Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

Deliverable 4.1

'Requirement Model'

Project Name: **Digitalising European Uncontested Claims Enforcement**

Grant Agreement No.: **101138437**

Call: **JUST-2023-JCOO**

Start date of the project: **1 April 2024**

Duration of the project: **24 months**

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

DEUCE Consortium Disclaimer

The DEUCE consortium consists of the following partners:

No.	Role	Short Name	Legal Name	Country
1	COO	VUB	VRIJE UNIVERSITEIT BRUSSEL	BE
2	BEN	UL	UNIVERZA V LJUBLJANI	SI
3	BEN	VU	VILNIAUS UNIVERSITETAS	LT
4	BEN	UniZg	SVEUCILISTE U ZAGREBU – PRAVNI FAKULTET	HR
5	BEN	UNINA	UNIVERSITA DEGLI STUDI DI NAPOLI FEDERICO II	IT
6	BEN	UB	UNIVERSITAT DE BARCELONA	ES
7	BEN	TalTech	TALLINNA TEHNIKAÜLIKOOL	EE
8	BEN	Adiconsum	ASSOCIAZIONE ITALIANA DIFESA CONSUMATORI ED AMBIENTE	IT
9	BEN	EUBF	FONDATION DE LA CHAMBRE EUROPEENNE DES HUISSIERS DE JUSTICE	BE
10	BEN	FBE	FEDERATION DES BARREAUX D'EUROPE	FR
11	BEN	ZEV	ZENTRUM FUR EUROPAISCHEN VERBRAUCHERSCHUTZ EV	DE

Document Information

Project short name and number	DEUCE (**101138437**)
Work package	4
Number	D4.1
Title	Requirement Model
Type[1]	R

[1]**Types.R:** Document, report (excluding the periodic and final reports); **DEM:** Demonstrator, pilot, prototype, plan designs; **DEC:** Websites, patents filing, press & media actions, videos, etc.; **OTHER:** Software, technical diagram, etc.

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

Dissemination level[2]	SEN
Contractual date of delivery	31.05.2024

Document History

Version	Date	Status	Authors, Reviewers	Description
v 0.01	25.03.2024	Template	A: Sajedeh Salehi [VUB]	Project deliverable template
v 0.02	27.05.2024	Draft	A: Oleksii Kharkov [TalTech] R: Artem Boyarchuk [TalTech]	Initial general description and scope
v 0.03	30.05.2024	Draft	A: Oleksii Kharkov [TalTech] R: Artem Boyarchuk [TalTech]	Detailed and fixed procedure
v 0.04	30.05.2024	Draft	A: Artem Boyarchuk [TalTech] R: Thomas Hoffmann [TalTech]	Minor corrections
v 1.0	31.05.2024	Draft	A: Thomas Hoffmann R: Marco Giacalone	Final Revision

[2]**Dissemination levels:** Public — fully open (e.g. web); Sensitive — limited under the conditions of the Grant Agreement; EU classified — RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444.

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

Table of Content

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

List of Figures

Index of tables

Co-funded by
the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

1. Background to the DEUCE project

DEUCE will rely on the successful results obtained within the previous three projects managed by the Consortium: SCAN (2018-2020, JUST-JCOO-AG-2017), EFFORTS (2020-2022, JUST-JCOO-AG-2019) and SCAN II (2018-2021, JUST-JCOO-AG-2017). In its activities, DEUCE will significantly benefit from SCAN II and EFFORTS databases (the former for ESCP Regulation and the latter for EEO and EOP guidelines), from SCAN experience for what concerns surveys and interviews for the creation of the comprehensive Roadmap as well as from the strong and supportive network of various stakeholders (i.e., ECC-Nets, legal practitioners, academics). From a methodological perspective, the synergic collaboration among the legal unit partners in conducting a plethora of research activities and hands-on tasks is demonstrated by the successful outputs achieved in the above-mentioned projects. Furthermore, DEUCE's objectives complement and support the EU-LISA widespread efforts to digitalize EU Justice. Currently the front-runner Agency in managing large-scale IT systems, EU-LISA's core activity consists of interoperability, namely the efficient communication and cooperation of IT systems to provide EU law enforcement officials with quicker access to comprehensive information and to improve cross border judicial cooperation. Hence, by promoting the use of EEO and EOP procedures, which offer simplified instruments for the recovery of monetary claims, DEUCE will enable the development of a favorable environment for the large-scale adoption of the e-CODEX Project, now being incorporated into the EU-LISA framework. The envisaged result thus consists of the implementation of an interoperable, secure and decentralised communication network between national IT systems in cross-border civil and criminal proceedings.

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

2. User Requirements Specification

2.1. Purpose

The purpose of the document is to gather and specify requirements and constraints on the planned set of products. Namely - the document is intended to be read by stakeholders, production team and contracting companies.

System Requirement Model is documentation, which presents the features and functionality of the software system under design. For this purpose, the system is considered as a "white box" – i.e., system with full details of its internal components and their interaction. For the System Requirement Model the system designers develop the context diagrams, use case diagrams followed by use case description and specific requirements.

2.2. Scope

Using the document, a set of products will be produced hereinafter referred as DEUCE platform.

The proposed software platform should allow to file and resolve small claims across the European Union. It should allow users to easily submit a small claim and get a legally binding resolution.

