Serums

HORIZON 2020

Project no. 826278

SERUMS

Research & Innovation Action (RIA)
SECURING MEDICAL DATA IN SMART-PATIENT HEALTHCARE SYSTEMS

Initial Report on Use Cases and Evaluation of Serums Technologies D7.3

Due date of deliverable: 31st December 2019
Extended until 29th February 2020

Start date of project: 1st January 2019

Type: Deliverable
WP number: WP7

Responsible Institution: Fundació Clínic per la Recerca Biomèdica (FCRB)
Editor and editor's address: Josep Pujol (jpujoll@clinic.cat), Santiago Iriso (siriso@clinic.cat)
Partners Contributing: FCRB, ZMC, USTAN, ACC, IBM, SOPRA, SCCH, UCY, INRIA

Approved by:
Reviewers: Marios Belk (UCY)
Vladimir Janjic (USTAN)
Technical Manager: Juliana Bowles

Version 1.0

Project co-founded by the European Commission within the Horizon H2020 Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Release History

Release No.	Date	Author(s)	Release Description/Changes made
V0.1	08/10/2019	Santiago Iriso FCRB, Josep Pujol FCRB	Empty document with executive summary and introduction
V0.2	11/10/2019	Santiago Iriso FCRB, Josep Pujol FCRB	Written FCRB Use Case
V0.3	11/11/2019	Ivo Buil ZMC Mark Mestrum ZMC	Added ZMC Use Case
V0.4	31/12/2019	Bram Elshof ACC, Giona Arts ACC, Wanting Huang ACC	Added PoC methodology
V0.5	7/12/2019	Santiago Iriso FCRB, Josep Pujol FCRB	Added structure for evaluation section
V0.6	24/02/2020	Marios Belk (UCY), Christos Fidas (UCY), Andreas Pitsillides (UCY)	Added the analysis of results and main findings for the baseline and PoC user authentication systems
V0.7	25/02/2020	Euan Blackledge(SOPRA)	Added analysis on security and perceived security and its KPIs
V0.8	26/02/2020	Wanting Huang (ACC)	Added analysis on Distributed Ledger Technologies and its KPIs
V0.9	27/02/2020	Vladimir Janjic (USTAN), Marios Belk (UCY), Josep Pujol (FCRB)	Reviewed and end version

SERUMS Consortium

Partner 1	**University of St Andrews**
Contact Person	Name: Vladimir Janjic, Juliana Bowles Email: vj32@st-andrews.ac.uk, jkfb@st-andrews.ac.uk
Partner 2	**Zuyderland Medisch Centrum**
Contact Person	Name: Mark Mestrum Email: m.mestrum@zuyderland.nl
Partner 3	**Accenture B.V.**
Contact Person	Name: Bram Elshof, Wanting Huang Email: bram.elshof@accenture.com, wanting.huang@accenture.com
Partner 4	**IBM Israel Science & Technology Ltd.**
Contact Person	Name: Michael Vinov Email: vinov@il.ibm.com
Partner 5	**Sopra-Steria**
Contact Person	Name: Andre Vermeulen Email: andreas.vermeulen@soprasteria.com
Partner 6	**Université Catholique de Louvain**
Contact Person	Name: Axel Legay Email: axel.legay@uclouvian.be
Partner 7	**Software Competence Centre Hagenberg**
Contact Person	Name: Michael Rossbory Email: michael.rossbory@scch.at
Partner 8	**University of Cyprus**
Contact Person	Andreas Pitsillides Email: andreas.pitsillides@ucy.ac.cy

Partner 9	**Fundació Clínic per a la Recerca Biomèdica**
Contact Person	Name: Santiago Iriso Email: siriso@clinic.cat

Table of Contents

Executive Summary

Serums aims to increase efficiency while also ensuring the increased safety of patients and the privacy of sensitive health data using innovative techniques that will increase resilience to cyber-attacks and promote trust in the safe and secure operation of the system. In order to meet this challenge, Serums will develop and implement innovative methods, tools and technologies addressing the need for cybersecurity in hospitals including remote care and home-care settings. Through these developments, the Serums project expects to achieve significant impact in each area that has been identified in the SU-TDS-02-2018 call, providing significantly more secure smart health care provision, with significantly reduced potential for data breaches, and significantly improved patient trust and safety.

The purpose of this deliverable is to report the effectiveness of the Serums technologies on real-world use cases from the domain of using and analysing medical data. These will be tested and validated on real health environments provided by the Use Case partners. Despite all the technologies have to be evaluated on at least two stages of the project (baseline and one Proof of Concept) to be able to report improvement,

Work related to the demonstration of the Serums technologies effectiveness on real-world use cases from the domain of using and analysing medical data, will proceed in *three phases*. This deliverable presents the work performed during the *first phase*. More specifically, during the first phase initial prototypes of the Serums technologies have been produced, integrated and evaluated against the overall project requirements and success criteria that were identified in D7.1, using initial use cases, developed for the use of Serums technology, supporting basic information sharing between patients and hospitals/medical centres. During this phase, the conclusions extracted from the different Proof of Concept done at Fundació Clínic de Recerca Biomèdica (FCRB), Zuyderland Medisch Centrum (ZMC) and University of St Andrews (USTAN), have also been considered. The lessons learned and the results extracted from this work will provide feedback into different technical work packages, steering the development of Serums technologies in the subsequent phases of the project.

The results associated with the *second and third phase* will be included in future versions of this deliverable. More specifically, during the *second phase*, the Serums technologies will be evaluated on use cases that will be refined and extended with mechanisms to share information between patients, hospitals/medical centres and local e-health providers. During this phase focus will be also given on ensuring ownership and appropriate involvement of all stakeholders/end-users within both medical centres, educate end-users on the future Proof of Concepts (POCs) and Pilots and measure the change progress. The analysis on the needs of the end-users towards successful POCs and Pilots, including the required behaviours, skills, capabilities, and knowledge, will be also part of this phase. The results will be reported in D7.5 on M25 of the project. In the *third (final) phase*, the final versions of the use cases will be produced, also extending them with mechanisms for information sharing between patients, hospitals/medical centres, local e-health providers and other caregiver organisations (general practitioners/paramedics). During this phase, the required educational/information/training materials and environments for the POCs and pilots will be designed, developed and tested, before the actual deployment of the POCs and the Pilots, of the Serums tool and technologies, with the end-users of both medical centres. The results will be reported in D7.6 on M36 of the project.

1 Introduction

1.1 Role of the Deliverable

The role of this deliverable is to present the results of the work performed during the first phase of the demonstration of the Serums technologies effectiveness on real-world use cases from the domain of using and analysing medical data. More specifically, this deliverable: **i)** defines a detailed specification of the initial use cases, supporting basic information sharing between patients and hospitals/medical centre; and **ii)** evaluate the initial prototypes of the Serums technologies developed, against the overall project requirements and success criteria that were identified in D7.1. During this first phase, the conclusions extracted from the different Proof of Concept done on Fundació Clínic de Recerca Biomèdica (FCRB), Zuyderland Medisch Centrum (ZMC) and University of St Andrews (USTAN), have also been considered.

The lessons learned and the results extracted from this work will provide feedback into different technical work packages, steering the development of Serums technologies in the subsequent phases of the project.

1.2 Relationship to Other SERUMS Deliverables

These are the relations of the Deliverable 7.3 with previous and future deliverables:

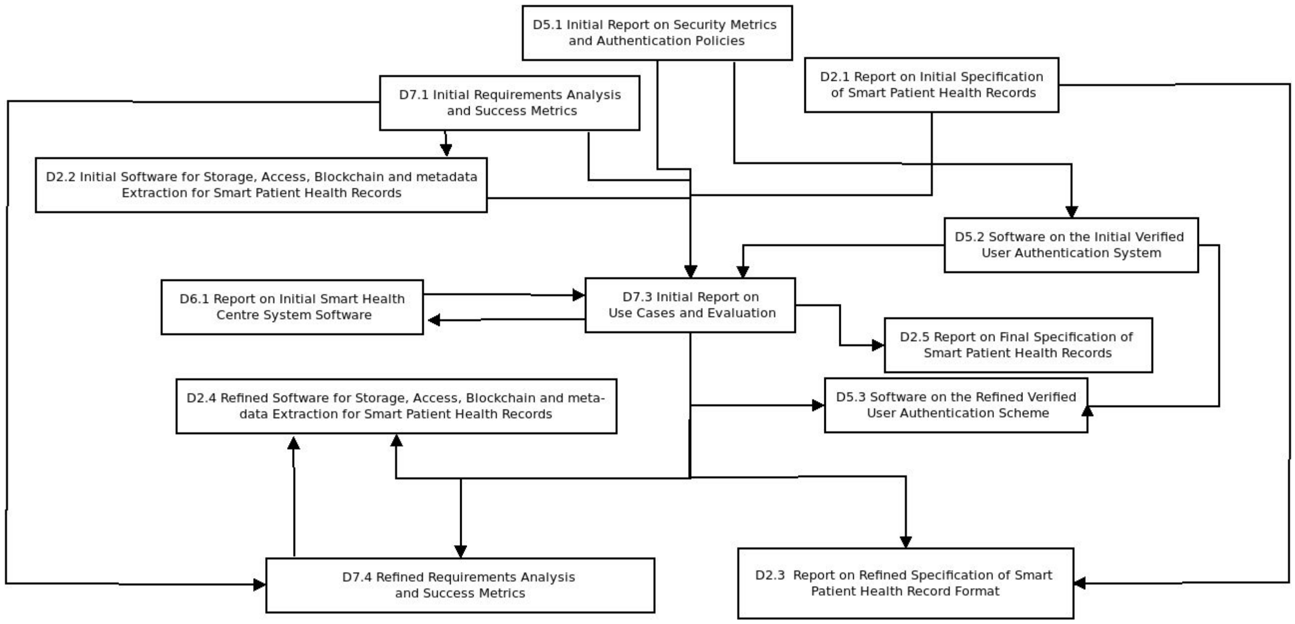

D5.1 Initial Report on Security Metrics and Authentication Policies
D7.1 Initial Requirements Analysis and Success Metrics
D2.1 Report on Initial Specification of Smart Patient Health Records
D2.2 Initial Software for Storage, Access, Blockchain and metadata Extraction for Smart Patient Health Records
D5.2 Software on the Initial Verified User Authentication System
D6.1 Report on Initial Smart Health Centre System Software
D7.3 Initial Report on Use Cases and Evaluation
D2.5 Report on Final Specification of Smart Patient Health Records
D2.4 Refined Software for Storage, Access, Blockchain and meta-data Extraction for Smart Patient Health Records
D5.3 Software on the Refined Verified User Authentication Scheme
D7.4 Refined Requirements Analysis and Success Metrics
D2.3 Report on Refined Specification of Smart Patient Health Record Format

Figure 1. Table of relations between deliverables.

