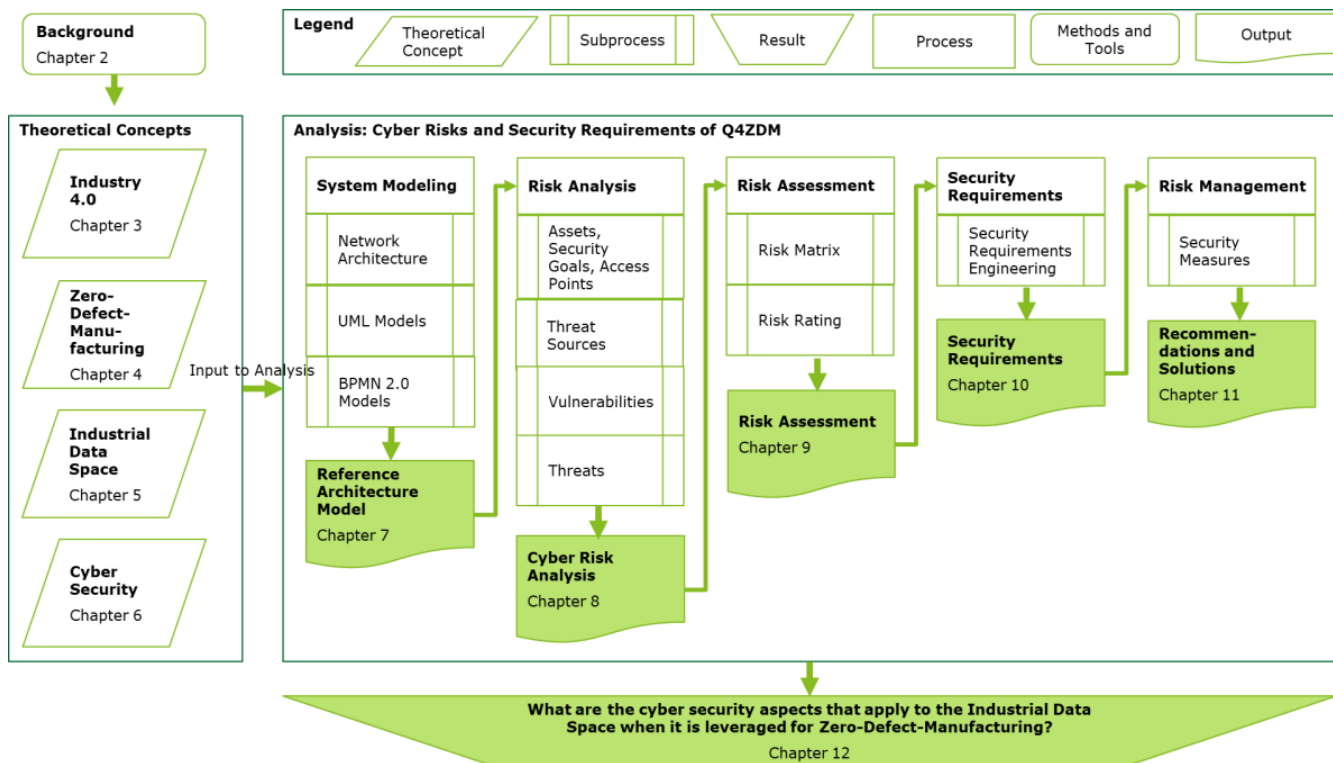


Figure 29: Overview of the Cyber Security and Risk Analysis Approach and Workflow

The approach proceeds as follows.

1. **System Modeling.** As a first step, the QU4LITY system is modeled in a Network Architecture Diagram, a UML model, and a BPMN model. For the system modeling, we used the modeling notations Unified Modeling Language (UML), the Business Process Modeling Notation (BPMN) 2.0 and network architecture diagrams. We used system models because system models deliver a visual overview of the system architecture, which helps to determine the risks.
2. **Risk analysis.** After system modeling, the cyber risks of the system are identified and analyzed. The cyber risk analysis steps are as follows:
  - Identification of assets, security goals, and access points.
  - Identification of threat sources.
  - Identification of vulnerabilities that could be exploited to get access to the assets.
  - Identification of threats.
3. **Risk assessment.** After the risks are identified, they are assessed by creating attack scenarios and assessing their impact and likelihood to determine their criticality. The risk assessment steps are as follows:
  - Mapping of threats to attack scenarios.
  - Prioritize risks according to likelihood and criticality in a risk

QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

matrix.

4. **Cyber security requirements definition.** For the cyber security requirements definition, the steps are as following:
  - Definition of requirements for the risks not to occur.
5. **Risk management.** The risk management steps are as following:
  - Selection of controls, solutions, and recommendations.

The author Sommerville (2016) suggests a risk analysis and assessment process to define security requirements during each stage of the system lifecycle. At this stage of the QU4LITY project, the decisions about the details of the system design, implementation, and other software development process steps have not been made public yet. Therefore, in this research, a preliminary risk assessment is conducted. The preliminary risk assessment process is used to define security requirements for the QU4LITY system. We recommend that another risk assessment takes place after the design decisions are made. Because at that point of the system development lifecycle, the technologies that are used in building the system, system design, and implementation decisions can be considered. In the final stage of the project, an operational risk assessment could consider the risks that could occur through users of the system.

#### • 4.4.2 Usage and Results


In this section, we demonstrate the developed modeling and analysis approach. The subject of the Risk Analysis demonstration is a simplified example derived from one of the QU4LITY application scenarios, namely a shaving blade manufacturing plant called SingleBlade.

As part of the demonstration, we present a structural overview of the International Data Spaces in a class diagram. This section also proposes QU4LITY system models of the data exchange processes. The author modeled the process models based on the information of the International Data Spaces-RAM (2019) . The system models are used for cyber security and risk analysis. The system models in this section model the data exchange process that is relevant for further analysis.

