Privacy & Us

Requirements Analysis

Deliverable Number	D2.1
Work Package	WP 2
Version	1.0
Deliverable Lead Organisation	VDS
Dissemination Level	Public
Contractual Date of Delivery (release)	31/05/2017
Date of Delivery	31/05/2017
Status	**Final**

Editor

Steven Murdoch (VDS)

Contributors

Poornigha Santhana Kumar (USE), Majid Hatamian (GUF), Juan Quintero (UNI), Lamya Abdullah (UNI), Alexandros Mittos (UCL), Andreas Gutmann (VDS), Tom De Wasch (VDS)

Reviewers

Emiliano De Cristofaro (UCL), Leonardo Martucci (KAU)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675730.

European Commission

Abstract

This deliverable summarises the initial results of ESR projects towards the development of technological artefacts that aim at increasing individuals' information privacy. The objective of these technological artefacts is to transfer the theoretical contributions from the different work packages to practice.

This report presents the results of the requirements analysis stage of initial development, following the Agile methodology and presented as User Stories. These analyses were contributed by the ESRs who will be developing technological artefacts – ESRs 4, 5, 7, 10, 11, and 13.

These User Stories show that the user is central to the design of the technological artefacts. In particular, users must have control over how their personal data is processed, and that processing is transparent to the user. The way in which this goal is achieved varies depending on which is the most appropriate approach for the technological artefact in question, taking into account economic incentives involved.

Table of Contents

1 Introduction

One of the major objectives of Privacy&Us is to transfer theoretical contributions from the different work packages to practice by producing different kinds of technological artefacts that aim at increasing individuals' information privacy. The main purpose of these technological artefacts is to demonstrate the validity and utility of the developed models and theories that come from different work packages. Therefore WP2, for which this document is the first report, will produce technological artefacts with different degrees of maturity and will not necessarily be full-functioning, market-ready tools, e.g. methods or algorithms will be developed to support the implementation of privacy technologies, software-based mock-ups will be designed to perform early-stage evaluations of concepts, prototypes will be developed to evaluate usefulness, usability, validity, and utility of specific aspects of theories, while proof of concepts will be close-to-market implementations of multi-facetted privacy tools.

In this report, the initial results of the development of these technological artefacts is provided, specifically the requirements analysis stage. These analyses were contributed by the ESRs who will be developing technological artefacts – ESRs 4, 5, 7, 10, 11, and 13. ESR 9 (TAU) is no longer included in WP2 as initially planned because in order to best contribute to her career development and to allow the project to best utilize her skills, the project plan will not develop a technological artefact. The revised project (Reframing Informed Consent in Information Privacy Law Through Behavioral Economics and the Paternalism-Libertarianism Spectrum) will instead use legal theory, concepts from behavioral economics and political economy, and comparative analysis with other fields, to analyze shortcomings in the validity and effectivity of the informed consent requirement in American and European Law, and explore suitable tools available to remedy or mitigate those shortcomings.

Following this report will be a more detailed final description of the technological artifacts (D2.2, month 24) and the final report of WP2 providing details about the validity and utility of the individual technological artifacts (D2.3, month 44).

1.1 Glossary of Acronyms / Abbreviations

ESR – Early Stage Researcher
WP – Work Package

2 Requirements Analysis

So as to facilitate the continual development of technological artefact design, based on new research results, and to familiarize ESRs with the latest development methodologies, requirements analysis has been performed following the Agile process [1][2]. Here, each requirement is tracked on a *User Story* "card" listing a *Story Narrative* that motivates the requirement, and *Acceptance Criteria* to identify properties that must be met for the requirement to be met. Each User Story is categorized by priority (maybe, could, should, must) depending on how critical this User Story is to the functioning of the technological artefact. The User Story complexity is also categorized by complexity: a "story" level requirement can be implemented without refinement; an "epic" will be split into multiple stories at a later stage of development; a "theme" will be used for grouping multiple user stories.