1.3 Structure of this Document

This document is organized having in mind the chronological order in which the tasks described on it have been executed. The first section corresponds to T7.2 and elaboration of the use-cases where FCRB, ZMC and USTAN describe their systems and platforms and their relation with the Serums technologies. The second section refers to T7.4, or Evaluation of technologies and Use Cases. Finally, the document ends with the information referring to T7.3 and the Proofs of Concept developed by Accenture and the respective Use-case partners together with the conclusions that have been provided by the users.

2 Use Cases Specification (Leader ZMC)

This chapter provides a detailed description of the initial use cases, supporting basic information sharing between patients and hospitals/medical centre, that have been used for the evaluation of the initial prototypes of the Serums technologies. For this first phase, three different use cases were used to test the Serums technologies in realistic conditions with synthetic but realistic data produced using data-fabrication methods from WP4, which were obtained from private, confidential medical data. Note that these use cases have been initially developed by ZMC, FCRB and USTAN and then adapted by: **i)** ACC based on the conclusions extracted from the different POCs and Pilot projects done on FCRB, ZMC and USTAN; and **ii)** SOPRA, SCCH, IBM and UCY in such a way that the smart health record, data analytics, data masking and semantic-preserving encryption and authentication technologies are incorporated into these use cases.

For the ZMC Smart Health Centre use case (see section 2.1), the whole system for gathering personal data about patients from within and outside of the individual ZMC hospitals will be developed. This use case exploits the smart patient records from WP2, privacy-preserving and secure communication mechanisms from WP4 for gathering data from different devices and authentication methods from WP5. The system developed was based on the Smart Health Centre System that will be developed in WP6.

The FCRB use case (see section 2.2) consists of the HCB - Smart Platform (HCB-SP). Together with the help of the technologies developed during the Serums project, we +intent to allow Joana, a 85 year-old patient with various chronic diseases, the easy gathering of vital signs measurements out of the hospital with the help of eHealth devices and the possibility to share them with all the professionals that care for her health. As the Use Case, the HCB-SP exploits the smart patient records from WP2, privacy-preserving and secure communication mechanisms from WP4 for gathering data from different devices and authentication methods from WP5.

The USTAN use case (see section 2.3) mostly focuses on communication mechanisms for fetching the selected information to the central patient portal and displaying this information to the user. Therefore, this use case mostly exploits mechanisms for smart patient records access from WP2, privacy preserving and secure communication mechanisms from WP4 and authentication mechanisms from WP5.

2.1 ZMC - A New Hip

Peter is a 70-year old male who has recently been provided with a new artificial hip at Zuyderland Medical Centre (ZMC). After a short stay at the hospital, Peter is dismissed and sent home to complete his recovery there. There he can already view his medical data related to his injury and operations in his account in the Personal Health Environment (PHE), because he arranged that before the operation.

Note: The medical files in the hospital regarding basic characteristics, injury, X-rays, operation details and stay in the hospital are easily accessible and compatible with the Personal Health Environment system. Identification and authentication for sharing hospital data with the PHE needs to be done in a secure and user-friendly way according to the principles of the European GDPR guidelines and MedMij in the Netherlands.

To ensure Peter's recovery, the physician has ordered physiotherapy and the use of an Activity Monitor (AM) with an E-coach for 1 week. Prior to his surgery, Peter has already used the Activity Monitor, to measure his mobility before the hip replacement. The Activity Monitor is a very precise instrument that measures if and how well a patient is active at a validated clinical level.

Commentary: To comply with the GDPR, Peter must provide explicit permission to:

- specifically allow the Activity Monitor to provide his personal activity data to i) each medical practitioner that needs the results from it, and ii) the SHC;
- specifically allow the E-Coach to share the advice that it provides with i) each medical practitioner that needs the results from it, and ii) the SHC;
- allow each medical practitioner to share their medical records with the SHC, and vice-versa.

Under the GDPR, Peter may revoke any of these permissions at any time, or choose to exclude some part of the information from being seen by any agent in the system, including historical information. Doing this may be detrimental to his treatment, lead to false diagnoses, incur additional treatment costs, require him to take unnecessary drugs etc.

From the first session and the letter from the surgeon, the physiotherapist knows that Peter also wears an Activity Monitor. He knows the results will tell him how stable Peter's condition is with his new hip. Together with giving Peter exercises he can do at home, the physiotherapist asks Peter if he will allow him to see all relevant medical files from the hospital and the results from the Activity Monitor. They agree that Peter will share the files regarding the surgery and the daily results on the E-coach. Informed consent to share the data with the physiotherapist can be given via Peter's Personal Health Environment.

Note: Peter can choose in his Personal Health Environment which medical files and how long he wants to transfer the medical files from the Hospital and the E-coach to the physiotherapist. The rights, rules and communications of the data access will be ensured, logged, checked and tracked via Blockchain.

Peter knows that the Activity Monitor needs charging every day. Because of its accuracy it is a very energy consuming instrument and will last only 24 hours. Therefore the nurse at the hospital explained to Peter that he needs to charge the battery every evening using the Smart Charger when he goes to bed. This Smart Charger then transfers the measured data to show the results in the E-coach.

Note: The transfer needs to be secure. Data must be private and not tampered with. The raw data of the Activity Monitor is transported to an external server, where this raw data is analysed by a validated algorithm. Once the Activity Monitor receives a confirmation that the raw data is transferred successfully, it purges its data.

The results are available the next day to the physician via the E-coach, the patient record of Peter in SAP and to Peter himself via his Personal Health Environment on his computer. Each morning Peter transfers the results from the Activity Monitor to the physiotherapist in his Personal Health Environment. Each day a trained nurse can then evaluate the stored results in the Electronic Patient Record (EPR) of the SHC or the E-coach and can take actions accordingly.

Note:

1. Both the Activity Monitor and the validation algorithm do not know which patient is using which Activity Monitor. Yet in the E-coach and in the SHC the link between the sensor ID of the Activity Monitor and the patient must be made. This is a potential danger for the patient when not done correctly.
2. The E-coach needs to send the results to SHC and the PHE in a secure way so that a patient cannot be identified during transport.

3. Identification and authentication in the E-coach or portal needs to be done in a secure and user-friendly way.

Data transport must be private and secure. The physiotherapist can now view the results Peter has sent them. The data transport is logged in Peter's record in the Personal Health Environment.

Peter finds it hard to get up from a chair or bed. He is afraid that his new hip will hurt him, causing him to use his muscles wrong and his first steps to be unstable. After a while that feeling goes away, but the fear prevents him from exercising correctly. During his physiotherapy session on the fourth day Peter is told that he should try to exercise more and that he needs to put more pressure on the leg with the new hip. The results have shown that Peter did not do his exercises and that when he gets up, he is not standing straight which might cause Peter to fall. Peter promises to improve his exercises. The physiotherapist is able to explain the effect of this to Peter from the graphical image of the results.

On the fifth day the physician looks at the results of the last four days and concludes that Peter should have done better, but also sees an improvement on the fourth day. He tells the nurse to contact Peter and prolong the Activity Monitor until his 6 weeks follow-up session at the hospital.

Note: The extension of the Activity Monitor is administered in both the SHC and the E-coach and automatically visible in Peter's Personal Health Environment.

Peter improves his stability within the next four days. This is shown in the results of the Activity Monitor. The physician acknowledges this improvement and orders a digital consult with Peter via his E-coach for his standard 6-weeks follow-up. There is no need to see him physically. Peter will be asked to transfer the data from his physiotherapist to his physician when his physiotherapy has ended. Peter agrees and transfers the physiotherapy journal to his Personal Health Environment and SAP for the physician.

Note: This is administered in SAP. The request for sending the data from the physiotherapist is automatically visible in Peter's Personal Health Environment in a secure and private way.

Peter transfers in his Personal Health Environment the journal from his physiotherapist to his physician in a private and secure way. He has control over the timing and content of this transfer.

Two weeks before the annual check-up, Peter is invited to the hospital for an X-ray of his hip and again receives the Activity Monitor and the E-coach from Zuyderland to monitor his recovery for 1 week. The results of the weekly AM and X-Ray are positive. The physician orders the physician assistant to have a digital consult with Peter, as it isn't necessary to see him physically.

The table below shows which problems or needs arise in the ZMC use case, what solutions need to be implemented and which technical implications it gives.