There are two scenarios associated with the QU4LITY system to identify the risks and requirements to the inter- and cross-organizational data exchange: 1) data is exchanged internally using the Internal Connector 2) data is exchanged externally using the External Connector.

Both scenarios are modeled using system modeling notations. The first scenario is modeled in a UML Class Diagram to show the interactions between a shop floor device and the Internal Connector. The second scenario is modeled using BPMN 2.0 to show the connections with other stakeholders as well as the data exchange process. The BPMN models are building on the International Data Spaces-RAM (2019) and are extended by the author's input to include QU4LITY system processes and components.

The UML class diagram architectures of the underlying report are based on the architecture modeled in the report (Kramer, 2016) and the International Data Spaces-RAM (2019). The UML class diagrams used in this report are in no way or

	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

form complete representations of the class diagram that is used for the implementation of the International Data Spaces or QU4LITY. A comprehensive class diagram would not fit on a sheet of paper and thus would not benefit the readability of this document. The goal of presenting the system models is to visualize an overview of the structure and processes in QU4LITY to identify a baseline of risks. Therefore, an abstract version is visualized in this report. Due to this, the UML models do not represent all International Data Spaces entities such as the Vocabulary Provider, Service Provider, App Store Provider, and App Provider as well as their activities.


In this section, we demonstrate the developed modeling and analysis approach. The subject of the Risk Analysis demonstration is a simplified example derived from one of the QU4LITY application scenarios, namely a shaving blade manufacturing plant called SingleBlade.

As part of the demonstration, we present a structural overview of the International Data Spaces in a class diagram. This section also proposes QU4LITY system models of the data exchange processes. The author modeled the process models based on the information of the International Data Spaces-RAM (2019) . The system models are used for cyber security and risk analysis. The system models in this section model the data exchange process that is relevant for further analysis.

There are two scenarios associated with the QU4LITY system to identify the risks and requirements to the inter- and cross-organizational data exchange: 1) data is exchanged internally using the Internal Connector 2) data is exchanged externally using the External Connector.

Both scenarios are modeled using system modeling notations. The first scenario is modeled in a UML Class Diagram to show the interactions between a shop floor device and the Internal Connector. The second scenario is modeled using BPMN 2.0 to show the connections with other stakeholders as well as the data exchange process. The BPMN models are building on the International Data Spaces-RAM (2019) and are extended by the author's input to include QU4LITY system processes and components.

The UML class diagram architectures of the underlying report are based on the architecture modeled in the report (Kramer, 2016) and the International Data Spaces-RAM (2019). The UML class diagrams used in this report are in no way or form complete representations of the class diagram that is used for the implementation of the International Data Spaces or QU4LITY. A comprehensive class diagram would not fit on a sheet of paper and thus would not benefit the readability of this document. The goal of presenting the system models is to visualize an overview of the structure and processes in QU4LITY to identify a baseline of risks. Therefore, an abstract version is visualized in this report. Due to this, the UML models do not represent all International Data Spaces entities such as the Vocabulary Provider, Service Provider, App Store Provider, and App Provider as well as their activities.

	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

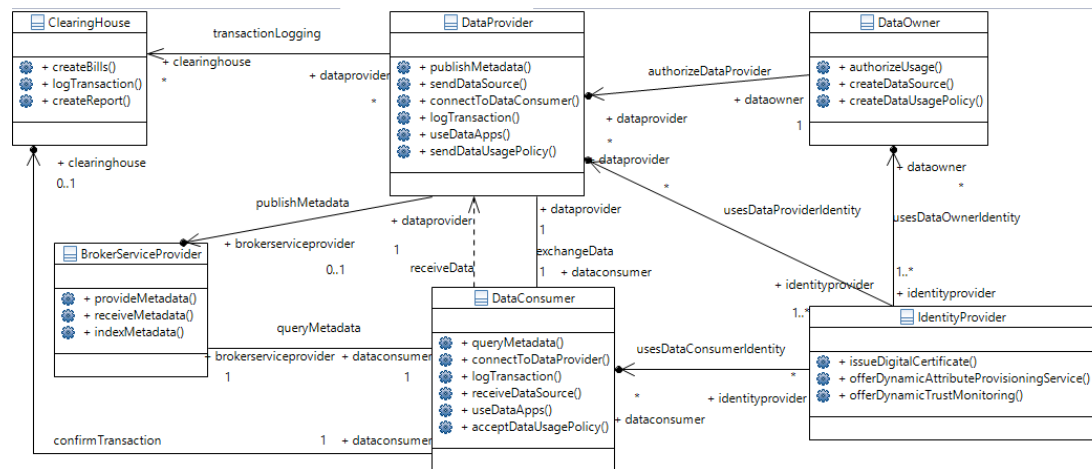


Figure 30: International Data Spaces Structural Overview in a UML Class Diagram

The above Figure shows the external entities and roles that are involved in the data exchange using the International Data Spaces. Each class represents an entity in the International Data Spaces. Some entities have multiple roles in the International Data Spaces Infrastructure. The methods are representing the activities that a specific role can execute, as mentioned in International Data Spaces Infrastructure. The model represents the entities in the perspective of SingleBlade as follows:


The SingleBlade plant is both the Data Owner and Data Provider and wants to share data with the Data Consumer. For simplicity, it is understood in the model that SingleBlade is both Data Owner and the Data Provider. SingleBlade being both Data Provider and Data Owner, creates the Data Source, decides upon Data Usage Control Policies, and authorizes the data exchange. SingleBlade publishes its Metadata at the Broker Service Provider database. The Broker Service Provider receives the Metadata and indexes it. A Data Consumer may use a Broker Service Provider to query the Metadata of SingleBlade. As a Data Provider, SingleBlade may use Data Apps to transform the data. Then the Data Provider Connector connects to the Data Consumer and sends the Data Source. The Data Consumer connects to the SingleBlade Connector and receives the Data Source. The Data Consumer may use Data Apps to transform the data. Both SingleBlade and the Data Consumer use the Clearing House service to log their data transaction. The Clearing House can then create bills and reports. The Identity Provider connects to all parties to issue Digital Certificates and offer DAPS and DTM services.