2.1 ESR4 (USE) Designing for Privacy & Security at Point of Sale Commercial Transactions

Technological artefact: A model for designing secure experiences in hybrid-commercial transactions
ESR: 4 – Poornigha Santhana Kumar (USE)

The research of ESR 4 is to examine the interplay of privacy and security within point of sale commercial transactions, looking for ways to promote privacy and security within this context. The ESR will investigate how point of sale commercial transactional experiences can be designed with interactive hybrid (which combine mobile tech with human/machine interfaces) elements to increase privacy, safety and security for these transactions. The design of "Secure Experiences" is assumed to be based upon the combination of technology (i.e. mobile-networked devices) and human factors with regards to commercial transactions. The technological artefact being developed is an experimental

platform for conducting experiments on hybrid commercial transactions, consisting of a payment terminal and NFC mobile device to assist in the development and validation of best practice models for designing scalable, robust and secure interfaces and services for hybrid commercial transactions. This artefact will lead to a commercially viable secure hybrid-experience prototype.

2.1.1 User stories

2.1.1.1 Payment terminal UI – NFC payment

Story Narrative	*Payment terminal UI*	*Priority*	High
As a	user	*Size*	Epic
I want	Easily scan my NFC mobile/card		
So that	The transaction will take place		

[front of card]

Acceptance Criteria	*Payment terminal UI*
Given	A scenario to pay
When	The user decides to pay using NFC card/mobile
Then	The card/mobile should be scanned against the terminal

[Back of card]

2.1.1.2 Payment terminal UI – payment feedback

Story Narrative	*Payment terminal UI*	*Priority*	Medium
As a	user	*Size*	Epic
I want	To receive visual and audio feedback		
So that	I can understand the state of the transaction		

[front of card]

Acceptance Criteria	*Payment terminal UI*
Given	A initiated transaction
When	The user has scanned the NFC card/mobile
Then	The payment terminal should provide visual and audio feedback on the transaction state

[Back of card]

2.1.1.3 Payment terminal UI – transaction end

Story Narrative	*Payment terminal UI*	*Priority*	High
As a	user	*Size*	Epic
I want	To be informed about the end of transaction		
So that	I can know if the transaction is completed successfully or not		

[front of card]

Acceptance Criteria	*Payment terminal UI*
Given	A processed transaction
When	The transaction is complete
Then	The payment terminal should provide visual and audio feedback on if the transaction is successful or not

[Back of card]

2.1.1.4 NFC Mobile UI – transaction list

Story Narrative	*NFC Mobile UI*	*Priority*	Low
As a	user	*Size*	Story
I want	To easily view my transaction list		
So that	I can check/prove my transactions		

[front of card]

Acceptance Criteria	*NFC Mobile UI*
Given	Several completed transactions
When	The user wishes to review the completed transactions
Then	The user should easily be able to navigate to the transaction list

[Back of card]

2.1.1.5 NFC Mobile UI – block card

Story Narrative	*NFC Mobile UI*	*Priority*	High
As a	user	*Size*	story
I want	To easily block my NFC card		
So that	I can prevent misuse of my card		

[front of card]

Acceptance Criteria	*NFC Mobile UI*
Given	Theft of NFC card
When	The user wants to prevent loss of money
Then	The user should easily be able to block the card

[Back of card]

2.1.1.6 NFC Mobile UI – change password

Story Narrative	*NFC Mobile UI*	*Priority*	Medium
As a	user	*Size*	story
I want	To easily change the password of my NFC app		
So that	I can assure that my credentials are safe		

[front of card]

Acceptance Criteria	*NFC Mobile UI*
Given	When the user feels insecure
When	The user wants assure the safety of the credentials
Then	The user should easily be able to change the password of the app

[Back of card]

2.2 ESR5 (GUF) Privacy Indicators in Smartphone Ecosystems

Technological artefact: An instrument to collect and display privacy experience reports in smartphone app ecosystems
ESR: 5 – Majid Hatamian (GUF)

Smartphone apps provide utility to their users by providing personalized and context-sensitive services. To achieve this, smartphone platforms allow these apps to access numerous sensitive resources on the device, such as device information, geolocation data, and user behavior information obtained from sensors. This capability however, poses important risks to user privacy, especially considering that apps do not have an appropriate level of transparency regarding the processing of sensitive information. Consequently smartphone users cannot identify data leakages and assess how their apps impact their privacy. Current privacy indicators in smartphone ecosystems have been shown to be ineffective regarding risk communication. Further, there are no means to help users make informed decisions regarding app selection.