No.	Problem/Need	Solution	Remarks/Notes	Technical Implication
1	**Under the GDPR Peter must provide explicit permission to share his health data across different caregivers, revoke these permissions or specify specific data to be shared in his Personal Health environment**			
a	Peters health data must	Peter's Health environment is	Aside from his health	**Smart Patient Health**

	be filling up in the personal health environment	connected to Peter's health organisations to which data is sent or can be retrieved on the fly.	data, this includes the names and roles of the Care professional involved per organisation.	**Record**: This is a centralised data source that allows all of the patient's records to be accessed from a single source, regardless of the source system
b	Peter must be able to connect any external device and E-coach he wants	The results from the Activity Monitoring E-coach can be shared with Peter's Health environment		**Smart Patient Health Record:** The structure of the record allows for seamless integration of any additional data sources
c	Peter must be able to log in with the method and options he prefers	Peter logs in to his Personal Health environment using Picture Guessing.	Of course all kind of authentication methods need to be accessible, (multiple authentication including 2 way factor authentication)	**Personalized User Authentication:** Based on the suggested flexible and personalized authentication approach, end-users have the option to choose their preferred authentication method (*i.e.*, graphical or textual) in order to login. After successfully entering the password secret, for adding an additional layer of security, a push notification is sent to the end-user's mobile device that (s)he needs to approve in order to complete the login process. After successful completion of the login process, the authentication system generates a security token (JWT) and sends it to the client that is used for subsequent requests to the Serums systems.
d	Patients need full control over which data is sent, to who (and who not), and for how long.	Peter sees in his Personal Health on a special page his health data grouped by device/organization (including external physiotherapy) and if it is shared, partly shared or not shared.	The view can be also the other way around. Peter selecting an organisation or Care professional and then see which data is shared with that organisation. In the end it all comes down to Care professional --> permissions <-- data. It is a n to m	**Blockchain:** The default permission for the caregiver to access the patient is defined by the hospital administrator. Patients have the possibility to view existing rules, create additional rules to permit or restrict access for a selected set of data.
e		Peter selects the Activity Monitor from the above mentioned list and allows		

		sharing	relation The same way sharing data is allowed, so is revoking sharing the data.	
f		Peter then sees the organisations he can share the data with and selects his physiotherapist		
g		Peter now has the option to choose a certain period of time he wants to share his Activity Monitor data. Since Peter only uses the Activity Monitor for a week, Peter chooses this time frame for sharing. Furthermore he checks all data to be shared		
h		Peter needs to confirm this request for sharing and is then led back to the page where he can see in health data and if it is shared, partly shared or not shared		**Blockchain:** Patient’s confirmation triggers the creation of the rule to allow the caregiver specified in the rule to access his data.
k	Setting specific documents to be shared	Some of the medical data from the hospital contains subsets of data. Peter can choose whether he wants to share all data or specific data. Peter selects his hip operation details.	Since this a specific part of the data and a single document no time frame will be asked.	**Smart Patient Health Record:** The record stores data in a Data Vault structure, wherein only highly correlated data is stored in the same satellite. This works in conjunction with the Blockchain to ensure granular control over the access

2.2 FCRB - Chronic Disease Management (HCB-SM)

Joana is an 85 years old female with several chronic diseases: she has diabetes and chronic heart failure (for which she receives medication). Joana lives in a private apartment close to a Primary Care Centre. She is getting some care via the Primary Care Centre but wants to remain independent for as long as possible. For that reason, her Doctor, from the Hospital Cli̗nic de Barcelona, specialist in Diabetes, has given her wearable medical devices: **i)** a wireless pulse oximeter, to monitor her oxygen blood percent and her cardiac frequency; and **ii)** a wireless glucometer to measure her own glycemia.

Note: The following sensors will be made available to the health professionals to give to the patients:

- Pulse oximeter
- Glucometer
- Thermometer
- Tensiometer

All these devices will connect wirelessly to a smartphone application through Bluetooth 5 in a secure way.
Serums Interaction: The user will gain access to the HCB-SP through the authentication system provided by UCY, which frontend will be embedded in the Patient application and Professional platform.

For the second device, Joana has been informed that she will have to periodically upload her glycemia and oxygen in blood results to the HCB-SP platform through a mobile phone application called Saludata which basic usage has been taught by the doctors.

Serums Interaction: All information concerning patient record data and the measurements taken by the eHealth devices will be securely stored on the Data Vault provided by SOPRA. None of the HCB-SP will never store personal data, these will always be retrieved from the Data Vault when needed.

Joana is happy with this because she can control her progress in this matter. With this smartphone application Joana is totally in control of the data generated by the devices and her patient record. Joana has therefore given the doctor her permission to access her data on that platform.

Serums interaction: The access and modification permissions over the patient data will be stored in the Blockchain solution developed by ACC. This will include various levels of information access, from only accessing the Patient Record to the granular access to only the information related to an aspect of the Record History (e.g. Endocrinology Record, Quirurgic Operation, etc.)

The Doctor has also commented to Joana that her General Practitioner would also need to have access to the glycemia web portal to monitor her evolution and he will contact her to follow up on that, and also on the rest of her health issues.

Note: The Blockchain solution is not only for personal permission and professional, but groupal, organizations and for the whole hospital.
In addition, more complex rules can be generated by Joana or the Hospital administrators.
Explanation: The Saludata application is to be in full compliance with the GDPR and by thus has to provide:

- Full control of who can access the patient data.

- Full control of which parts of the patient record each hospital, professional or service can access.

On the other side, a cardiology medical team is in charge of taking care of her chronic heart failure and is composed of two nurses and one cardiologist. One of their tasks is to monitor the evolution of the patients with chronic heart failure at home, they receive and monitor all the data generated by the wireless pulse oximeter through an application installed in local servers of the hospital, where they can review Joana's list of measurements and communicate with her through notes with her smartphone app if necessary.

The hospital nurse periodically generates a clinical note with the events that have occurred and sends this to the patients. With this information and the glycemic control from Joanas device, the General Practitioner can (with Joana's approval) collaborate to monitor, control and detect abnormalities not only in one of those two diseases but can merge all of Joana's health issues and provide her with a better quality of life, by taking an holistic approach of her health status.

In terms of the technical flow of the use case, first the patient will be told by the hospital or their caregivers to download a Smartphone application in order to communicate with the eHealth Devices and with the Central System. Patient's devices will be connected to the application in a secure standard way and all the health data generated for this application will be stored into the Central System's Data vault. The application can also retrieve the history of personal health measurements, grant or revoke permits to the professionals, groups or caregivers stored in the blockchain and send notes to them in a secure way.

The second part of this platform is the one to be used by the caregiver to retrieve and review patient data to which has permits and send notes in the case it is considered necessary.

As the smartphone application, this system communicates with the Authentication System, the Blockchain solution and the Datavault in order to perform adequately. Nevertheless, this platform won't be installed in the user system but will be integrated with our Information Communications and Technologic Systems (ICT) and will be presented to the patient as a web application only accessible through the Hospital Network.

Both systems will communicate with the Central System provided by the SERUMS project using the Authentication Schema (UCY) and retrieving and storing data from the Data Vault (SOPRA) depending on the permits each user has on the Blockchain Solution (ACC)

The table below shows which problems or needs arise in the FCRB use case, what solutions need to be implemented and which technical implications it gives.

No.	Problem/Need	Solution	Remarks/Notes	Technical Implication
1	**Vital Sign Monitoring**			
a	The health professionals need to have all the vital signs stored in only one platform.	The Saludata smartphone application would gather all the measurements from different devices in only one platform facilitating a complete monitoring of the patients.	Professionals often find themselves having to access multiple platforms from different vendors and devices	**Smart Patient Health Record**: This is a centralised data source that allows all of the patient's records to be accessed from a single source, regardless of the source system
b	The ability to have a periodic stream of vital sign data from chronic disease patients would greatly help the health professionals to treat them	The Saludata smartphone application for patients is able to read vital signs measurements and store for review or for the professionals to see them.		**Authentication system**: patient and professional have to be authenticated and thus in possession of their security token (JWT), that will be used to utilize all the other technologies **Blockchain**: When health professionals need to access the new measurement data, it will be checked whether the requestor has the corresponding permission to access this patient's data. When positive, a request will be triggered to retrieve the data. **Smart Patient Health Record**: The data will be retrieved from this system and sent to the end-systems in a secure way using SFTP
2	**Improvement in Security**			
c	Data exchanged between health assistance actors and patients' needs to be secure.	In the whole platform securely communications, storage and access will be enforced	This includes each element in the communication chain or any component with which the system has relation	**Smart Patient Health Record:** When a rule is successfully triggered on the Blockchain, the corresponding set of data will be moved to a secure location in the Data Lake and encrypted by a unique public key provided by the request. Once it is encrypted, it

				can be passed to the Serums system, with only the correct private key allowing the decryption
3	**In compliance with the GDPR compliance and data protection**			
d	Joana needs to be able to grant and deny access to her data to the distinct actors in their health assistance (doctors, nurses, hospitals, services, etc)	Through the Saludata application Joana will be able to create and eliminate these permits, allowing her to manage granular access to her patient record.		**Authentication system**: patients and professionals have to be authenticated and thus in possession of their security token (JWT), that will be used to use all the other technologies. **Blockchain:** Permission rules to grant or restrict access can be defined by the patient for health organizations, individuals or groups.
e		Joana is able to remove access to certain professionals or assistance services that are part of an allowed organization.		**Blockchain:** Although default rules for the caregiver to access the patient is defined by the hospital administrator according to national regulations. Patients have the possibility to create specific rules to permit or restrict access.
4	**Improvement in Patient-Health Assistant communication**			
f	Communication between professionals and patients would be beneficial in the treatment of chronic diseases.	Both the patient application and the professional platform allow us to exchange messages through secure channels.		

2.3 USTAN - TOXICITY PREDICTOR

Emma is a 38 years old patient in the Western General Hospital (WGH) who has recently been diagnosed with breast cancer. To prevent the spreading of the tumour, she underwent breast surgery. After her surgery, chemotherapy treatment is given as a follow-up to her surgery. She is now dismissed and only visits the hospital for her chemotherapy appointment.

To ensure her recovery (i.e. by being able to determine the correct given dose for her treatment), a treatment plan and regimen have been established (this will be over several months with treatment in the hospital every three weeks). Emma also has comorbidity. As any cancer patient on chemotherapy, she might have higher toxicity levels as a result, but it is crucial to guarantee that the scale does not go above level two. Toxicity levels range from 0 (no toxicity) to 5 (very high toxicity).