In the following, the International Data Spaces infrastructure is combined with the data exchange scenarios.

## QU4LITY Internal Data Exchange Processes

In this section, we propose system models for the first scenario of the internal data exchange in a class diagram.

Scenario 1 Data is exchanged internally: The first scenario is looking at how the data is exchanged in the QU4LITY system internally from the sensors on the shop floor

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

level to the internal systems as well as the Internal Connector in the SingleBlade plant.

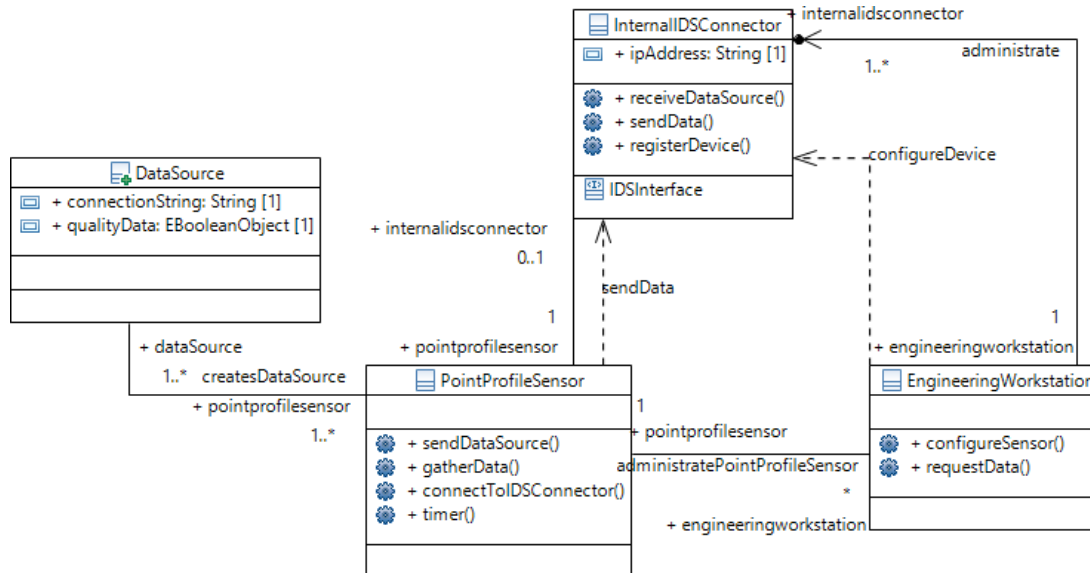


Figure 31: Structural Overview of the Internal Data Exchange in a UML Class Diagram

In scenario 1) a SingleBlade engineer that is working at an engineering workstation is configuring a 3D Point Profile Sensor1 (PointProfileSensor) for quality control as part of the QU4LITY system. Profile sensors are Smart sensors that use a single laser point to scan an object at a high speed (LMI Technologies, 2019).


The sensor measures the thickness, height, and surface roughness of the shaving blade. From the gathered data, the sensor can detect displacement. Based on the measured features, the sensor checks the measurements against the entered tolerated parameters to generate a pass/fail decision for quality control.

When the engineer configured the sensor (configureDevice), the sensor registers itself (registerDevice()) at the Internal Connector and starts collecting data (gatherData()). Every 10 seconds a new part arrives at the checkpoint. A timer (timer()) counts to 10 to send (sendDataSource()) the quality data (qualityData: EBooleanObject [1])) together with data to authenticate itself (connectionString), to the Internal Connector.

The Internal Connector (InternalIDSCConnector) is accessible through an internal IP address. The International Data Spaces Interface is a communication interface to send and receive data at the Connector. The human operator administrates all Internal Connectors at the Engineering Workstation.

### Gathering QU4LITY Data Process

The SingleBlade data exchange process starts with the collection of data. It is assumed that data is gathered by SingleBlade as the Data Owner, from various sources at the shop floor level.

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

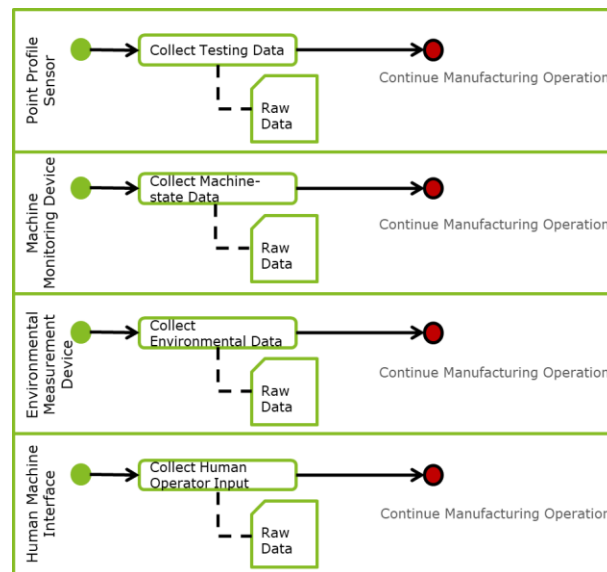


Figure 32: Data Collection subprocess in a BPMN Diagram

The above Figure visualizes the Data Collection process on the Shop floor level for the example of Single-Blade. The BPMN shows examples of devices that could be leveraged to collect data. For example, the point profile sensor could collect testing data about quality parameters, the machine monitoring device that is installed at the actuator could gather machine-state data, an environment measurement device could collect data about the temperature, or dust level in the manufacturing plant, and the human operator input could be collected from the HMI. The devices and types of data can be inter- changed with any other device or type of data that is relevant for QU4LITY. We assume that SingleBlade stores the gathered data at the Inmation Data Historian.