2.3. Legal framework

DEUCE is a project concerned with Regulation on European Enforcement Order for uncontested claims (EEO - Regulation No. 805/2004) and the Regulation on European Order for Payment Procedure (EOP - Regulation No. 1896/2006). The EEO Regulation introduced the most significant innovation in the field of European judicial cooperation since the adoption of the Brussels Convention in 1968.

2.4. Definitions, acronyms, and abbreviations

- DEUCE - Digitising European Uncontested Claims Enforcement;
- EEO - European Enforcement Order;
- EOP - European Order for Payment.

2.5. Modal verbs (RFC 2119)

1. MUST– This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.
2. MUST NOT –This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
3. SHOULD – This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full

implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT – This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the behavior is acceptable or even useful, but the full implications should be understood, and the case carefully weighed before implementing any behavior described with this label.

5. MAY– This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

2.6. Overview

The document describes logical and physical constraints and requirements for the system alongside with vision of application, scalability, maintenance and after production improvements.

The document is structured in the following way: the first half is a general description which contains different sights and constraints of the problem, and the second one describes specific constraints which are separated into distinct categories.

In this document system is viewed as a black box, where it's internals are obscured and deliberately omitted.

2.7. General requirements

2.7.1. Product perspective

In its activities, DEUCE will significantly benefit from EFFORTS databases (the former for ESCP Regulation and the latter for EEO and EOP guidelines), from SCAN experience for what concerns surveys and interviews for the creation of the comprehensive Roadmap as well as from the strong and supportive network of various stakeholders (i.e., ECC-Nets, legal practitioners, academics).

2.7.2. Concerned parties

- TalTech;
- Experts.

2.7.3. User characteristics - actors

- Claimant - end-user submitting claims;
- Defendant - end-user receiving a claim;
- Judge - end-user reviewing a claim;
- Bailiff - end-user, enforcer;
- Operator - maintenance staff;
- System administrator - technical staff;

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

- Governor - administrator of the node.

2.7.4. General constraints

- EEO/EOP;
- System interfaces must be properly specified and easily accessible for integrations to the third parties,
- GDPR. The immutability, public accessibility and the peer to-peer organisational structure of public blockchains may conflict with the principle of data minimisation as well as the data subject's right to be forgotten (Article 17 GDPR), its right to restriction of processing (Article 18 GDPR) and the right to rectification (Article 16 GDPR) (Erbguth 2019). While the platform to be developed in this project does not necessarily need to store personal data, the platform may require some more sophisticated feature in order to render it GDPR-compliant in terms of the subject's right to be forgotten.

2.7.5. Project specific constraints

- Blockchain for verifiability and document anchoring;
- Digital identity system for digital signatures.

2.7.6. Assumptions and dependencies

The system is considered to run on easily accessible hardware. We assume that open specifications are the key to transparency. System must be easily accessible to the broad scope of users, it's external representation should be easily and user-friendly. Protocols used must be open source.

2.8. Specific requirements

2.8.1. Capability requirements

End-user

- UR-CU-0 User must be able to sign up into the system using either combination of mail/password, phone/password;
- UR-CU-1 Claimant must be able to answer questionnaire to determine whether they are eligible for a small claim application;
- UR-CU-2 Claimant must be able to fill a form detailing small claim (Form A);
- UR-CU-3 Claimant must be able to specify defendant - the subject of the small claim;
- UR-CU-4 Defendant must be notified of the claim submitted to them;
- UR-CU-5 Defendant must be able to respond to a claim by filling a form(Form C) or providing free-form response;
- UR-CU-6 Defendant should be able to submit counterclaim;
- UR-CU-7 Judge must be able to review submitted claim before accepting it;

- UR-CU-8 Judge should be able to rule in favor of claimant if defendant fails to respond in specified time frame (30 days);
- UR-CU-9 Claimant and Defendant should be able to request testimonies from the witnesses;
- UR-CU-10 Judge should be able to review witness statements;
- UR-CU-11 Claimant and defendant may be able to request assistance from a lawyers;
- UR-CU-12 Claimant and defendant may be able to connect with lawyer utilizing video conferencing software;
- UR-CU-13 Users must be able to prove their actions with digital signatures;
- UR-CU-14 Users must be able to verify digital signature authenticity on a document, form etc.;
- UR-CU-15 Claimant and defendant may be able to request a hearing;
- UR-CU-16 Users may be able to receive a translated version of a claim, response, counterclaim, appeal or ruling;
- UR-CU-17 Claimant and defendant should be able to submit an appeal (Form D);
- UR-CU-18 Bailiff must be able to obtain a ruling from a judge;
- UR-CU-19 Bailiff must be able to verify the authenticity of a ruling obtained;
- UR-CU-20 Judge must be able to issue a European enforcement order for the uncontested claim;
- UR-CU-21 Judge must be able to issue a European order for payment for the uncontested claim;
- UR-CU-22 Defendant must be able to lodge a statement of opposition.

2.8.2. Constraint requirements

Communication interfaces

- UR-CI-1 Communication protocols between external and internal services must be based on IP, TCP, and HTTP;
- UR-CI-2 System must have interfaces based on open standards or conventions;
- UR-CI-3 Communication protocols evolving must not break backwards-compatibility but only for serious reasons like security, efficiency, maintainability.

Hardware

- UR-HA-1 System should be easily accessible using modern Web Browser;
- UR-HA-2 The data center may have a reserve power supply and internet connections to prevent long downtime;
- UR-HA-3 System should have potentiality of implementing all the client facing features on mobile.