Emma agrees on using and sharing data between treatment visits via the cancer data gateway and patient portal. Emma determines who in the medical team sees this information: The oncologist/nurse and her GP. Emma is also informed about how to use the web application and pass on relevant information to the clinical team.

Via a user-friendly web application, Emma can provide information on symptoms daily throughout the treatment. These Patient Reported Outcome Measures (PROMS) are based on questionnaires. Severe reported symptoms can be picked up by the clinical team and acted upon as soon as possible.

Note: The conditions that are being monitored and provided by the patients are nausea, vomiting, diarrhoea, constipation, oral mucositis, oesophagitis, neurotoxicity, , hypersensitivity, and fatigue. With this condition, the oncologist can determine the level of patients' toxicity.

The information Emma provided, data about patient characteristics, cancer information hospitalization data, and information about comorbidities are all combined.

This combined data will help clinicians adapt treatments better to Emma as an individual patient which results in controlled toxicity levels and improved health outcomes. It uses data from several patients treated over the years with comparable characteristics.

If during the treatments there are signs that toxicity levels are high or that the condition of Emma is deteriorating, one of the members of the clinical team (e.g. oncologist, specialist consultant, nurse, GP) notes in the irregularities in Emma's data and phones Emma to intervene.

During a phone call, a decision is made for the GP/nurse to visit Emma at home and provide some additional medication to alleviate symptoms. Admission to hospital is not necessary. As scheduled, Emma comes to WGH for the next chemotherapy treatment. This procedure is iterative until the end of the chemotherapy treatment.

Overall, Emma can have more personalised treatment. If a complication arises, the clinical team can act more quickly. Furthermore, Emma's well-being increases as she gets more involved in her treatment plans.

We are developing a dashboard to help oncologists observe, monitor, and analyse the condition of their patients over time. It can also be used to analyse the effect of different chemotherapy treatments when given to patients with similar characteristics, and consequently influence future decisions to improve the well-being and survival rate of patients. Our ultimate aim is to have a system to predict the toxicity of chemotherapy treatments based on history and feedback from patients. The overall features of the system is shown below.

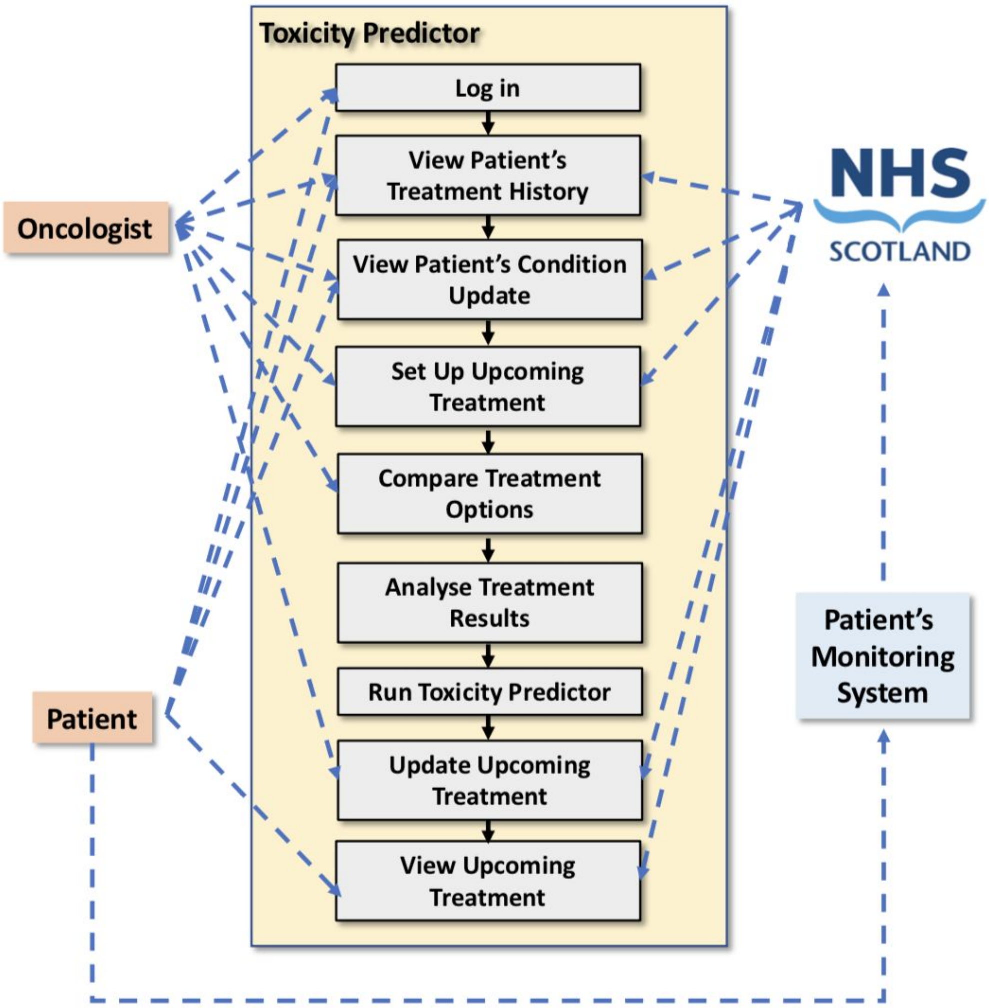

Toxicity Predictor
Log in
View Patient's Treatment History
View Patient's Condition Update
Set Up Upcoming Treatment
Compare Treatment Options
Analyse Treatment Results
Run Toxicity Predictor
Update Upcoming Treatment
View Upcoming Treatment
Oncologist
Patient
NHS SCOTLAND
Patient's Monitoring System

Figure 2. Use case analysis for USTAN

The table below shows which problems or needs arise in the USTAN use case, what solutions need to be implemented and which technical implications it gives.

No.	Problem/Need	Solution	Remarks/Notes
1	**More personalised treatment with improved and more regular monitoring of side effects. This will enable the clinical team to act more quickly when complications arise.**		
a	The oncologist needs to be able to observe the patient's condition before giving them the next chemotherapy treatment.	The developed system (SESO Gateway) provides the patient timeline visualisation, which shows the overall patient's cancer care journey. It allows the oncologist to see the latest patient's toxicity/condition measurement result.	The oncologist may need to access multiple platforms for monitoring the patient's condition.
b	Streamline the process of providing the patient's condition.	The monitoring application allows the patient to inform his/her condition anytime, anywhere. NHS Lothian starts developing a smartphone application which allows the patients to input their condition. The data is directly stored and collected in the NHS database.	The SESO Gateway can directly access the information from the database.
c	The oncologist can access tools that provide second opinions regarding the upcoming treatment of the patient.	The SESO Gateway has a feature for predicting the upcoming treatment result by inputting the treatment into machine learning models.	The accuracy of the predictor needs to be improved. At the moment, we develop it as proof of concept due to data scarcity.
2	**In compliance with the GDPR and data protection**		
d	The patient gives their consent for their data use	Assuring the patients that the application can securely access and store the patient data	At the moment, the NHS owns their patients’ data.

3 Proof of Concept (Leader: ACC)

The first proof of concept took place in January and February 2020 at all three end-user locations with all stakeholders involved as a result of the previously drawn up hospital-specific use cases. The measurements have been carried out both qualitatively, through semi-structured interviews and a small focus group, and quantitatively, through usability metrics and questionnaires. In this section we will further dedicate these measurements and by whom the measurements will be carried out.

3.1 End-users

In this consortium, three hospitals have been designated as end users to carry out the PoC measurements and to test the future Serums policy. These three end users are:

- Fundació Clínic per a la Recerca Biomèdica (FCRB)
- Zuyderland Medical Centre (ZMC)
- Edinburgh Cancer Centre (ECC)

Although the PoC should have been done in the three locations, the PoC carried out by USTAN at the ECC was not done due to delays in the obtainment of the Ethics committee approval.

3.2 Participants

For the PoC, three stakeholder groups were measured. The stakeholder groups involved were: patients, healthcare professionals and IT staff.

Patients (ZMC=31; FCRB=24) were included in the PoC measurement, with the largest group coming from the patient population belonging to the proposed hospital-specific use case (oncology patients from ECC, chronic diabetic/heart disease patients from FCRB and orthopaedical patients from ZMC). Patient data has been measured by means of questionnaires. These questionnaires were taken in each of the hospitals at the same time. In addition, an interview with one patient was conducted per end-user location to obtain more in-depth information in addition to the results of the questionnaires. The questionnaire and interview guide for the patient group can be found in Appendix 1. The patient chosen for the interview have been randomly selected from the entire patient participant population on a voluntary basis.

Care professionals (ZMC=4; FCRB=5) were carefully selected by the hospitals themselves and included in the PoC measurement after voluntary consent. Data of the care professionals was collected by means of semi-structured interviews per end-user location, in which the questions corresponded to the questions from the questionnaire. The healthcare professionals who were included for the measurements were specifically selected per hospital based on the proposed use case, so medical specialists as well as other healthcare providers (e.g. physiotherapists and nurses) have been included.

The *IT staff* (ZMC=5; FCRB=2) participating in this PoC measurement were measured by means of a small focus group per end-user location facilitated by the University of Cyprus (UCY). The IT staff were the final stakeholder group measured in order to use their input, mainly focused on the security of data processing, for the whole process and further developments of the Serums policy. Feedback from the security and IT experts will be used for further refining the Serums technologies in the next development life-cycle, *e.g.*, feedback on security aspects of the user authentication technology will be used as input and reported in D5.3 - Software on the Refined Verified User Authentication Scheme (due on M22).