### Processing QU4LITY Data Process

The processing QU4LITY process describes how, after the data is gathered, it is processed and sent to the Data Knowledgebase Platform to enrich the data. These steps are not specified in the International Data Spaces-RAM (2019). However, they are relevant to the QU4LITY system.

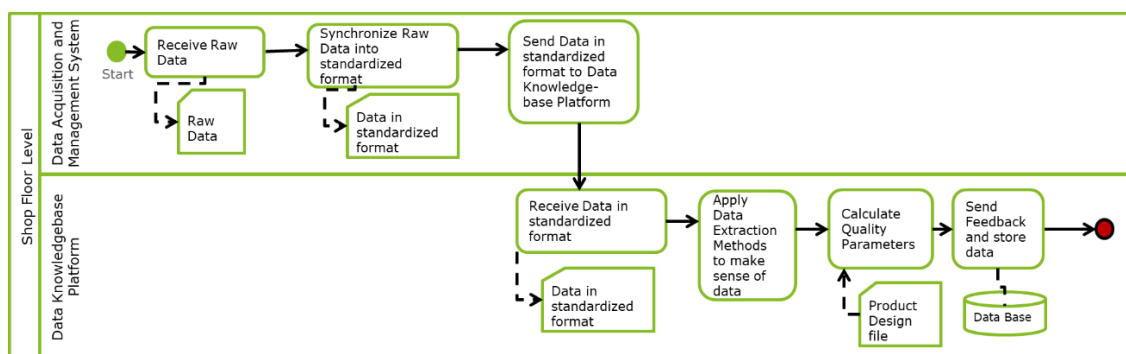



Figure 33: Data Acquisition System and Data Management System of the Data Provider in a BPMN Diagram



	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

The above figure visualizes this process. Consecutively after the data is gathered, it is sent in and raw, unprocessed format over an OPC UA connection to the Data Acquisition and Data Management System that was already mentioned. For SingleBlade, we assume that the gathered data is sent to the Information Data Historian. The data acquisition system synchronizes the raw manufacturing data into a standardized format. We assume that this is taken care of the Apache Hadoop ecosystem and the Data Historian. After processing, the standardized acquired data is sent to the Data Knowledgebase Platform.

The Data Knowledgebase Platform receives the acquired data and applies data extraction methodologies to enrich the data. It is assumed that for SingleBlade, this is taken care of by the Neuronal Process Control System (NPRES). The system calculates the quality parameters of the production process and compares it to the desired measurements in the product design file to predict the outcome at the end-of-line test. This information is pushed back to the shop floor devices as part of the feedback loops.

For the SingleBlade scenario, it is assumed that after the process, the Data Source is sent from the Level 2 Site Manufacturing Operations and Control Zone through a firewall to the Internal Connector that is in the OT DMZ.

### Providing QU4LITY Data through the International Data Spaces Process

After the data arrives at the Internal Connector, the Internal Connector makes the data available to the External Connector. The External Connector is in the Enterprise DMZ. It is assumed that the process steps of the Deploy Connector, Publish Metadata and setup security subprocess are equal to the process steps illustrated in the International Data Spaces-RAM (2019). Thus, these steps are indicated by the green plus sign but not illustrated separately in the underlying report.

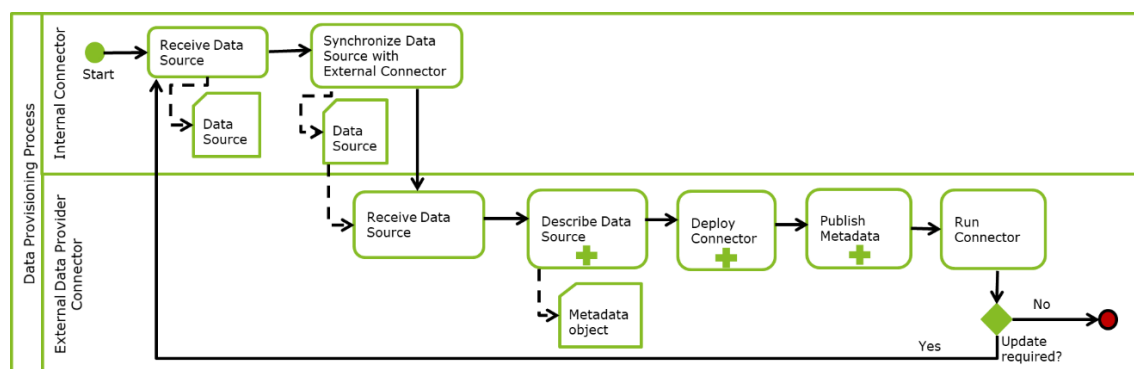



Figure 34: Data Provisioning Process from the Internal Connector to the External Connector in a BPMN Diagram

The above figure visualizes the data provisioning process. The data providing process starts at the synchronization of the data between the Internal and External Connector of the SingleBlade plant. For the synchronization, the data is sent from the Internal Connector to the External Connector.



	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

To be able to publish the Metadata at the Broker Service Provider, the Data Provider describes the Data Source using the vocabulary information model vocabularies. The description is conducted as a subprocess which is indicated by the plus sign. The result of the subprocess is the Metadata object that describes the Data Source. The Metadata also includes Data Usage Policy information.

After the Metadata object is created, the Data Provider deploys the Connector and publishes the Metadata at the Broker Service Provider. The Broker Service Provider receives the Data Source Description Metadata, sends an acknowledgment of receipt of the Metadata back to the Data Provider. In the meanwhile, the Broker Service Provider indexes and publishes the Metadata in the Metadata Repository. This subprocess is indicated by the plus sign in the Publish Metadata process step.