Human-computer interaction

- UR-HC-1 The system should have an admin panel application for:

    - (a) staff: system administrators
  - (b) operators
  - (c) governors
- UR-HC-2 The system must provide specialized interface for service users:
  - (a) lawyers
  - (b) bailiffs
  - (c) judges
- UR-HC-3 The system may include reference mobile application implementation.

Availability

- UR-AV-1 95% of all requests must be responded by a server within 5 seconds;
- UR-AV-2 The system must be able to scale during high load (using reserved capacity or service of an external provider for dynamic scaling);
- UR-AV-3 The system should detect and block suspicious traffic and report the analysis to system administrators;
- UR-AV-4 The system must be able to restart its services within 10 minutes;
- UR-AV-5 The system must be able to automatically roll back to the previous version of the software in case of patch failures;
- UR-AV-6 The system should have at least one and maximum half hour old backup at any given time;
- UR-AV-7 The system must be able to process at least 100 transactions per second.

Accessibility

- UR-AD-1 The system should be able to evolve its external and internal protocols;
- UR-AD-2 The system should constantly fix found issues and must prioritize security and safety ones, i.e., system should be able to change the configuration during execution in response to the predefined sequence of events;
- UR-AD-3 The system should be able to scale horizontally in response to high load (e.g., for every 1000 requests per second, launch additional instances).

Portability

- UR-P-1 Communication protocol specifications must be platform independent;
- UR-P-2 The development team may provide adaptors or native versions of the library in other languages or OS.

Security

- UR-SE-1 The system must support cryptographic signatures;
- UR-SE-2 The system must grant access to account management to end-user based on the combination of login and password;
- UR-SE-3 The system should provide an option of 2FA to end-user;
- UR-SE-4 The system must use existing cryptographic standards of European Union to secure transactions and other operations within the system.

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

Safety

- UR-SA-1 The system may support "trash can" feature to prevent accidental removal of important data.

2.9. Glossary

Need:

- must;
- should;
- may.

Priority:

- highest;
- high;
- medium;
- low;
- lowest.

Stability:

- stable;
- unstable.

Source:

- Concerned parties
- General constraints

Clarity:

- clear;
- unclear.

Verifiability:

- verifiable;
- non-verifiable.

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

3. Software Requirements Specification

3.1. Introduction

3.1.1. Purpose

The purpose of this section is to analyze the requirements and constraints stated in the user requirements section and produce coherent software requirements.

Software requirements are constructed by:

- Examining the user requirements;
- Building logical model.

Software requirements specify:

- Functionality;
- Performance;
- Interfaces;
- Quality;
- Reliability;
- Maintainability;
- Safety.

Methods used at this stage include, but not limited to:

- Functional decomposition;
- Structured analysis;
- Dependency analysis;
- Interface decoupling;
- Loose coupling of logical components.

3.2. General description

3.2.1. Relation to other systems

DEUCE will rely on the successful results obtained within the previous three projects managed by the Consortium: SCAN (2018-2020, JUST-JCOO-AG-2017), EFFORTS (2020 2022, JUST-JCOO-AG-2019) and SCAN II (2018-2021, JUST-JCOO-AG-2017). In its activities, DEUCE will significantly benefit from SCAN II and EFFORTS databases (the former for ESCP Regulation and the latter for EEO and EOP guidelines), from SCAN experience for what concerns surveys and interviews for the creation of the comprehensive Roadmap as well as from the strong and supportive network of various stakeholders (i.e., ECC-Nets, legal practitioners, academics). From a methodological perspective, the synergic collaboration among the legal unit partners in conducting many research activities and hands-on tasks is shown by the successful outputs achieved in the above-mentioned projects. Furthermore, DEUCE's objectives complement and support the EU-LISA widespread efforts to digitalise EU Justice. Currently the front-runner Agency in managing large-scale IT systems, EU-LISA's core activity consists of

interoperability, namely the efficient communication and cooperation of IT systems to provide EU law enforcement officials with quicker access to comprehensive information and to improve cross border judicial cooperation. Hence, by promoting the use of EEO and EOP procedures, which offer simplified instruments for the recovery of monetary claims, DEUCE will enable the development of a favourable environment for the large-scale adoption of the e-CODEX Project, now being incorporated into the EU-LISA framework. The envisaged result thus consists of the implementation of an interoperable, secure and decentralized communication network between national IT systems in cross-border civil and criminal proceedings.

3.2.2. Environmental considerations

DEUCE has a potentiality of simplifying processes, which benefits environment.

One more aspect must not be overlooked. Often, blockchain technology is equated with cryptocurrency. Obviously, it's not the case. To say more, blockchain is considered by be harmful for the environment, as one of the most famous cryptocurrencies - Bitcoin - utilizes a so-called Proof-of-Work consensus algorithm, which leads to Bitcoin network to consume a substantial amount of energy.

There exist a number of consensus algorithm for blockchain nodes, and in DEUCE projects we would most possibly move in a direction of Federated consensus algorithms. Federated consensus algorithms do not require nodes to solve complex problems, thus do not require massive computation.

To conclude, DEUCE would most possibly benefit environment by simplifying paper-based processes.

3.2.3. Role of blockchain in DEUCE platform

The role of blockchain in the DEUCE project is straightforward.

One of the aspects integrating blockchain into any project is to define clearly set of goals set to be met. Blockchain should not be equated with:

- Digital currency;
- Distributed network of nodes;
- Digital identity system.