The objective of this research project is to find appropriate ways to inform users about benefits and potential privacy consequences that will allow them to decide between competing applications (apps in app markets). An important aspect to be considered is how information from crowd-sourced comments of other users can help in the decision-making process. Another aspect will be to find ways to understand privacy threats of apps, considering that data-flows and types of data to be processed are becoming more complex. For example, the new types of data that apps today begin to exploit have not been analyzed in depth with respect to the privacy threats associated with them. Examples are behavioral data collected in daily activities, such as switching on devices in the household, or data related to the “quantified-self” paradigm, such as performance data from sports. The project will emphasize the attempt to gain an understanding of aspects, such as the context of app usage and the purpose and functionality of apps when assessing their privacy properties.

The technological artefact that will be developed is mechanisms that a software developer can integrate into a mobile application so that the application satisfied the need of user protection while enabling them to benefit from services dealing with personal information. Those mechanisms will support users on informed decision making (i.e. what information are they offering for which purpose); including an instrument to collect and display experience reports, e.g., in app markets.

2.2.1 User stories

2.2.1.1 Smartphone Scanning

Story Narrative	Smartphone Scanning	*Priority*	must
As a	application developer	*Size*	theme
I want	to implement a tool that is able to constantly monitor data accesses on users' smartphones		
So that	the user will be able to scan and monitor installed apps on smartphone		

front of card

Acceptance Criteria	Smartphone scanning
Given	Installed applications on users' smartphones
When	The data are accessed
Then	The users will be informed about the frequency and details of these accesses

Back of card

2.2.1.2 Log History

Story Narrative	Log history	*Priority*	should
As a	application developer	*Size*	epic
I want	to enable users to store the history of scanned permissions and accesses to their personal data		
So that	the user will be able to compare the functionalities of apps in terms of access to resources		

[front of card]

Acceptance Criteria	Log history
Given	Installed applications on users' smartphones
When	The data are accessed
Then	The users will be to store the details of these accesses on their phones for further investigation

[Back of card]

2.2.1.3 Permission granting

Story Narrative	Permission granting/restriction	Priority	should
As a	application developer	Size	epic
I want	to enable users to grant/limit a specific kind of permission that is aggressively used by an app		
So that	the user will be able to understand the consequences of using a certain app. Therefore, we support them to make informed decision (this is done by bypassing users to permission manager of Android OS		

[front of card]

Acceptance Criteria	Permission granting/restriction
Given	Installed applications on users' smartphones
When	The data are accessed and the user is informed regarding these accesses
Then	The users will be to decide whether they still feel comfortable granting that application or not

[Back of card]

2.2.1.4 Privacy risk score

Story Narrative	Privacy risk score	Priority	should
As a	application developer	Size	epic
I want	to provide users with a metric that makes it clear for the users to figure out the privacy invasiveness level of an application extent an application might be privacy invasive		
So that	the user will be able to understand to which extent an application is actually privacy invasive		

[front of card]

Acceptance Criteria	Privacy risk score
Given	Installed applications on users' smartphones
When	The installed application show up some privacy invasive activities
Then	The users will be provided by a privacy risk score

[Back of card]

2.2.1.5 Network connection

Story Narrative	Network connection	Priority	should
As a	application developer	Size	epic
I want	to support users to work with the artefact with both data and wifi connection		
So that	the user will be comfortably able to interact with the artefact		

[front of card]

Acceptance Criteria	Data connection
Given	Proposed artefact
When	The state of the data or wifi connections are not accessible
Then	The users will be choose switch between the connections

[Back of card]