As the last step, the Connector runs. Once the Connector runs, it is checked if an update of the data is required. This is indicated by the green gateway. This process iterates until the Connector is synchronized and the Data Consumer can access the data. For SingleBlade, the Data Consumer could be one of the International Data Spaces Connections that were already mentioned. The connection to the Data Consumer is part of the external data exchange process, which is illustrated in the next section.

### **QU4LITY External Data Exchange Processes**

This section models scenario 2, the external data exchange process in BPMN 2.0 diagrams.

Scenario 2 Data is exchanged externally: as illustrated in the use case, the SingleBlade plant needs to exchange data with the material and part suppliers, as well as the headquarters and remote manufacturing sites of the consumer-goods firm. When data is exchanged with the external parties of the SingleBlade plant, the External Connectors and the infrastructure of the International Data Spaces are used.

We modeled this system in BPMN models to show the flow of information and the processes that are involved in the external data exchange process between SingleBlade and the remote manufacturing site. The BPMN models are showing a more in-depth view of the process of the data exchange of scenario 1) and 2).

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

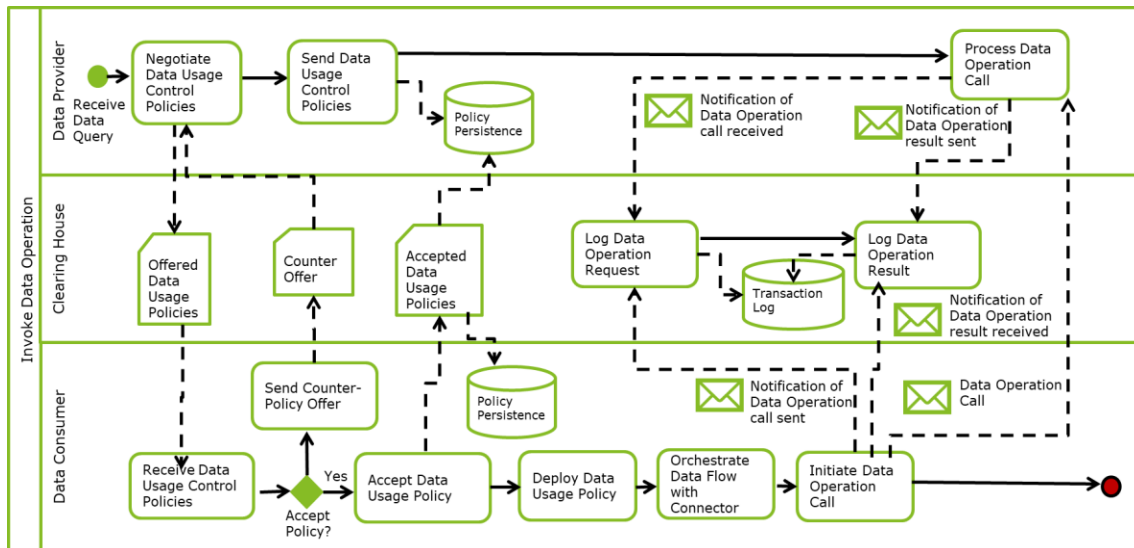


Figure 35: High-level Overview of Invoke Data Exchange Process in a BPMN Diagram (Otto et al., 2019)

The above figure shows how the data exchange process is invoked from a high-level point of view. The overview was taken from the International Data Spaces-RAM (2019). Each process is looked at individually in the following.

### Exchanging QU4LITY Data through the International Data Spaces Process

The exchange data process, as per International Data Spaces-RAM (2019), has three subprocesses.

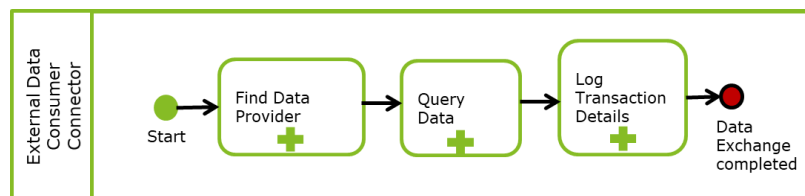



Figure 36: Data Exchange Process in a BPMN Diagram

The above Figure illustrates the three steps to the data exchange process. The three steps are the A) Find Data Provider process, B) the query and send data process, and C) the log transaction process. It is assumed that the onboarding process and the Connector configuration subprocess are equivalent to the processes illustrated in the International Data Spaces-RAM (2019) and thus are not illustrated in this document.

### Find Data Provider Subprocess

The Find Data Provider subprocess is from the perspective of the Data Consumer. In the case of SingleBlade, the Data Consumer is the remote manufacturing site.