Blockchain is a way to store data in a chain of so-called blocks. It could be beneficial, if data to be stored should not be manipulated and should not be changed later. Blockchain itself is not enough to prevent said manipulation. That is where cryptographic signatures come to life, since they allow to supplement blocks and data stored in blocks with signatures, which would allow to prove authenticity of data. Distributed network of blockchain nodes would also be beneficial, since it would allow to implement data redundancy and have complex sync algorithms, which here and after would be referred to as *consensus algorithms.*

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

Consensus algorithm's role is to ensure that nodes can agree on some value, in case of blockchain – on the next block.

There exist several consensus algorithms, which are suitable for different purposes. In case of DEUCE, federated consensus algorithms are among few to consider.

3.2.4. Model description

This section deals with logical model of the system, when logical components assigned abstract responsibilities and their concrete behavior is not considered.

This section presents context diagram – diagram in which system's usage is presented on high level.

Use case diagram and use cases description provide more detailed step by step view of its capabilities.

3.2.4.1. Context diagram

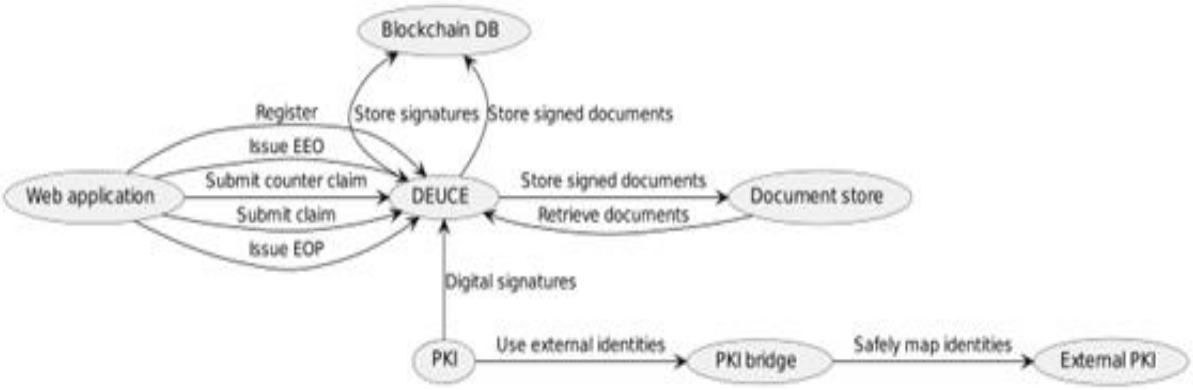

Figure 1.1: DEUCE context diagram

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

3.2.4.2. Use case diagram

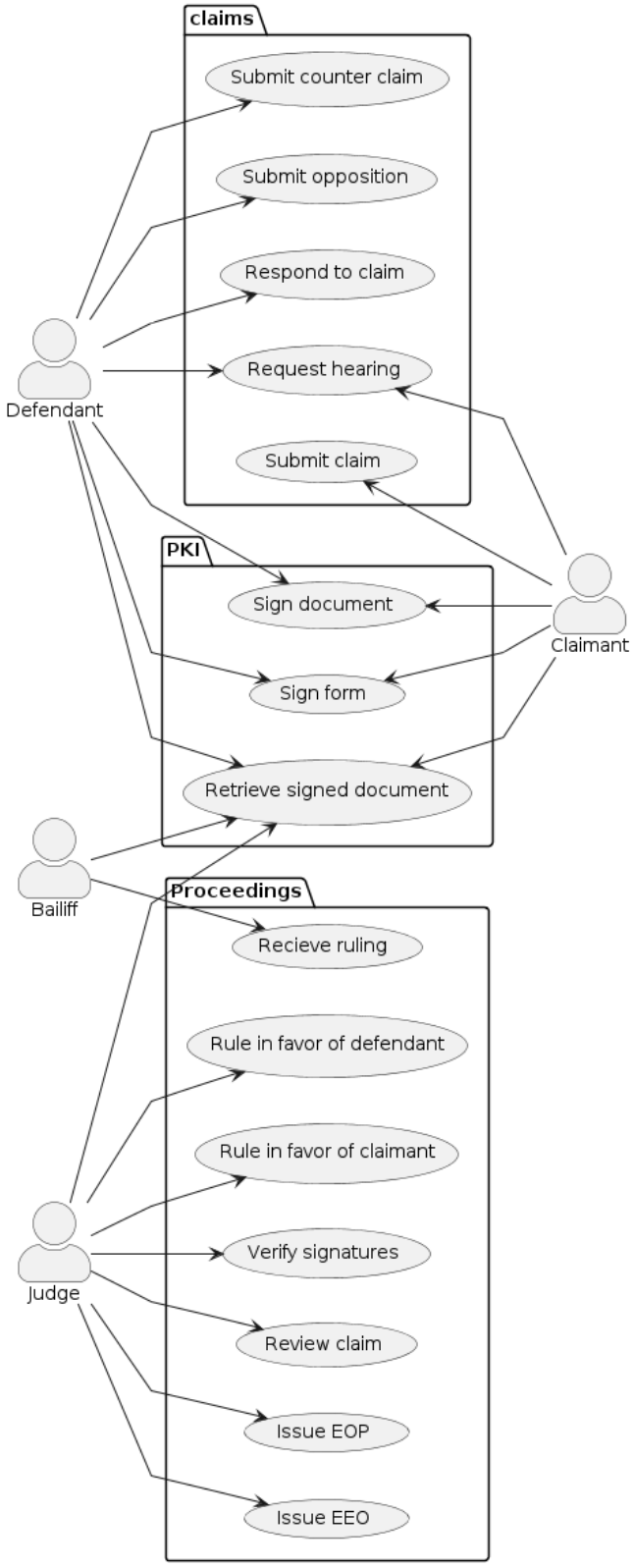

Figure 3.2: DEUCE use case diagram

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

3.2.4.3. Use cases description

Use Case: Register (Create account)	
Actors	Claimant, Defendant
Pre-conditions	None
Optimistic Flow of Events	1. User undergoes authentication using one combination of login and password. Login can be one of the following: - Email - Phone number 2. System checks for prior account existence with the provided login 3. Account with provided login does not exist 4. System requests login confirmation and sends OTP via: - SMS to the provided phone number - Letter via email 5. User confirms phone or email 6. User's account is created in the system 7. Keypair is generated and securely stored
Conditional Flows	3. Account with provided login exists 4. User is redirected to "Account restore" page
Post-conditions	*Optimistic:* Account created *Conditional: None*

Table 3.1: Use case "Register (Create account)"

Use Case: Log in	
Actors	Claimant, Defendant, Judge, Bailiff, System Administrator, Operator
Pre-conditions	Account created.
Optimistic Flow of Events	1. User enters login and password 2. System verifies existence of the user with provided login 3. System verifies password is correct

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

	4. User has signed in
Conditional Flows	**Login is incorrect** 2. Account with provided login does not exist. 3. User is prompted to check login or register in the system **Password is incorrect** 3. Password is incorrect 4. System prompts user to undergo account restoration
Post-conditions	*Optimistic: User signed in.* *Conditional: None*

Table 3.2: Use case "Login"

Use Case: Restore account	