2.2.1.6 Extensibility

Story Narrative	Extensibility	Priority	should
As a	application developer	Size	epic
I want	to take the future growth of the proposed artefact into consideration while designing and developing it		
So that	the artefact is capable of being extended in case of any new requirement		

[front of card]

Acceptance Criteria	Extensibility
Given	Proposed artefact
When	There is a need for adding new features/requirements
Then	The proposed artefact should be adapted according to these needs. The potential extension should minimally or not affect the whole functionalities and behavior of the original artefact

[Back of card]

2.3 ESR7 (UNI) The Role of Sealed Cloud Concept and Technology in User Acceptance and Usability of Privacy Applications

Technological artefact: A sealed computing prototype
ESR: 7 – Juan Quintero (UNI)

Sealed Cloud is a technology developed by UNI that can be used as a building block for privacy applications. Sealed Cloud implements a tamper-proof execution environment with strong perimeter security and trust in the operator through technically enforced division of power. This means that the operator of the Sealed Cloud can only access and modify the system with the help of a trusted third party (e.g., an accredited independent auditor). Sealed Cloud is therefore not only a technology but it is also a metaphor that facilitates users to understand what privacy properties the applications that are built upon Sealed Cloud actually guarantee in terms of personal data protection.

The ESR will investigate how users of Sealed Cloud-based privacy applications (such as IDGARD, privacy boxes etc.) understand and use applications running in the Sealed Cloud environment. The ESR will gain insights into (1) the general expectation of potential and current users concerning privacy, (2) how different ways to explain and motivate the environment shape the user's mental model of the privacy application, and (3) how the usability affects mental models of the technology and user acceptance of the applications. The final goal is to be able to successfully create new execution environment for privacy applications and thus increase the level of privacy that users can control.

To perform the investigation, the ESR will develop a sealed computing prototype implementing a Connected Car scenario. When networked cars drive through the streets their sensors and cameras can get PII and non-PII data, such as: the car's position and speed (PII), road state and weather conditions (non-PII), energy consumption (PII), and other data. In Connected Car (Fig. 1), that huge amount of data should be stored, accessed, and processed according to the privacy regulations.

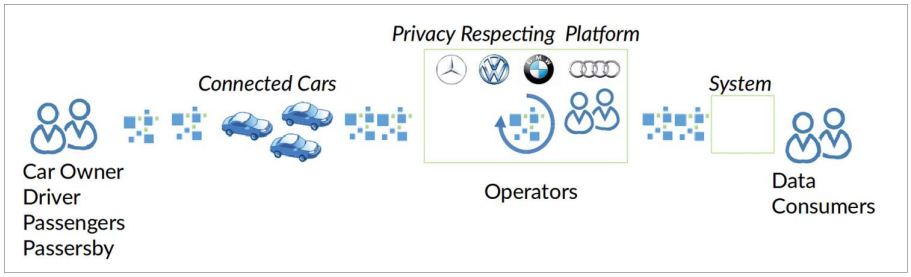

Fig. 1. Connected Card system model

The goal in the Connected Car Scenarios is to build a service platform that uses privacy-preserving analysis of data collected from the networked cars in scenarios.

	Data Subject	Data Controller	Data Processor
Car Owner	yes	yes	
Driver	yes	yes	-
Passenger	yes	-	-
Passerby	yes	-	-
Operator	-	-	yes
Data Consumer	-	-	yes

Car Owner, Driver, Passengers, Passersby, Operators and third parties can be Data Consumers

Table. 1. Mapping of Scenario to Terminology and Definitions of GDPR

2.3.1 User stories

2.3.1.1 Car's predictive maintenance

Story Narrative	Car's predictive maintenance	*Priority*	must
As a	Original Equipment Manufacturer (OEM)	*Size*	epic
I want	to analyzes the Connected Car's data		
So that	I can suggest to the Car Owner/Driver to make a car's check to avoid a big damage in the car in the future		

[front of card]

Acceptance Criteria	Car's predictive maintenance
Given	A connected car with a problem
When	The OEM detected a problem based on Connected Car data
Then	Car Owner/Driver receives a notification with the problem description and a suggested date to make a car's check