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

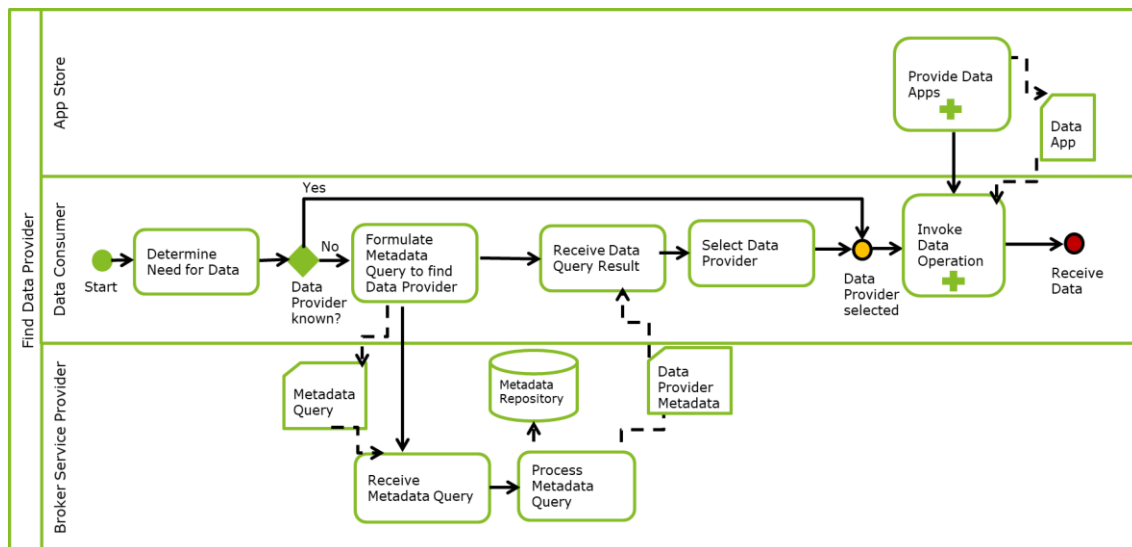


Figure 37: Find Data Provider Subprocess in a BPMN Diagram


The above figure illustrates the process. The Find Data Provider process starts when the Data Consumer recognizes a need for data. Then the remote manufacturing site needs to determine whether a Data Provider who can provide such data is already known to the Data Consumer or not. If the Data Consumer does not know a Data Provider, the Data Consumer can find a suitable Data Provider at the Broker Service Provider. In this case, the Data Consumer formulates a Metadata Query at the Broker Service Provider. In the query, the Data Consumer asks for a specific kind of data, and whether a Data Provider is available with that information.

Then, the Broker Service Provider receives the query for Metadata from the Data Consumer and processes it. Then the Broker Service Provider sends a list of Metadata back to the Data Consumer. The list is describing the Data Sources of the different Data Providers that suit the Metadata Query.

Afterward, the Data Consumer selects a Data Provider from that list. Once the Data Provider is chosen, the data flow with the Connector is orchestrated. In this case, this occurs when the remote site finds the SingleBlade Connector as a Data Provider to connect to. This process is connected to the query data process.

If the Data Provider is already known to the Data Consumer before the Metadata query at the Broker Service Provider, the consultation is not necessary. Meaning, if the remote site already has the details of the SingleBlade Connector, the remote site can directly configure its Connector (Data Consumer) to connect to the corresponding Connector of SingleBlade (Data Provider).

Before the orchestration of the data flow, the legal agreement must be established between the Data Consumer and the Data Provider.

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

## Query and Send Data Subprocess

Data Usage Control Policies are a fundamental aspect of International Data Spaces concepts. The process of implementing the Usage Control Policies is not modeled in the International Data Spaces-RAM (2019) because the legal agreement terms and conditions are not decided upon yet. Thus, the query data process has been modeled as per the authors understanding of the International Data Spaces concept.

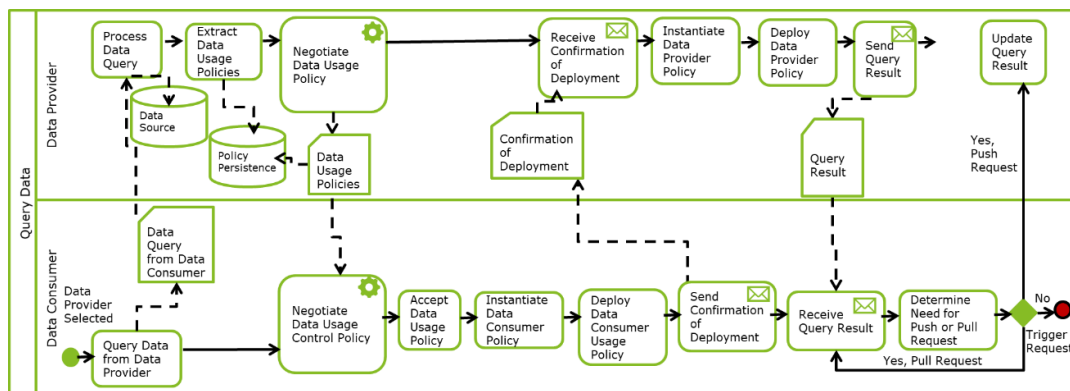


Figure 38: Query Data subprocess in a BPMN Diagram


The above figure visualizes this process. The Query Data subprocess starts with the request of the remote manufacturing site to receive QU4LITY data from the SingleBlade plant. The Data Consumer queries the data from the Data Provider at the representing Connector. As another option the remote manufacturing site could have a subscription at SingleBlade, then the Data Consumer receives a notification if new data is available and can take action to query the data.

SingleBlade receives the query and processes the query by searching for appropriate data in the system. Then the Data Provider extracts the Data Usage Control Policies and negotiates the Data Consumer policy by sending the Data Usage Control Policies to the remote site in an automated negotiation process.

If agreed upon, the remote site then instantiates and deploys the Data Usage Policy at its Connector. After deployment, the remote site sends a confirmation to SingleBlade.

Then Data Provider receives the confirmation that the Data Consumer has deployed the Data Usage Policy. Then, the Data Provider instantiates the Data Provider policy at its Connector. Next, the Data Provider implements the Data Provider policy and sends the Data Query result to the Data Consumer through the External Connector.

The communication between the Connectors can be in an asynchronous manner. This means the Data Consumer does not have to wait for the data to arrive. The Data Consumer will be notified by the Data Provider Connector as soon as the data is available. Subsequently, the Data Consumer receives the Data Query result. The Data Consumer can also send a push request that asks for updates of the re- requested data. Once the Data Provider has updated the queried data, the process iterates. If

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

the Data Consumer triggers a push request, it is subscribed to the updates of the queried data results by the Data Provider. If the Data Consumer triggers a pull-event, the last process part of the query data process iterates.

As the last step, the Connector looks for a push request. If there is a push request, the query process iterates. If there is no push request, the process ends, and the transaction is logged.