3.3 Measurement design

The questions for both the questionnaires and the semi-structured interviews and focus group were prepared by UCY. The questions have been used to gain information about perceived usability, perceived memorability, perceived security, trust in the proposed Personalized User Authentication (PUA) system and patient trust. The focus group at the two end-user locations was taken from the IT staff from the relevant hospitals and was therefore a homogeneous internal focus group. Prior to all measurements, permission was requested from all participants by means of an Informed Consent drawn up in their own language. The research was approved for each hospital by the ethics committee before the baseline measurement was carried out.

3.4 Planning

In total three PoC measurements will be carried out throughout the Serums consortium. The first PoC (which is also described in full above) was carried out in month 13 (M13) in January and early February 2020. Subsequently, two more PoC measurements will be performed in all three hospitals in month 25 (M25) in January 2021 and month 34 (M34) in October 2021.

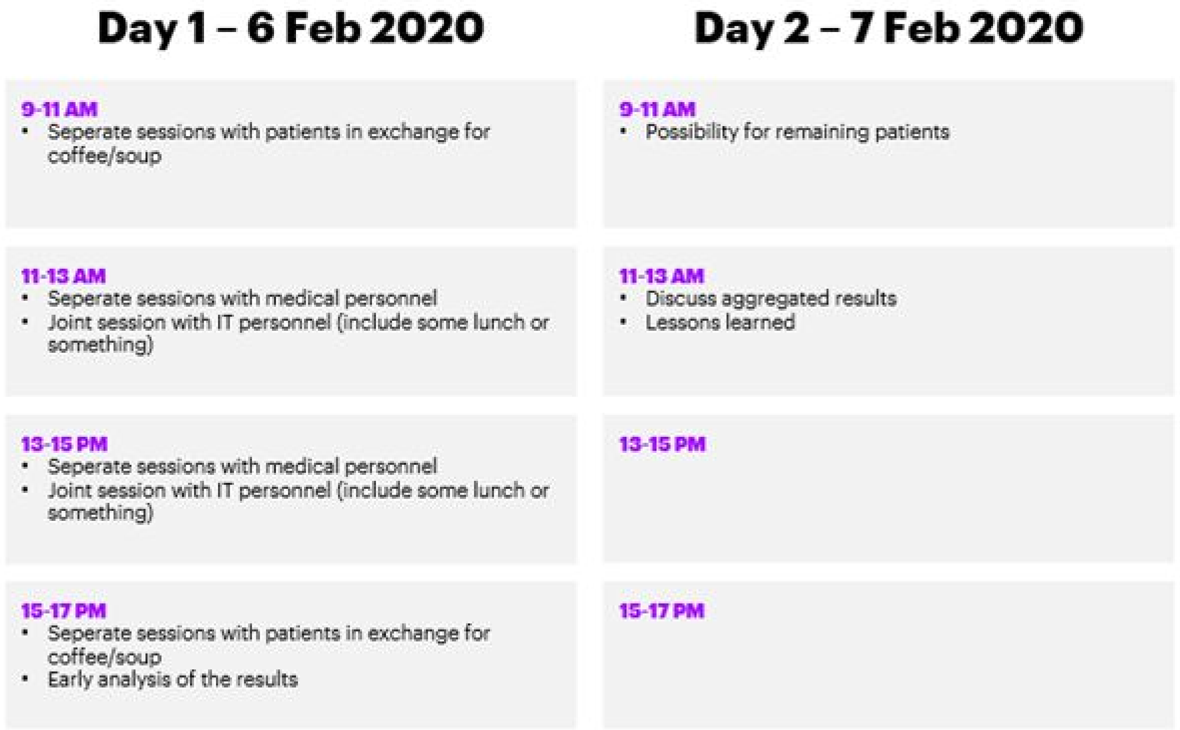
After this first PoC (M13) the results per end-user were evaluated and the lessons learned will be considered to improve the design of the next PoC (M25), including the questionnaires and interview guides developed by UCY. Also, the results over the different end-users have been compared and evaluated for further improvements of the next PoC (M25). This will be done again after the second PoC (M25) for the third PoC (M34). The results of the last PoC (M34) will also be compared with the results obtained during the baseline measurement where the current information standards per hospital apply.

Two months after the first and second PoC (M13 and M25), the initial results will be shared with the stakeholders via newsletters. The results of the last PoC (M34), will also be shared in a newsletter.

The first PoC was only measured in two of the three previously agreed locations due to USTAN not having approval before the date of the PoC or the date of submission of this Deliverable.

In the case of ZMC, the first PoC that took place on 14 and 15 January 2020. On the first PoC day, the patients were recruited and tested first in separate sessions in exchange for free coffee or soup, followed by separate semi-structured interviews with the medical personnel and a joint focus group session with the IT personnel. On the second PoC day there was some time scheduled to measure possible remaining patients and to discuss the aggregated results and lessons learned.

On the other hand, at FCRB the PoC took place on 20 and 21 January 2020. In the morning of the 20th, the patients were recruited by one of the resident doctors in the Hospital Clínic de Barcelona, and asked to test the authentication system proposed by UCY and answer a questionnaire in a consultation room next to the one of the doctor. That same day, as in ZMC the interviews with the IT personnel and focus groups with health professionals took place. The second PoC was fully invested in the gathering of more patients to answer the questionnaire and to discuss the aggregated results and lessons learned. Due to a lack of staff to do concurrent tests with patients these had to be carried out during the following days.



Day 1 – 6 Feb 2020	Day 2 – 7 Feb 2020
9-11 AM • Seperate sessions with patients in exchange for coffee/soup	**9-11 AM** • Possibility for remaining patients
11-13 AM • Seperate sessions with medical personnel • Joint session with IT personnel (include some lunch or something)	**11-13 AM** • Discuss aggregated results • Lessons learned
13-15 PM • Seperate sessions with medical personnel • Joint session with IT personnel (include some lunch or something)	**13-15 PM**
15-17 PM • Seperate sessions with patients in exchange for coffee/soup • Early analysis of the results	**15-17 PM**

Figure 3. Example of PoC at the Edinburgh Cancer Centre. In this image an example of the PoC (M13) planning can be found for the measurements with all stakeholder groups in the Edinburgh Cancer Centre corresponding to the oncology – breast cancer use-case that was formulated by USTAN.

4 Evaluation (Leader: FCRB)

The interviews and questionnaires from the PoC and the measurements of the metrics defined for each KPI mentioned in the Deliverable 7.1 allows FCRB to report the values of the evaluation of the First Version of the Serums technologies. These first evaluations are especially important to have a baseline of the state of the technologies to evaluate the progress and improvement achieved with the use of the technologies.

In the case of the Baseline measurements, due to the inexistence of equivalent technologies in the Organizations of the Use Case partners, values provided by the literature in the corresponding field has been reported, and in other cases, the measurement system itself worked for the current state. In the same way, some values in the first evaluation of the technologies there are some numbers that have not been reported (like KPI 3.5). This can be due to two reasons, the technology related to the KPI/ metric has not reached the point of being able to be evaluated in this aspect or that the metric requires some level of integration of the Serums technologies to be evaluated. The integration of the technologies at the Month 14 has not been achieved.

Although there is a previous section in which the PoC, here referred as Trial Measurement, has been explained, there is left to be explained how the baseline measurements where gathered. These were not taken in certain dates in the different Use Case locations, alternatively, there were taken during separately during the previous months of the PoC.

At the end of the chapter, the lessons learned from this dual stage task evaluation will be listed and reported for the expected use of providing feedback into different technical work packages, steering the development of Serums technologies in the subsequent phases of the project.

As defined in the Deliverable 7.1, three types of Success Indicators, that pertain to the next impacts, will be reported in the following pages i) Quantifiable improvement in the secure provision of health and care services ii) Significantly reduced risk of data privacy breaches iii) Increased patient trust and safety.

4.1 Remarks on the evaluation method

During the elaboration of the tasks that are reported in this Deliverable some issues arose on the matter of how the results of the Metrics and KPIs had to be generated and merged to obtain the Success Indicators. These issues were primarily two, the first being that in any previous Deliverable it was described the way in which the metrics and the KPIs with different units had to be merged and the second being that it was considered that all the KPIs had the same importance. The solution to these two problems is explained in the following sections (4.1.1 and 4.1.2).

4.1.1 The AMPI method

As can be seen in the following pages and in the Deliverable 7.1 the KPI consist of metrics, each of these having different units and ranges. This resulted in the problem of having to merge these numbers, sometimes being as diverse as 20 bits and 1.38E-23, into one single number (the KPI). For obvious reasons this was impossible to do by a simple arithmetic addition. The chosen method to achieve the calculations of the KPI has been the AMPI Index [1] (De Muro et al., 2011).

$$r_{ij} = \left[\frac{\left(y_{ij} - min\, y_i \right)}{\left(max\, y_i - min\, y_i \right)} \right]$$

Figure 4. AMPI index formula

As can be seen, to use this formula two limits have to be chosen, and in a very thoughtful way, since these will set the maximum and minimum range of the improvement and do not have to change from this initial report to the Final Evaluation of the Serums project.

Each of the intervals chosen for the measurements and KPIs (since some measurements are KPI by themselves) can be found on the following chart:

KPI/Measurement	**Minimum value**	**Maximum value**
KPI 1.1: Guessability / Theoretical Entropy	0 bits	105.4 bits
KPI 1.1: Guessability / Practical Entropy	0 bits	105.4 bits
KPI 1.1: Guessability / Guess Number	1	5.35256E+31
KPI 1.1: Guessability / Graphical password complexity	0%	100%
KPI 1.1: Guessability / Push notification accuracy	0%	100%
KPI 1.2: Password leaks (through social engineering) / Memory time	0	N*24
KPI 1.2: Password leaks (through social engineering) / Shoulder surfing	0%	100%
KPI 1.3: System vulnerability	24	240
KPI 2.1: Password cracking resistance	0%	100%
KPI 2.2: Data Breaches	10	110
KPI 2.3: Enhanced model privacy		
KPI 2.4: Granular access to patient record	0	10
KPI 2.5: Authorization data integrity	0	10
KPI 3.1: Perceived usability	1	5
KPI 3.2: Perceived memorability	1	5
KPI 3.3: Perceived security	1	5
KPI 3.4: Trust in the proposed PUA scheme	1	5
KPI 3.5: Patient trust	1	5
KPI 3.6: Data Analytics Model Utility	0%	100%
KPI 4.1: Data Analytics Model Utility	0%	100%

Intervals used to calculate the AMPI indicator

4.1.2 KPI and metric weights

During the gathering and calculation of the metrics and KPIs two issues arose. The first one was the finding that there were differences in the importance of the different measurements (KPIs and metrics) and that reporting them with the same importance into the Success Indicators would be a great mistake. Secondly, after reviewing some of the metrics it was found out that there could be some of them that weren't necessary or were not the object of the study. Only one of the metric is considered to share these circumstances, and it is the Theoretical Entropy on KPI 1.1.