[Back of card]

2.3.1.2 Bonus in car insurance

Story Narrative	Bonus in car insurance	*Priority*	*must*
As a	Insurance company	*Size*	*epic*
I want	to analyzes the Car Owner/Driver data to find out behavior patterns (driving style, speed, etc.)		
So that	Car Owner/Driver gets a reward with new offers or discounts in his car insurance		

[front of card]

Acceptance Criteria	Bonus in car insurance
Given	Car Owner/Driver with a contracted car insurance
When	A good driving style is obtained from the Data Subject data
Then	Car Owner/Driver receives a notification with the reward

[Back of card]

2.3.1.3 Warnings on the road

Story Narrative	Warnings on the road	*Priority*	*must*
As a	OEM,insurance companies,Organizations of infrastructure maintenance	*Size*	*epic*
I want	to use the data of Data Subjects		
So that	I can warn other car drivers about the dangers, obstacles, accidents, or traffic jams		

[front of card]

Acceptance Criteria	Warnings on the road
Given	accident on the road, traffic jam, obstacles on the road
When	A Car Driver drives near a road with an accident/traffic jam/obstacle
Then	Car Driver receives a notification with the incident details

[Back of card]

2.3.1.4 Preventive and corrective road infrastructure maintenance

Story Narrative	Preventive and corrective road infrastructure maintenance	*Priority*	*should*
As a	Organizations of infrastructure maintenance	*Size*	*epic*
I want	to process the data of Data Subjects		
So that	I know which infrastructure (street, traffic light, light, etc.) needs to be repaired		

[front of card]

Acceptance Criteria	Preventive and corrective road infrastructure maintenance
Given	Road in bad state
When	A Data Subject send information about a road in bad state
Then	Organizations of infrastructure maintenance receives a notification with the position and details of the road

[Back of card]

2.3.1.5 Bonus in car insurance

Story Narrative	Parking management	*Priority*	could
As a	Organizations of infrastructure maintenance	*Size*	epic
I want	to look for a free parking slot		
So that	I can inform to the Car Driver about the localization of free parking slot		

[front of card]

Acceptance Criteria	Parking management
Given	Car Driver is looking for a free parking slot
When	A Data Subject send information about a free parking slot near to the Car Driver
Then	Organizations of infrastructure maintenance receives a notification with the position and details of free parking slot, Car Driver receives a notification from Organizations of infrastructure maintenance with the position and details of free parking slot

[Back of card]

2.4 ESR10 (UNI) Adaptive Data Privacy for Smart Environments

Technological artefact: A prototype of a privacy-aware and context-adaptive mobile service
ESR: 10 – Lamya Abdullah (UNI)

The convergence of technologies in artificial intelligence, data management and pervasive computing has generated interest in the design and implementation of smart environments. Smart environments may have an enormous impact on society, sustainability, and the quality of life. Valuable functions include independent living, and aging well. Smart environments offer services that heavily rely on the collection of contextual data from sensor-equipped devices, including data about the position and movements of individuals, their habits and activities at home, work, and in public spaces.

The ESR project targets all issues related to understanding the privacy threats in these environments and in designing techniques and technologies to increase transparency, user awareness and control of how personal data is collected and used in these environments by third parties. The technological artefact that will be developed is a tool for the release by an authorized data collector of smart space data to third parties, while providing privacy guarantees, including adaptive methods to semi-automatically adjust privacy preferences based on mobile device context.