### Log transaction data subprocess

After the data transaction is completed, the transaction is registered at the Clearing House.

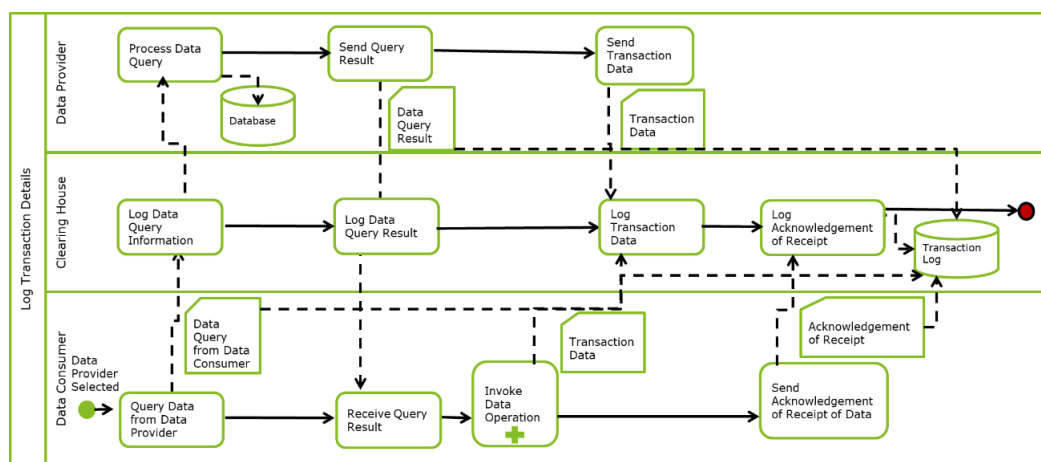



Figure 39: Transaction Logging Subprocess in a BPMN Diagram

The above Figure visualizes the transaction logging process. For the transaction logging, both the Data Consumer and the Data Provider send a message to the Clearing House that states that the transaction is completed successfully. The Clearing House logs any query information as well as the query result. The Clearing House logs what kind of data was queried by the Data Consumer, and what type of data was sent by the Data Provider.

### QU4LITY Data Exchange Process Security Dependencies

This section highlights why security is an essential aspect of QU4LITY. Based on the previous system models, a UMLsec check on the QU4LITY system shall deliver the first overview of any security risks to the system. The UMLsec approach is based on the description already given.

To illustrate the external data exchange process, both infrastructures are combined in a UML class diagram, which looks like the following:

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

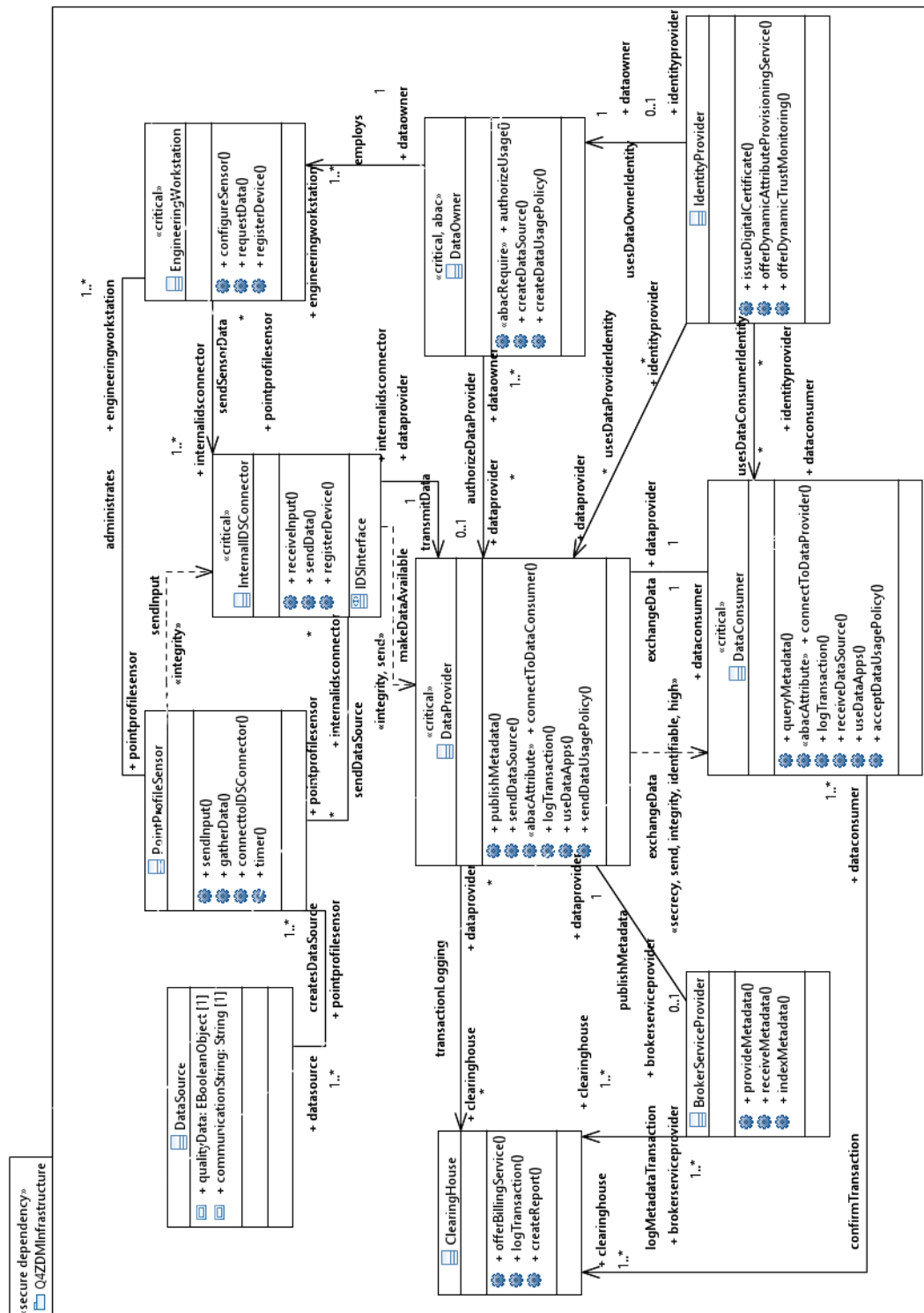



Figure 40: QU4LITY Infrastructure in a class diagram with <<secure dependency>> UMLsec check