Actors	Claimant, Defendant
Pre-conditions	Incorrect password entered, access to the account lost
Optimistic Flow of Events	1. User enters login for their account 2. System verifies that account with provided login exists 3. System sends an OTP to the phone or email of the user. 4. User enters OTP 5. User is prompted for a new password 6. User enters and submits new password
Conditional Flows	4. User does not enter OTP 5. System prompts user to try again
Post-conditions	*Optimistic: Account restored* *Conditional: Account not restored*

Table 3.3: Use case "Restore account"

Use Case: Submit claim	
Actors	Claimant
Pre-conditions	Log-in; User wants to submit a claim

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

Optimistic Flow of Events	1. User answers to the questionnaire about her claim. 2. System determines user is eligible to submit a claim based on questionnaire. 3. User is presented with Form A filled based on her answers. 4. User is offered to review & edit form in case of errors. 5. User is prompted to sign the form. 6. User signs the form. 7. Form is stored in document store and forwarded to a judge 8. Signature details are stored in the blockchain DB.
Conditional Flows	**Not eligible for a claim** 2. System determines user is not eligible for a claim. 3. User is notified
Post-conditions	*Optimistic: Claim submitted, Form signed, signed form is securely stored, defendant and judge are notified of the claim* *Conditional: None*

Table 3.4: Use case "Submit claim"

Use Case: Submit counter claim	
Actors	Defendant
Pre-conditions	Log-in; User wants to submit a counter claim
Optimistic Flow of Events	1. User answers to the questionnaire about their claim. 2. System determines user is eligible to submit a counter claim based on questionnaire and claim submitted. 3. User is presented with Form C filled based on their answers. 4. User is offered to review & edit form in case of errors. 5. User is prompted to sign the form. 6. User signs the form with their keypair 7. Form is stored in document store and

	forwarded to a judge 8. Signature details are stored in the blockchain DB.
Conditional Flows	**Not eligible for a claim** 2. System determines user is not eligible for a counter claim. 3. User is offered to agree to claim
Post-conditions	*Optimistic: Counter claim submitted, Form signed, signed form is securely stored, claimant and judge are notified of the claim* *Conditional: None*

Table 3.5: Use case "Submit counter claim"

Use Case: Accept claim	
Actors	Defendant
Pre-conditions	Log-in; Defendant wants to
Optimistic Flow of Events	1. User accepts the claim 2. User is presented with Form C to fill. 3. User is prompted to sign the form. 4. User signs the form with their keypair 5. Form is stored in document store and forwarded to a judge 6. Signature details are stored in the blockchain DB.
Conditional Flows	None
Post-conditions	*Optimistic: Response submitted* *Conditional: None*

Table 3.6: Use case "Accept claim"

Use Case: Verify signatures	
Actors	Claimant, Defendant, Judge, Bailiff
Pre-conditions	Log in; Signed forms present in the system; User wants to verify authenticity of the document
Optimistic Flow of Events	1. User wants to verify authenticity of a document or a form.