To solve both of these problems, the technical partners with technologies evaluated by the KPIs directly agreed on a list of coefficients that would be used to weigh all their metrics/KPIs. These will grade the importance of the measurements in the evaluation of the Serums technologies.

These weights can be in the rage from 0 to 3:

0: This metric should not affect the Success Indicator, and will probably be removed in Deliverable 7.4 when KPIs are refined.

1: This measurement does not affect the Success Indicator in a very noticeable manner.

2: This measurement does affect the Success Indicator in an important way.

3: This measurement does have great importance in the Success Indicator.

Success Indicator	Coefficient	KPI	Coefficient	Metric
SI 1	1*	KPI 1.1: Guessability	0	Theoretical Entropy
			2	Practical Entropy
			3	Guess Number
			2	Graphical password complexity
			2	Push notification accuracy
	2*	KPI 1.2: Password leaks (through social engineering)	3	Memory time
			1	Shoulder surfing
	3	KPI 1.3: System vulnerability		
SI 2	2	KPI 2.1: Password cracking resistance		
	3	KPI 2.2: Data Breaches		
	1	KPI 2.3: Enhanced model privacy		
	2	KPI 2.4: Granular access to patient record		
	1	KPI 2.5: Authorization data integrity		

SI 3	2	KPI 3.1: Perceived usability	
	1	KPI 3.2: Perceived memorability	
	2	KPI 3.3: Perceived security	
	3	KPI 3.4: Trust in the proposed PUA scheme	
	3	KPI 3.5: Patient trust	
	1	KPI 3.6: Data Analytics Model Utility	
SI 4	1	KPI 4.1: Data Analytics Model Utility	

* these coefficients are left for possible modifications

4.2 Impact I, Success Indicator 1

The Success Indicator that will be used for measuring SERUMS progress and specific impact in terms of "Secure provision of health and care services", is:

- **S1)** Quantifiable improvement in secure provision of health and care services (by at least a factor of 2), evidenced by reduced vulnerability of the Smart Health Centre to common cyber-attacks, as measured by standard indexes determining system resilience, robustness and availability during and after the attacks.

Below, the various SERUMS tools/technologies and techniques contributing to S1, clear definitions of the Key Performance Indicators (KPIs) along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring S1, are provided.

S1) Quantifiable improvement in secure provision of health and care services (by at least a factor of 2), evidenced by reduced vulnerability of the Smart Health Centre to common cyber-attacks, as measured by standard indexes determining system resilience, robustness and availability during and after the attacks.	
SERUMS' Technologies Contributing in Achieving the Success Indicator: - **Personalized User Authentication (PUA)** - **Smart Patient Record (SPR)** - **Verification Technologies (VOT)**	
KPI 1.1: Guessability	**PUA**

<u>Key space</u>:

The set of all different permutations of a key. The key space range is determined by the adopted password policy which declares number of unique codes and password length.

Baseline Measurement:

Key space for the baseline study was calculated based on the user authentication policy applied at each end-user organization. A thorough description of the current authentication policies and practices of each organization is reported in *Deliverable 5.1 (Initial Report on Security Metrics and Authentication Policies)* which resulted based on a series of semi-structured interviews with various stakeholders at each end-user organization (security and IT experts, policy makers, project managers, etc.). Accordingly, the authentication password policy of each end-user organization is listed below:

- *USTAN password creation policy:* Textual password type, length>=8 characters, at least 1 lowercase letter, 1 uppercase letter, 1 number, 1 special character

- *ZMC password creation policy:* Textual password type, length>=8 characters, at least 1 lowercase letter, 1 uppercase letter, 1 number, 1 special character

- *FCRB password creation policy:* Textual password type, length>=8 characters, no restriction applied

Accordingly, the password key space for each organization is summarized in the table below.

	USTAN	***ZMC***	***FCRB***	
Baseline	***21,150,899,968***	***21,150,899,968***	***21,150,899,968***	

Trial Measurement:

We calculated the key space of the Serums user authentication technology (PoC1) following the same calculation as in the baseline study. Given that the Serums user authentication system is based on a novel flexible authentication approach, it consists of two complementary user authentication types; a text-based password and a picture-based password. Following existing practices and guidelines for the textual password [2, 3] and for the picture password [4, 5], we have set the following policies for all three end-user organizations.

- *Textual password creation policy:* A passphrase consisting of 16 characters with no composition restrictions applied

- *Picture password creation policy:* A combination of 8 gestures (tabs, lines and circles) made on an image with no composition restrictions applied

	USTAN	***ZMC***	***FCRB***	
1º Trial	***passphrase: 2.79905E+13*** ***graphical: 34,359,738,368***	***passphrase: 2.79905E+13*** ***graphical: 34,359,738,368***	***passphrase: 2.79905E+13*** ***graphical: 34,359,738,368***	

Commentary on results:

With regards to the baseline study, all three policies require a minimum of eight alphanumeric characters (94 characters including lower- and uppercase letters, numbers and special characters) in the creation of the textual passwords, hence the key space is the same for all three policies.

Compared to the PoC study, the textual passphrase of the Serums user authentication has a significantly larger key space since it requires users to enter a minimum of sixteen alphanumeric characters (94 characters including lower- and uppercase letters, numbers and special characters) as a passphrase, however with no composition restriction applied. Similarly, the key space of the suggested graphical password policy is larger than that of the baseline policies. Nonetheless, in future studies we will investigate the effects of these policies on usability and memorability aspects over time to evaluate the feasibility of the suggested policies.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline				
1 Trial				

Theoretical entropy:

Entropy is a measure on how difficult it is to guess a password. Entropy is measured as the expected value (in bits) of the information contained in a string, and can be related to authentication key strength by providing a lower bound on the expected number of guesses to find a text. The primary difference between key space and entropy is that key space is an absolute measure of maximum combinations, whereas entropy is related to how users select from the key space. The password key space (k_p) can be related directly to the maximum entropy as follows:

$$H_{max} = log_2 k_p \text{ [bits]}$$

The minimum and maximum value that could be achieved are 0 and 105.4 bits respectively.

Baseline Measurement:

The baseline is determined by the current authentication system for all end user systems. For measuring theoretical entropy, we followed state-of-the-art predictions reported in [2, 3]. Accordingly, considering that at all the end users, the password consisted of a minimum of 8 characters, this resulted in an entropy value of 52.7 at all end users. The difference between FCRB and both ZMC and USTAN is that the former does not have restrictions/rules bound to them, while the latter two do.

	USTAN	***ZMC***	***FCRB***	
Baseline	***52.7***	***52.7***	***52.7***	

Trial Measurement:

Contrary to the baseline, the trial results are based on the authentication rules created for the Serums user authentication system developed by UCY. Because the system consisted of two types of authentication, a picture password (8 gestures) and a passphrase (minimum 16 characters), each login credentials has its own theoretical entropy. According to [2-5], these are 53.7 bits and 105.4 bits for the picture password and passphrase respectively.

	Picture	***Passphrase***	
1º Trial	***53.7***	***105.4***	

Commentary on results:

Results reveal that the theoretical entropy of the PoC authentication system for both picture password and textual password are significantly higher than the entropy of the textual password systems of the baseline for all three end-user organizations.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline	***0.5***	***0.5***	***0.5***	***0.5***
1 Trial	***0.51, 1.00***	***0.51, 1.00***	***0.51, 1.00***	***0.75***

Practical entropy:

A true measure of theoretical entropy cannot be computed in cases of user-chosen authentication keys since users tend to choose more memorable than random keys. For measuring practical entropy, we have considered the work and results described in [2-5] which provide estimates of practical entropy of different password policies.

The minimum and maximum value that could be achieved are 0 and 105.4 bits respectively.

Baseline Measurement:

The baseline is determined by the current authentication system for all end user systems. At all the end users, the password consisted of a minimum of 8 characters. The difference between FCRB and both ZMC and USTAN is that the former does not have restrictions/rules bound to them, while the latter two do. Because of this, the practical entropy for FCRB is 29.43 bits, while for ZMC and USTAN it is 34.3 bits.

	USTAN	***ZMC***	***FCRB***	
Baseline	***34.3***	***34.3***	***29.43***	

Trial Measurement:

Contrary to the baseline, the trial results are based on the authentication rules created for the Serums user authentication system developed by UCY. Because the system consisted of two types of authentication, a picture password (8 gestures) and a passphrase (minimum 16 characters), each login credentials has its own practical entropy, which are 35 bits and 44.67 bits respectively.

	Picture	***Passphrase***	
1º Trial	***35***	***44.67***	

Commentary on results:

Results indicate that practical entropy is lower than theoretical entropy for all user authentication systems (both baseline and PoC). Furthermore, the practical entropy of the PoC authentication system for the textual password type is significantly higher than the entropy of the textual password systems of the baseline for all three end-user organizations. The picture password of the PoC authentication system has similar levels of practical entropy as the textual password systems of the USTAN and ZMC case study, while significantly larger than the textual password systems of the FCRB case study.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline	***0.33***	***0.33***	***0.28***	***0.31***
1 Trial	***0.33, 0.42***	***0.33, 0.42***	***0.33, 0.42***	***0.38***

Guess number:

Guess number refers to how many guesses a particular password-cracking algorithm with particular training data would take to guess a password.