2.4.1 User stories

2.4.1.1 Collected Data Secrecy

Story Narrative	Collected Data Secrecy	*Priority*	must
As a	User	*Size*	story
I want	My personal collected data to be stored confidentially		
So that	It is not disclosed for unauthorized access		

[front of card]

Acceptance Criteria	Data is Confidential
Given	Data storage accessibility
When	1: authorized data process takes a place 2: unauthorized data processing takes a place
Then	1: only data required for the processing is used 2: data is not readable/accessible

[Back of card]

2.4.1.2 Data availability

Story Narrative	Data Availability	*Priority*	*must*
As a	Service provider	*Size*	*story*
I want	The minimum required data needed to be available		
So that	The basic function of the service to be acceptable		

[front of card]

Acceptance Criteria	Data Availability
Given	Authorized access to the collected data
When	The service is requested – function to be run on the data
Then	Then computation is complete and service runs appropriately – no missing data

[Back of card]

2.4.1.3 Data Privacy Transparency

Story Narrative	Data Privacy Transparency	*Priority*	*must*
As a	User	*Size*	*story*
I want	To know how my data is processed, used, and disclosed.		
So that	I am aware of what should I expose and what not.		

[front of card]

Acceptance Criteria	Data Privacy Transparency
Given	Certain data is to be disclosed/shared with third party
When	A user set preference / profile / the system
Then	The user should be notified/told with the data disclosure/sharing details.

[Back of card]

2.4.1.4 Intervenability

Story Narrative	Intervenability	*Priority*	must
As a	User	*Size*	story
I want	To be able to change which collected data is used / processed/ accessed		
So that	I can limit disclosure of my sensitive data		

[front of card]

Acceptance Criteria	Intervenability
Given	Amount of collected data stored confidentially
When	A user sets / changes privacy requirement
Then	The data restricted data is not accessible anymore until the restriction is removed again

[Back of card]

2.5 ESR11 (UCL) Secure and Privacy-Preserving Personal Genomic Testing

Technological artefact: Privacy-preserving protocols for secure and private genome testing
ESR: 11 – Alexandros Mittos (UCL)

The rapid progress and increasing affordability of Whole Genome Sequencing prompts the creation of large datasets of digitized genomes, made available for research purposes, and allows individuals motivated by medical reasons or personal curiosity to have their genome sequenced. Testing can be performed, more effectively and inexpensively, in computation, thus enabling so-called "personalized medicine," i.e., the practice of tailoring healthcare to patients' genetic makeup. Genomic data disclosure, however, raises privacy and ethical issues as genomes not only uniquely and irrevocably identify their owner, but also contain personal and sensitive information. Consequently, in order for computational genomic tests to be accepted and commonplace, efficient, usable, and privacy-respecting versions of such tests need to be designed, developed, tested, and trial-deployed. The research will attempt to design the necessary technology to securely and privately handle storage and testing of genomic data. Technological artefacts will be developed to investigate how to securely and efficiently store genomic data (e.g., preventing unauthorized parties from accessing genomic information and binding a genome to its owner) and how to design and implement user-centric secure and privacy-preserving genomic testing, including ancestry testing, genetic screening, partner and organ donor compatibility, and supporting collaborative genomic research across multiple entities.

2.5.1 User stories

2.5.1.1 Privacy-preserving disease susceptibility test

Story Narrative	Privacy-preserving disease susceptibility test	*Priority*	Must
As a	Physician	*Size*	Theme
I want	study the genome of my patient		
So that	I can learn his/her potential susceptibility to disease X		

[front of card]

Acceptance Criteria	Privacy-preserving disease susceptibility test
Given	that the patient's genome is sequenced from a trusted third party
When	the patient asks for a specific test OR when I infer that this information will be important to his/her health
Then	I will learn the result of this test in a privacy-preserving manner, meaning, I won't learn anything else than the result of test conducted

[Back of card]

2.5.1.2 Anonymized Sharing of Genomic Data - Donor

Story Narrative	Anonymized Sharing of Genomic Data - Donor	*Priority*	Must
As a	Donor	*Size*	Epic
I want	donate my sequenced genome		
So that	A pool of research entities can access it, in order to conduct biomedical research		

[front of card]

Acceptance Criteria	Anonymized Sharing of Genomic Data - Donor
Given	that my genome is sequenced from a trusted third party
When	An entity wants to access my genome for research and I give them explicit access to parts of my genome or the whole genome
Then	The entity will conduct its research in a privacy preserving manner, meaning they will never learn my identity

[Back of card]