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

	2. User is prompted to retrieve signature from the blockchain DB and compare it with the one of the documents. 3. Signature is verified and user is prompted with notification of authenticity.
Conditional Flows	3. Signature is invalid. 4. User is notified of invalid signature 5. Document or form is flagged as corrupted or invalid 6. Source of the document is notified of invalid signature
Post-conditions	*Optimistic: Signature is verified* *Conditional: Document is flagged as having invalid signature, source of the document is notified*

Table 3.7: Use case "Verify signatures"

Use Case: Verify signatures (Implicitly)	
Actors	Claimant, Defendant, Judge, Bailiff
Pre-conditions	Log in; Signed forms present in the system; User wants to verify authenticity of the document
Optimistic Flow of Events	1. User wants to verify authenticity of a document or a form. 2. Signature is verified. 3. Pictogram indicating document is authentic is displayed near the document
Conditional Flows	2. Signature is invalid. 3. Pictogram and warning indicating document signature is invalid are displayed near the document
Post-conditions	*Optimistic: Signature is verified.* *Conditional: Document is flagged as having invalid signature, source of the document is notified.*

Table 3.8: Use case "Verify signatures (Implicitly)"

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

Use Case: Review claim	
Actors	Judge
Pre-conditions	Log-in; Claim submitted in the system; Judge's authority is suitable to review the claim
Optimistic Flow of Events	1. User is notified of the pending claim 2. User reviews the claim and associated documents 3. User approves to proceed with the claim
Conditional Flows	3. Claim is rejected
Post-conditions	*Optimistic: Claim is reviewed and approved by a judge* *Conditional: Claim is rejected, claimant is notified*

Table 3.9: Use case "Review claim"

Use Case: Issue European order for payment procedure	
Actors	Judge
Pre-conditions	Log-in; Claim submitted in the system; Judge's authority is suitable to review the claim; Claim is uncontested; European Enforcement Order issued;
Optimistic Flow of Events	1. User is notified of the pending claim 2. User reviews the claim and associated documents 3. User reviews the enforcement order 4. User issues order for payment procedure
Conditional Flows	3. Claim is rejected
Post-conditions	*Optimistic: Order for payment procedure is issued* *Conditional: Claim is rejected, claimant is notified*

Table 3.10: Use case "Issue European order for payment procedure"

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

Use Case: Submit the statement of opposition	
Actors	Defendant
Pre-conditions	Log-in; Claim submitted in the system; Claim is uncontested; European Enforcement Order issued; Order for payment procedure issued
Optimistic Flow of Events	1. User is notified of the pending claim 2. User reviews the claim and associated documents 3. User reviews the enforcement order 4. User issues statement of opposition
Post-conditions	*Optimistic: statement of opposition is submitted*

Table 3.11: Use case "Submit the statement of opposition"