The actual number of guesses is typically calculated by applying a certain brute-force attack on the actual user passwords in a database. However, due to security restrictions at each end-user organization, we could not get access on an actual database which includes the hashed user passwords, and hence we could not run an actual brute-force attack on the user passwords. Due to this, we are reporting the predicted guess numbers by following existing state-of-the-art studies and reports in [2-5] for similar policies.

The minimum and maximum number of guesses are 1 and 5.235256E+31 respectively.

Baseline Measurement:

The baseline is determined by the current authentication system for all end user systems. At all the end users, the password consisted of a minimum of 8 characters. For measuring the guess number, we have considered the work and results described in [2-5] which provide estimates of guess number of different password policies. The difference between FCRB and both ZMC and USTAN is that the former does not have restrictions/rules bound to them, while the latter two do. Because of this, the guess number for FCRB is 723,290,519, while for ZMC and USTAN it is 21,150,899,968.

	USTAN	***ZMC***	***FCRB***	
Baseline	***21,150,899,968***	***21,150,899,968***	***723,290,519***	

Trial Measurement:

Contrary to the baseline, the trial results are based on the authentication rules created for the Serums user authentication system developed by UCY. Because the system consisted of two types of authentication, a picture password (8 gestures) and a passphrase (minimum 16 characters), each login credentials has its own guess number. According to [2-5], these are 34,359,738,368 and 2.79905E+13 guesses for the picture password and passphrase respectively.

	Graphical	***Passphrase***	
1^o Trial	***34,359,738,368***	***2.79905E+13***	

Commentary on results:

Results indicate that the guess number of the PoC authentication system for the textual and picture password types is significantly higher than the guess number of the textual password systems of the baseline for all three end-user organizations.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline	***21,150,899,968***	***21,150,899,968***	***723,290,519***	
1 Trial	***34,359,738,368 2.79905E+13***			

Graphical password complexity:

An additional measure for graphical passwords is graphical password complexity which describes how complex a graphical password is based on the users' image selections and gestures. This is currently work in progress within WP5 and will be available by the end of the second development live-cycle, and hence evaluated in PoC2. For calculating graphical password complexity we will consider existing state-of-the-art works such as Sun et al. [6] which considers various measurements in their strength metric such as the size of the password (*i.e.*, total number of images), physical length of the password (*i.e.*, the sum of the Euclidean distances between the selected images of the password); total number of intersections (*i.e.*, when two non-consecutive line segments have a common point); and the number of overlaps of the password pattern (*i.e.*, when a line segment of the password pattern is covered by another segment). The higher the score, the more complex the password is.

The minimum and maximum value of graphical password complexity is 0% and 100% respectively.

Graphical password complexity is not applicable for the baseline study since all three end-user organizations do not implement a graphical password system. This metric will be applied in a future trial for the Serums graphical password system.

Push notification accuracy:

Measures the accuracy of the users' approval of push notifications. Given that the push notification system has not been implemented in PoC1 and is part of our work in WP5 for the next development life-cycle, push notification accuracy has not been evaluated in the current study and will be evaluated in PoC2 evaluation.

KPI 1.2: Password Leaks (through Social Engineering)	**PUA**

Memory time:

Memory time will be measured over time by considering actual login attempts of the end-users. In particular, memory time refers to the greatest length of time between a password creation and a successful password login using the same password. Large memory times indicate higher memorability. Memorable passwords lead to potentially less social engineering-based password leaks because users will not need to follow coping strategies (*e.g.*, write down their passwords).

Memory time data could not be measured for the baseline study since the relevant data was not supported by the existing authentication systems at the end-user organizations (or not available due to privacy regulations and policies of the corresponding organization). In addition, given that memory time requires participants using the system over time, we did not measure this in PoC1 since the aim of the first evaluation of the user authentication system was to elicit the users' perceptions and likeability towards the first PoC authentication system.

Another metric for memorability relates to the number of password resets as well as time needed to login. For the baseline authentication system, we received summarized password reset data from ZMC. The table below summarizes the amount of resets and the average amount of days between the resets at ZMC starting from January 01, 2019 until October 31, 2019.

Baseline Measurement:

Number of resets at ZMC	**Average amount of days between resets**	**Total number of occurrences**
1	0	1893
2	91	738
3	69	222
4	64	92
5	42	20
6	47	6

Trial Measurement:

During the PoC study, participants interacted with the current user authentication prototype by creating a textual and picture password and then using their password to login. Within this session, we measured the number of resets required by the end-users. The number of resets for each user authentication type are summarized in the table below.

	ZMC	**FCRB**

	Passphrase	Picture	Passphrase	Picture
# resets	0/15	1/16	0/4*	1/18
Login time (sec)	15.41	6.19	n/a	6.14

**note: the number of occurrences for each password type varies since users chose and logged in with their preferred authentication type (textual vs. graphical). In the case of the FCRB study, 4 users chose a passphrase to login, while 18 users chose a picture password.*

Commentary on results:

With regards to the PoC, results are promising with regards to the number of resets and login time since only 2 end-users were required to reset their password in both case studies. With regards to login time, results suggest that the picture password authentication system is efficient in both case studies, while an increase of time required to login is observed in the case of passphrase-based login in ZMC. While results are promising, further studies are required to investigate the PoC authentication system over time in order to increase external validity and investigate memory time.

KPI 1.3: System Vulnerability	**SPR**

System Vulnerability: The measure of how susceptible the system is via penetration testing as well as the security of the authentication methods. The types of penetration that we will use will be both external network and internal network penetration testing. This will allow us to see how vulnerable the system is from the outside as well as once they have gained some form of access. Additionally, we will score the security of the programming languages used, as well as the lifespan of security support that is left for these.

Baseline Measurement: This took form as a questionnaire that was given to the use case partners. Due to the sensitive nature of the questions, it was only possible to receive a complete and usable set of responses from FCRB.

Each result of the questionnaire was scored on a scale of 1 - 10, with 1 being critical and 10 being no known issues. These scores were calculated through known knowledge of vulnerabilities as well as length of time left of support for the various programming languages and frameworks. This gave a minimum score of 24 and a maximum score of 240, with FCRB scoring 109.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline	***N/A***	***N/A***	***109***	***109***

Trial Measurement: At the time of writing, we have been unable to take a trial measurement for this KPI. This is due to the system still being very early in development and is still awaiting integration between the technical partners.

Commentary on results: As expected, the security of the existing system is high. However, there are areas to improve upon by using more up to date versions of the programming languages, as well as the underlying operating system on which the platform runs. Additionally there are further small changes we can make to the system security, such as the hardening of password encryption, which will have measurable improvements over the baseline score. The above score has been applied to the AMPI method to give the following result.

	USTAN	*ZMC*	*FCRB*	*TOTAL*
Baseline	*N/A*	*N/A*	***0.39***	***0.39***

4.3 Impact II, Success Indicator 2

The Success Indicator that will be used for measuring SERUMS progress and specific impact in terms of “Less risk of data privacy breaches caused by cyber-attacks”, is:

- **S2)** Significantly reduced risk of data privacy breaches (at least 75%), evidenced by quantitative metrics showing the quantity of private data that is revealed through a number of common cyber-attacks.

Below, the various SERUMS tools/technologies and techniques contributing to S2, clear definitions of the Key Performance Indicators (KPIs) along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring S2, are provided.

S2) Significantly reduced risk of data privacy breaches (at least 75%), evidenced by quantitative metrics showing the quantity of private data that is revealed through a number of common cyber-attacks.	
SERUMS’ Technologies Contributing in Achieving the Success Indicator: - **Credential Hardening (CH)** - **Smart Patient Record (SPR)** - **Privacy-preserving Data Analytics (PDA)** - **Verification Technologies (VOT)** - **Distributed Ledger Technology (DLT)**	
KPI 2.1: Password Cracking Resistance	**CH**
<u>Password cracking rate:</u> Password cracking rate will be measured in a leaked database storing hardened credentials through an offline brute-force attack. This is work in progress within WP5 and will be evaluated in the second evaluation cycle (PoC2).	
KPI 2.2: Data Breaches	**SPR**
Data Breaches: The measure of data that will be able to be accessed by unauthorised or inappropriate sources. Through the use of the log files for the database we will take measurements on how much data can be accessed by both an unknown user and a known user for unauthorised reasons. Additionally, we can apply a score against the ease at which physical copies of the data can be generated.	

Baseline Measurement: This took form as a questionnaire that was given to the use case partners. Due to the sensitive nature of the questions, it was only possible to receive a complete and usable set of responses from FCRB.

Each result of the questionnaire was scored on a scale of 1 - 10, with 1 being critical and 10 being no known issues. The questions covered the access that staff have to patients' records as well as the options available to create physical copies of the data. This gave a minimum score of 11 and a maximum score of 110, with FCRB scoring 49.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline	***N/A***	***N/A***	***49***	***49***

Trial Measurement: At the time of writing, we have been unable to take a trial measurement for this KPI. This is due to the system still being very early in development and is still awaiting integration between the technical partners.

Commentary on results: The baseline results were to be expected. The hospital must balance the ability to see relevant patient data in an emergency with the potential for data breaches. There are sensible policies in place, however the Serums system would remove the need for physical copies of data to be made which will result in a higher score. The above score has been applied to the AMPI method to give the following result.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline	***N/A***	***N/A***	***0.44***	***0.44***

KPI 2.3: Enhanced Model Privacy **PDA**

KPI 2.4: Granular access to patient record **DLT**

This KPI will measure how granular the solution will offer the ability to manage the access to the patient record.