2.5.1.3 Anonymized Sharing of Genomic Data – Research Center

Story Narrative	Anonymized Sharing of Genomic Data – Research Center	*Priority*	Must
As a	Research Center	*Size*	Epic
I want	have access to a pool of sequenced genomes		
So that	I can conduct biomedical research		

[front of card]

Acceptance Criteria	Anonymized Sharing of Genomic Data – Research Center
Given	A pool of genomic data
When	I request to view the whole genome or parts of it, of one or more individuals
Then	I can access the whole genome or parts of the individuals who accepted

[Back of card]

2.5.1.4 Deletion of data

Story Narrative	Deletion of data	*Priority*	Should
As a	Donor	*Size*	Theme
I want	To be able to delete my data		
So that	My privacy is protected		

[front of card]

Acceptance Criteria	Deletion of data
Given	A deletion request
When	I request it
Then	My data will be deleted

[Back of card]

2.5.1.5 Transparency

Story Narrative	Transparency	*Priority*	Must
As a	Donor	*Size*	Theme
I want	To know when someone has accessed my data		
So that	No one can access my data without my approval		

[front of card]

Acceptance Criteria	Transparency
Given	An access request
When	My data is asked to be processed
Then	I should get a prompt in my personal device in order to accept or decline

[Back of card]

2.6 ESR13 (VDS) Privacy Preserving Transaction Authentication for Mobile Devices

Technological artefact: Security-enhanced authentication protocols
ESR: 13 – Andreas Gutmann (VDS)

Objectives: Secure authentication is one of the key requirements for allowing the use of online services. The predominant method of username and password fails to offer usability because the requirements put on users: of choosing a different complex password for every online service and not writing any down. Username and passwords also fail to provide adequate security for today's computing environment: malware on users' computers can harvest passwords and security breaches of servers reveal large databases of usernames and passwords likely shared over different websites. Single Sign On (SSO) services partially address these problems by replacing multiple passwords with a single password, but introduce a new problem of privacy. The SSO service operator gains knowledge of all services a user is making use of, how often they are used, and when. There is a substantial danger to privacy and self-determination of this information being leaked because it could disclose sensitive information about a user such as their health in the context of e-healthcare scenario. SSO solutions have also not adapted to the new class of malware attacks – "man-in-the-browser" seen against online banking applications but likely to be extended to online services. These malware attacks do not merely record passwords, but misrepresent a user's intentions to the online service. In the case of online banking this is usually for the goal of moving a user's money to a criminal, but with a SSO service the malware could force a user to log into a service they did not wish to, or to reveal information which they have not consented to have revealed. Traditional authentication solutions such as one-time-passwords do not address this problem.

This project will design and evaluate a technological artefact implementing new approaches for authentication, addressing the limitations of existing SSO systems. Firstly, unlinkable and anonymous credentials shall be used so that a SSO service provider is unable to discover the identity of the user they are providing authentication services to. This is achieved by ensuring that each authentication protocol run is unlinkable to the SSO service, but obviously not to the online service which needs to perform the authentication. Secondly protocols will be developed to prevent a network-based adversary being able to establish the identity of the user by observing or interfering with an authentication protocol exchange. This will prevent the attacker from being able to use targeted malware attacks against certain users. Thirdly, SSO protocols will be extended to provide not just protection of log-in information, but also transaction information so as to defend against man-in-the-browser attacks.

2.6.1 User Stories

2.6.1.1 Transaction Authentication

Story Narrative	Transaction Authentication	*Priority*	*must*
As a	user	*Size*	*epic*
I want	to authenticate a transaction		
So that	the transaction will be processed		

[front of card]

Acceptance Criteria	Transaction Authentication
Given	an initiated but unauthorised transaction
When	being authorised by legitimate and eligible user
Then	transaction will be processed in a timely manner

[Back of card]

2.6.1.2 Transaction Privacy

Story Narrative	Transaction Privacy	*Priority*	must
As a	user	*Size*	epic
I want	assurance that any party has only reasonable access to data related to any of my transactions as is necessary for this transaction		
So that	my privacy is protected		