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

3.2.4.4. Logical component diagram

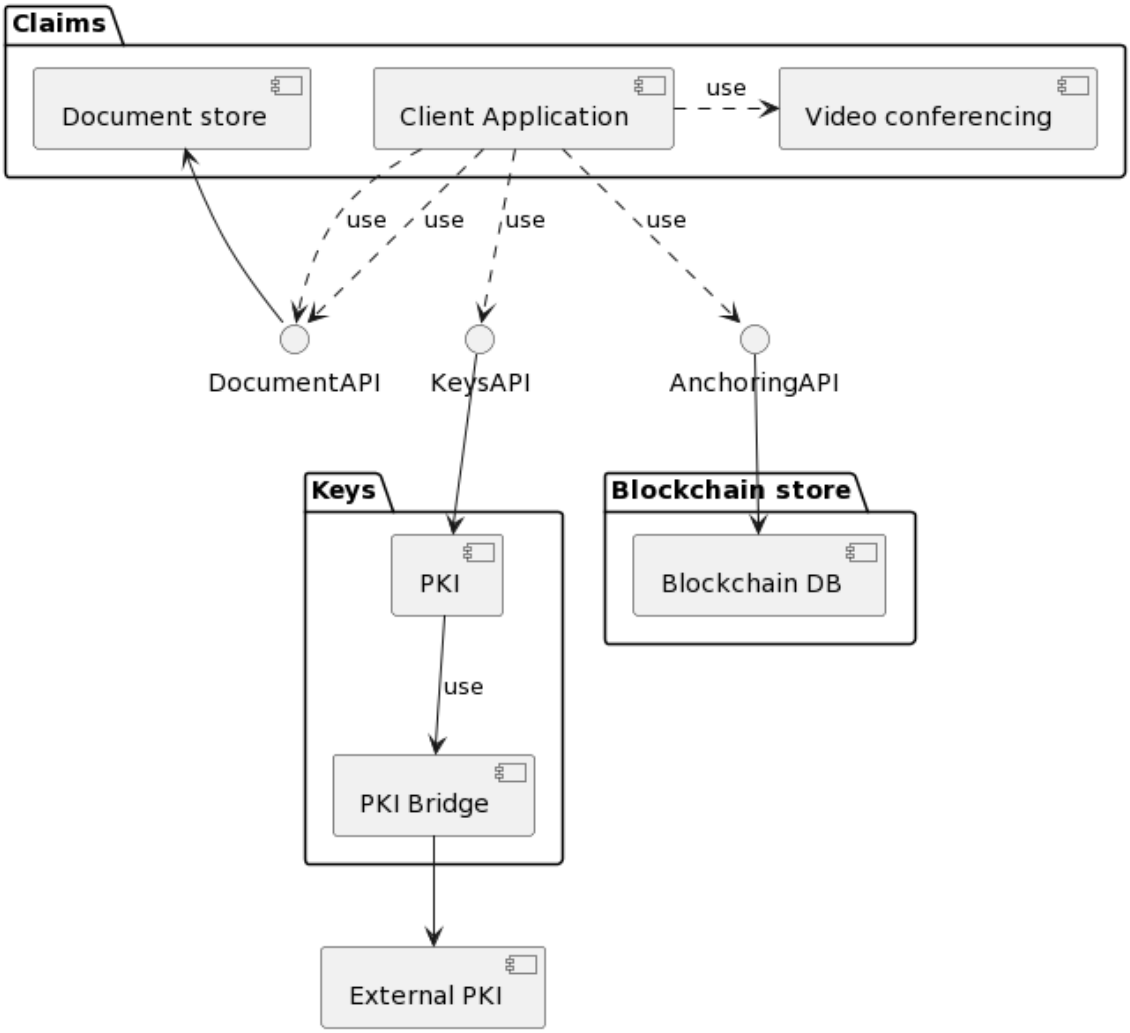

Figure 3.3: DEUCE logical component diagram

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

3.3. Specific requirements

3.3.1. Functional requirements

System:

- SR-FR-1 Must allow claimant & defendant to register in the system;
- SR-FR-2 Must allow users to obtain key-pair on registration;
- SR-FR-3 Must allow claimant & defendant to answer questionnaire about eligibility for claim/counter claim;
- SR-FR-4 Must allow users to sign forms (Form A, Form C, Form D) with their keys;
- SR-FR-5 Must allow judge to review claim;
- SR-FR-6 Must allow judge to accept claim;
- SR-FR-7 Must allow judge to reject the claim;
- SR-FR-8 Must allow to store the signed documents;
- SR-FR-9 Must allow to verify signature on the document submitted;
- SR-FR-10 Must allow to notify user of their invalid signature on the document;
- SR-FR-11 Must allow users to see the who signed the document;
- SR-FR-12 Must allow to restore account;
- SR-FR-13 Must allow operator to register special account for judges and bailiffs;
- SR-FR-14 Must allow to block or restrict users;
- SR-FR-15 Should allow to bind external identity to the account (see chapter on external identities);
- SR-FR-16 Should allow to sign a document with external keys;
- SR-FR-17 Should allow to verify external signature;
- SR-FR-18 Must allow users to submit documents along with the forms;
- SR-FR-19 Must allow users to sign documents uploaded;
- SR-FR-20 Must allow claimant & defendant to fill and submit forms;
- SR-FR-21 Must notify users of their involvement in any action - claim or counterclaim submitted;
- SR-FR-22 Must allow judge to rule in favor of claimant;
- SR-FR-23 Must allow judge to rule in favor of defendant;
- SR-FR-24 Must allow bailiff to receive ruling from a judge;
- SR-FR-25 Should allow registered users to contact each other via embedded video conferencing software;
- SR-FR-26 Must allow judge to issue a European enforcement order for the uncontested claim;
- SR-FR-27 Must allow judge to issue a European order for payment for the uncontested claim;
- SR-FR-28 Must allow defendant to lodge a statement of opposition;
- SR-FR-29 Must allow claimant to request a hearing;
- SR-FR-30 Must allow defendant to request a hearing.

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

3.3.2. Performance requirements

- SR-PR-1 Blockchain store should be able to tolerate up to 1000 transactions per minute;
- SR-PR-2 In case of events requiring attention of users, notifications should be dispatched in a less than a minute;
- SR-PR-3 Document store should be able to return the document in less than 30 seconds;
- SR-PR-4 Incremental backups of critical data should be made at least hourly.

3.3.3. Interface requirements

- SR-IR-1 Basic communication protocol is IP;
- SR-IR-2 System components must use gRPC or REST, depending on the context.

3.3.4. Operational requirements

- SR-OP-1 DEUCE web application should allow user to perform the following operations:
  (a) register;
  (b) sign in;
  (c) submit claim;
  (d) submit counter claim;
  (e) accept claim;
  (f) reject claim;
  (g) verify authenticity of the document/form;
  (h) verify signature of the document;
  (i) restore account;
  (j) request hearing;
  (k) submit opposition (defendant only).

- SR-OP-2 DEUCE privileged user application should allow user - judge, to perform the following operations:
  a) sign in;
  b) review claim;
  c) reject claim;
  d) accept claim as valid;
  e) rule in favour of claimant;
  f) rule in favour of defendant;
  g) restore account;
  h) verify authenticity of the document/form;
  i) verify signature of the document;
  j) issue enforcement order;

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

k) issue order for payment procedure.

- SR-OP-3 DEUCE privileged user application should allow user - bailiff, to perform the following operations:
  (a) review ruling;
  (b) verify authenticity of the document/form;
  (c) verify signature of the document/form;
  (d) restore account.

- SR-OP-4 DEUCE admin user application should allow user to perform following operations:
  (a) sign in;
  (b) create account for judge;
  (c) create account for bailiff;
  (d) restrict user account;
  (e) block user's account;
  (f) restore user's account.

3.3.5. Resource requirements

- SR-RR-1 Client web applications must be able to run in modern-day web browsers;
- SR-RR-2 Server-side components must be able to run on generic hardware.

3.3.6. Verification requirements

- SR-VR-1 Public interface functions must be covered with unit tests;
- SR-VR-2 Every module or class must be covered with integration test;
- SR-VR-3 Every software part (client application, document store etc. must have tests for critical paths - user-data sensible operations, hot paths, integrity testing;
- SR-VR-4 System should be able to withstand stress test with increased traffic;
- SR-VR-5 Fuzzy testing may be used to ensure corner cases for critical functions are being processed as expected.