The UML Class Diagram in the above figure was annotated with the <<secure dependency>> check of UMLsec using the CARISMA profile in Eclipse. This figure combines the UML Class Diagrams of the two earlier figures.

	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

The Data Provider, Data Owner, and Data Consumer are annotated with the <<critical>> label for the UMLsec check. The data that is transmitted from the Data Provider to the Data Consumer must oblige to a high- security standard and preserve integrity and secrecy. Therefore the link is annotated with the tags <<secrecy, send, integrity, identifiable, high>>.

The sendInput function represents the connection from the point profile sensor to the Internal Con- nector. The Internal Connector is located in the internal company network. The Internal Connector of SingleBlade is located in the OT DMZ. The connection is therefore annotated with the <<integrity>> tag.

The makeDataAvailable function represents the connection from the Internal Connector to the External Data Provider Connector. The Internal Connector facilitates access to the DataSources to provide the data to the External Data Provider Connector. The connection is annotated with the <<integrity>> and <<send>> tag.

The exchangeData function represents the exchange of the Data Source file together with the Usage Control Policy from the Data Provider to the Data Consumer. The exchangeData function is annotated with the <<send>> and <<high>> label, because the exchangeData function rep- resents a link to an external entity over the internet. The connection through the internet makes it prone to attacks from the outside. Therefore, the connection must fulfill the requirements of <<secrecy>>, <<integrity>> and <<identifiable>>.

The Data Owner has sovereignty over its data. The Data Owner can decide who gets access to the data and thus receives the <<abac>> annotation. The Data Provider and Data Consumer must present their <<abacAttribute>> upon exchanging data. If the attributes do not fulfill the requirements, the transaction is cancelled. One identity can have several attributes. The DAPS hold dynamic and up-to-date information about the identity and its Connector. The Digital Certificate holds static information about the identity and IP addresses of the Connector. Only if the Data Consumer accepts the Usage Control Policy, is a connection made and the data transferred as per the requirements.

After annotating the UML class diagram with the <<secure dependency>> check, the model was checked using the CARiSMA tool. The CARiSMA check resulted in no errors. No errors mean that there were no issues found, given the default attacker. Providing that the system is implemented as per the underlying models, it would mean that the default UMLsec threat actor cannot breach the annotated security requirements. The result of no errors with the default threat actor does not mean that another threat actor with different capabilities cannot breach the annotated security requirements or carry out attacks. With an exploit kit, an attacker can identify and exploit vulnerabilities in systems, download malware to clients without consent, and manage attacks. According to Symantec (2019), exploit kits are responsible for two-thirds of web activity and contain ten exploits on average. New exploit kits are regularly released, containing both old and new exploits. The BlackHole exploit kit was discovered in 2010 and prevalent until 2013. The kit contained sound rental strategies at a fee from \$50 per day to \$1500 per year (Tuptuk & Hailes, 2018a).



<b>QU4LITY</b>	Project	<b>QU4LITY - Digital Reality in Zero Defect Manufacturing</b>		
	Title	<b>QU4LITY SPT Framework (final version)</b>	Date	<b>28/09/2021</b>
	Del. Code	<b>D3.10</b>	Diss. Level	<b>PU</b>

## 5. Conclusions

The SPT aims to provide cybersecurity, privacy and trust functionalities to industry 4.0 systems. We designed the SPT to be able to cover as many needs from the industry domain as possible, dividing the solutions we offer in different areas of the lifecycle of any system. This way, we have supported tools for design time (covering requirement elicitation, tracking and description, and system modeling), development time (by means of API or components providing services for enhancing the resilience, security and trust of systems) and run-time (for monitoring, protection, etc.). The tools provided so far aimed to cover the bigger needs identified in the project by the use partners but, due to the nature of these systems and how cyberattacks keep progressing, the SPT can be extended with more tools in order to tackle more needs or future technologies. This way, the SPT would be a living platform that would be updated as needed and adapt to the changing landscape.

Although we have worked in the cybersecurity tools of the SPT for covering as much functionalities as possible, we are aware they could be continuously extended in order to support more functionalities and diverse systems. This is one of the more important points, or even critical, for us, because we are aware that usually these types of systems are distributed, large, composed of different technologies, etc. so the refinement is not only in terms of functionality but also to accommodate or adapt to different architectures. As an example, the component for data protection could be adapted to new or old technologies as depending on the system that wants to use it. This could all be provided as a single component but with different specializations.

Another important aspect we found when working in the area of cybersecurity in this project was about how to better provide the information to the users. Cybersecurity is as critical for a system as complex for understanding, as there is a minimum level of knowledge necessary for being able to know about what is happening in a system. We aimed to cover this from the design point of view and the output the solutions provide, as it is very important to be able to adapt the information, resources and output as much as possible to people with a low level of understanding of cybersecurity. Still, we think this is a work in progress and there is room for improvement for adapting better the functionality and results of the tools to users.



QU4LITY	Project	QU4LITY - Digital Reality in Zero Defect Manufacturing		
	Title	QU4LITY SPT Framework (final version)	Date	28/09/2021
	Del. Code	D3.10	Diss. Level	PU

## Partners