[front of card]

Acceptance Criteria	Transaction Privacy
Given	one or more transactions
When	any party has knowledge related to it
Then	having this knowledge is reasonable, and in the user's interest or a legal requirement

[Back of card]

2.6.1.3 Service Provider Incentive

Story Narrative	Service Provider Incentive	*Priority*	*must*
As a	service provider	*Size*	*epic*
I want	to earn money		
So that	it is in my economic interest to provide this service		

[front of card]

Acceptance Criteria	Service Provider Incentive
Given	an authorised transaction
When	transaction is being processed
Then	service provider either directly or indirectly earns money (e.g. transaction fee, knowledge of economic value, …)

[Back of card]

2.6.1.4 Authentication Integrity

Story Narrative	Authentication Integrity	*Priority*	*must*
As a	user or service provider	*Size*	*theme*
I want	integrity of transaction data		
So that	all transactions are processed as intended		

[front of card]

Acceptance Criteria	Authentication Integrity
Given	a transaction
When	being processed
Then	this transaction has been authenticated by the corresponding user

[Back of card]

2.6.1.5 Compliance Money Laundering Act

Story Narrative	Compliance Money Laundering Act	*Priority*	must
As a	service or content/product provider	*Size*	theme
I want	to retain all necessary documents/information related to financial transaction and, if required, be able to identify the user (possibly joint effort)		
So that	I comply with the Money Laundering Act (or similar legislation)		

[front of card]

Acceptance Criteria	Compliance Money Laundering Act
Given	any documents or information related to financial transaction
When	this information should be retained according to the Money Laundering Act (or similar legislation)
Then	the service and content/product provider are able to retain this information

[Back of card]

2.6.1.6 Authentication Credential Reset and Change

Story Narrative	Authentication Credential Reset and Change	*Priority*	must
As a	user	*Size*	theme
I want	to have a convenient and secure method to reset or change my authentication credentials		
So that	I can recover from losing my credentials or if I don't consider them being secret anymore.		

[front of card]

Acceptance Criteria	Authentication Credential Reset and Change
Given	the artefact
When	user wishes to reset or change authentication credentials
Then	a reasonably convenient and secure method of resetting or changing credentials is available

[Back of card]

2.6.1.7 Transaction Receipt

Story Narrative	Transaction Receipt	*Priority*	should
As a	user	*Size*	theme
I want	to be able to produce a receipt		
So that	I can prove a payment to a content/product provider		

[front of card]

Acceptance Criteria	Transaction Receipt
Given	a completed transaction
When	the user wants to prove this transaction to another party
Then	the user can produce a receipt with authenticity guarantees.

[Back of card]

2.6.1.8 Content/Product Provider Incentive

Story Narrative	Content/Product Provider Incentive	*Priority*	would
As a	content/product provider	*Size*	theme
I want	competitive costs (time, setup, maintenance, fees, user experience, …)		
So that	it is in my economic interest to accept this service		

[front of card]

Acceptance Criteria	Content/Product Provider Incentive
Given	any cost for the service burdened to the content/product provider
When	put in relation with potential gains from the service
Then	it is in the content/product provider's economic interest to accept it

[Back of card]

3 Conclusions

The preliminary requirements analysis results have been developed by ESRs 4, 5, 7, 10, 11, and 13 following the Agile methodology and presented as User stories. This analysis shows that the designs of technological artefacts put users at the center of system development, and offer both control and transparency over processing of personal data. As a result, this work matches the ambitious goals of the Privacy&Us project.

4 References

[1] Beck, K., Grenning, J., Martin, R.C., Beedle, M., Highsmith, J., Mellor, S., van Bennekum, A., Hunt, A., Schwaber, K., Cockburn, A., Jeffries, R., Sutherland, J., Cunningham, W., Kern, J., Thomas, D., Fowler, M., and Marick, B.(2001). "Manifesto for Agile Software Development". Agile Alliance.

[2] Martin, R.C. (2002) “Agile software development: principles, patterns, and practices”. Prentice Hall.