3.3.7. Documentation requirements

- SR-DR-1 Should be written with the consideration that readers might not have technical background;
- SR-DR-2 Should contain all the technical details of inner system processes;
- SR-DR-3 Should contain information regarding system administration;
- SR-DR-4 Should contain information on system diagnostics methods;
- SR-DR-5 Should contain information on system manual and automatic scaling;
- SR-DR-6 Must contain information on system extensibility;

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

- SR-DR-7 Must contain information on system configuration & deployment.

3.3.8. Security requirements

- SR-SCR-1 System should be able to withstand data loss (redundancy should be in place);
- SR-SCR-2 System may restart failed components automatically;
- SR-SCR-3 System should have capabilities to ban suspicious users;
- SR-SCR-4 System administrators should be able to temporarily restrict or ban users.

3.3.9. Portability requirements

- SR-POR-1 System server-side software should be able to run on Linux based operating systems;
- SR-POR-2 Web application should be accessible and usable on any modern web browser;
- SR-POR-3 Web application should be able to run on HTML5, CSS3, ECMAScript 5 compatible browsers.

3.3.10. Quality requirements

- SR-QR-1 External project dependencies should be clearly defined and inspected for system vulnerabilities;
- SR-QR-2 Occasional audits of development process & deliverables should be performed.

3.3.11. Reliability requirements

- SR-RELR-1 System continuous downtime should not exceed 2 hours;
- SR-RELR-2 Fallback to older versions of software should be available in case of dormant (undiscovered) issues.

3.3.12. Maintainability requirements

- SR-MR-1 Average time to repair the system should not exceed 4 hours;
- SR-MR-2 System's components should be decoupled from one another for easier maintainability.

3.3.13. Safety requirements

- SR-SFR-1 Committed data must not be lost in case of incidents;
- SR-SFR-2 User data should be stored securely, i.e. sensitive information should be encrypted;
- SR-SFR-3 User data should be stored in a redundant way.

3.3.14. Safety requirements

To be defined in the coming phases.

3.4. Traceability matrix

The purpose of traceability matrix is to map specific capability requirements to one or more software requirements.

Some of the user requirements cannot be transformed to software requirements. Some of them are concerned with the system configuration, deployment, administration etc., i.e. - a certain part of user requirements cannot be defined in terms of software requirements.

URD identifier	SRD identifier
UR-CU-0	SR-FR-1
UR-CU-1	SR-FR-3
UR-CU-2	SR-FR-20
UR-CU-3	SR-FR-20
UR-CU-4	SR-FR-21
UR-CU-5	SR-FR-4, SR-FR-20
UR-CU-6	SR-FR-20
UR-CU-7	SR-FR-5
UR-CU-8	SR-FR-22, SR-FR-23
UR-CU-9	-
UR-CU-10	-
UR-CU-11	-
UR-CU-12	-
UR-CU-13	SR-FR-4, SR-FR-8, SR-FR-9, SR-FR-10, SR-FR-11, SR-FR-15, SR-FR-16, SR-FR-17, SR-FR-19
UR-CU-14	SR-FR-9, SR-FR-11, SR-FR-17
UR-CU-15	-
UR-CU-16	-
UR-CU-17	SR-FR-25
UR-CU-18	SR-FR-24
UR-CU-19	SR-FR-9, SR-FR-11, SR-FR-17
UR-CU-20	SR-FR-26
UR-CU-21	SR-FR-27

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

UR-CU-22	SR-FR-28
UR-CI-1	SR-IR-1
UR-CI-2	SR-IR-2
UR-CI-3	-
UR-CI-4	SR-RR-1
UR-HA-1	-
UR-HA-2	-
UR-HA-3	SR-OP-4
UR-HC-1	SR-OP-2, SR-OP-3
UR-HC-2	-
UR-HC-2	-
UR-AV-1	-
UR-AV-2	-
UR-AV-3	-
UR-AV-4	SR-RELR-2
UR-AV-5	SR-SFR-2, SR-SFR-3
UR-AV-6	-
UR-AV-7	-
UR-AD-1	SR-SCR-2
UR-AD-2	-
UR-AD-3	-
UR-P-1	-
UR-P-2	-
UR-SE-1	-
UR-SE-2	-
UR-SE-3	-
UR-SE-4	-
UR-SA-1	-

Table 3.12: SR Traceability matrix

Co-funded by the European Union

'Funded by the European Union. Views and opinions expressed are however those of the author (s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.'

Conclusions

The aim of the deliverable 4.1. is to develop and analyze the set of system and operation requirements to be implemented by the DEUCE platform. For this purpose, System Requirement Model is considered as documentation, which presents the features and functionality of the software system under design. For the System Requirement Model the system designers develop the context diagrams, use case diagrams followed by use case description and specific requirements.

The document is structured in the following way: the first half is a general description which contains different sights and constraints of the problem, and the second one describes specific constraints which are separated into distinct categories.

The document is concluded with the traceability matrix. The purpose of traceability matrix is to map specific capability requirements to one or more software requirements.

References

1. Ashby, Ross W. 1956. An Introduction to Cybernetics. London: Chapman and Hall.

2. Erbguth, Jorn. 2019. Five ways to GDPR-compliant use of blockchains. European Data Protection Law Review (EDPL), 5(3), 427-433.

3. Gramoli, Vincent. 2020. From blockchain consensus back to Byzantine consensus. Future Generation Computer Systems, 107, 760-769.