We have defined 4 levels of permission granularity of patient record access with a scale of 1-4 where level 4 is the most satisfactory level. The DLT solution aims to reach level 4.

1. No digital access management of the patient record
2. Access can be managed by the organization (e.g. hospital) at patient record level. which means the record can be accessed or not as a whole for the caregiver.
3. Access can be managed by the organization (e.g. hospital) at a granular level (e.g. a subset of the patient record)
4. Access can be managed by the organization (e.g. hospital) and the patients themselves at a granular level (e.g. a subset of the patient record)

Baseline Measurement:

The baseline measurement was collected based on the assessment of the current systems in place in the hospitals.

	USTAN	*ZMC*	*FCRB*	*TOTAL*
Baseline	***1***	***1***	***1***	***1***

Commentary on results:

Currently there is no equivalent solution in place to manage the permissions digitally. , thus the result will be (level 1) for all parties. At the time of writing, we have been unable to take a trial measurement for this KPI. Although the specific component for the DLT solution has already been developed, it is yet to be integrated into the overall solution.

	USTAN	*ZMC*	*FCRB*	*TOTAL*
Baseline	***0***	***0***	***0***	***0***

KPI 2.5: Authorisation Data Integrity **DLT**

This KPI will be measuring how resilience the current system is handling the authorisation data.

In case a party on the DLT network is compromised, and it has been identified that data has been tampered with. The solution is able to identify the exact data that has been tampered with and retrieve the original value. We have defined 4 levels of with a scale of 1-4 where level 4 is the most satisfactory level. The DLT solution aims to reach level 4.

1. No means to traceback when (authorization) data has been compromised.
2. Is able to retroactively track when data is compromised but cannot track which specific data was compromised.
3. Retroactive tracking when data is compromised, and is able to identify which data has been compromised but cannot restore the original value.
4. Retroactive tracking when the data is compromised, and is able to identify and restore the data which has been compromised.

Baseline Measurement:

The baseline measurement was collected based on the assessment of the current systems in place in the hospitals.

	USTAN	*ZMC*	*FCRB*	*TOTAL*
Baseline	***1***	***1***	***1***	***1***

Commentary on results:

Currently, permissions are not being managed digitally, thus the result will be (level 1) for all parties. At the time of writing, we have been unable to take a trial measurement for this KPI. Although the specific component for the DLT solution has already been developed, it is yet to be integrated into the overall solution.

	USTAN	*ZMC*	*FCRB*	*TOTAL*

Baseline	***0***	***0***	***0***	***0***

4.3 Impact III, Success Indicators 3 and 4

The Success Indicators that will be used for measuring SERUMS progress and specific impact in terms of "Increased patient trust and safety" are:

- **S3)** Quantifiable improvement in levels of patient trust in the provision of smart health care (at least a factor of 2), evidenced by patient surveys and questionnaires.
- **S4)** Quantifiable improvement in patient safety (at least a factor of 2), evidenced by reduced risk of harm through incorrect treatments or medicines mediated by reduced risk of tampering with medical records, and measured vulnerabilities of connected medical systems.

Below, the various SERUMS tools/technologies and techniques contributing to S3 and S4, clear definitions of the Key Performance Indicators (KPIs) along with their corresponding metrics, as well as the Baseline and the Trial measurements that will be used for measuring S3 and S4, are provided.

S3) Quantifiable improvement in levels of patient trust in the provision of smart health care (at least a factor of 2), evidenced by patient surveys and questionnaires

SERUMS' Technologies Contributing in Achieving the Success Indicator:

- **Personalized User Authentication (PUA)**
- **Smart Patient Record (SPR)**
- **Privacy-preserving Data Analytics (PDA)**

KPI 3.1: Perceived Usability	**PUA**

One of the primary aims of the first PoC evaluation of the user authentication system was to get feedback from end-user patients on aspects such as likeability towards the suggested flexible and personalized approach in authentication, and the end-users' perceptions towards usability, memorability, security and trust. For this purpose, we have designed a questionnaire by following state-of-the-art works and guidelines on usability, user experience, security and trust (*e.g.*, SUS, AttrakDiff, Technology Acceptance models, etc.).

With regards to perceived usability, we have asked questions that relate to the password creation process and login, *e.g.*, *"Overall, how difficult or easy do you find the password creation task?"*, *"Overall, how difficult or easy do you find the login task?"*, *"I could easily log on to the FlexPass password system"*, etc. Users rated the statements through a 5-point Likert scale (*e.g.*, 1: Not at all - 5: Absolutely).

Baseline measurement:

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline		***3.8***	***3.71***	***3.75***

ZMC baseline (patients)

With regards to questions that relate to the password creation difficulty, the majority of users find the creation process medium-to-easy (18/19 - Difficult: 1; Medium: 7; Easy: 6; Very easy: 5). With regards to login difficulty, 16 out of 19 find the login task as easy to use. When users were asked to report on the password reset difficulty, responses varied, with the majority stating that the reset process has moderate difficulty (Difficult: 2; Medium: 10; Easy: 3; Very easy: 4). Also, users have reported mixed methods for resetting their password (Email: 7; Mobile app: 5; Reset tool: 7).

ZMC (feedback from professionals)

Similar to the patient responses, the majority of responses received from the ZMC professionals reveal that the baseline user authentication system is usable. In particular, 13/19 professionals perceive the password creation as easy to use, 17/19 professionals login in the system without any difficulties, and 16/19 professionals find the reset process as easy to use.

FCRB baseline (patients)

With regards to questions that relate to the password creation difficulty, the majority of users find the creation process medium-to-easy (17/21 - Difficult: 2; Difficult-Medium: 2; Medium: 3; Easy: 4; Very easy: 10). With regards to login difficulty, 16 out of 21 find the login task as easy to use. When users were asked to report on the password reset difficulty, responses similarly varied as in the ZMC case, with the majority stating that the reset process has moderate difficulty (10/21). Also, users have reported mixed methods for resetting their password (Email: 9; Mobile app: 7).

FCRB (feedback from professionals)

Mixed responses were received from professionals with regards to perceived usability. A total of 8/19 professionals find the password creation task as easy to use, 5 as moderate difficulty, and 6 professionals find the task as difficult to use. Similar findings are observed in the case of login task with 11/19 professionals rating the login task as easy to use, while 4 professionals find the login task as moderate and difficult to use respectively. With regards to the password reset process, 11/19 professionals find the task as easy to use, 7 rated moderate difficulty and 1 user rated the task as difficult.

Trial measurement:

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Trial 1		***4.06***	***3.65***	***3.85***

ZMC PoC (patients)

Patients at ZMC found the password creation task as easy to use (password creation - easy: 21/31; moderate: 8/31). Similarly, with regards to password login usability, the majority of users found the login task as easy to use (25/31). When users were asked whether they would like to use the Serums user authentication system as their alternative password system, *the majority of users (25/31) were positive and would be willing to use it as an alternative authentication system.*

When ZMC end-user were asked on whether they like to personalized and flexible approach for user authentication, the majority of users extremely (18/31) or very much (9/31) liked the idea, with 5 users either moderately (2/31), slightly (2/31) or not liking (1/31) the idea.

ZMC (feedback from professionals)

All ZMC professionals (4) like the flexible and personalized authentication paradigm, 3 professionals believe that the Serums authentication technology would be a good alternative method for patients, 1 showed moderate interest. Overall, 3 professionals find the authentication system as easy to use while 1 professional rated the system as difficult to use.

FCRB PoC (patients)

Patients at FCRB found the password creation task as easy to use (easy: 14/24; moderate: 6/24) and fast to use (fast: 14/24; moderate: 6/24). Nonetheless, 4 patients found the password creation task as both difficult and slow to use. Similarly, in the case of login usability, the majority of users found the login task as easy to login (easy: 21/24; moderate: 5) while 3 users found the login task as difficult to use.

With regards to likeability towards the flexible and personalized approach, the majority of users very much (11/24) liked the idea, with 2 users extremely like the idea, 7 moderately, 3 slightly and 1 user did not like the idea.

FCRB (feedback from professionals)

The majority of FCRB professionals (4/5) like the flexible and personalized authentication paradigm, as well as believe that the Serums authentication technology would be a good alternative method for patients, 1 showed moderate interest. Overall, 4 professionals find the authentication system as easy to use while 1 professional rated the password creation task ease of use as moderate. All professionals believe that the creation task is fast to use. A total of 2 professionals believe that patients will easily log in while 3 professionals rated ease of use as moderate.

Likeability	**Extremely**	**Very much**	**Moderately**	**Slightly**	**Not at al**
ZMC	18	9	2	2	1
FCRB	2	11	7	3	1
Total	***20***	***20***	**9**	**5**	**2**

Commentary on results:

Results are encouraging for further research on the idea of flexible and personalized user authentication since the majority of users liked the proposed approach, as well as perceived both the password creation process and login task as easy to use. In comparison to the baseline measurements, the PoC authentication system has improved usability in the ZMC case study (3.8 *vs.* 4.06) whereas in the case of FCRB, the usability value has been slightly decreased from 3.71 to 3.65. Based on qualitative feedback received from the end-users this can be accredited to some users (*n*=4) that had difficulties in creating gestures on the image during the graphical password creation task.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline		***3.8***	***3.71***	***0.68***
1 Trial		***4.06***	***3.65***	***0.71***

KPI 3.2: Perceived Memorability	**PUA**

Similar to perceived usability, we have asked participants questions on whether they recalled effectively their passwords and whether the login process was mentally demanding. Users rated the statements through a 5-point Likert scale (*e.g.*, 1: Not at all - 5: Absolutely).

Baseline measurement:

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline		***4.36***	***3.63***	***3.49***

ZMC baseline (patients)

The majority of patients from the ZMC case study responded positively to perceived password memorability; 8 users find the mental demand to recall their password as very low: 8; 10 require a low mental demand, and 1 users requires a moderate mental demand.

ZMC (feedback from professionals)

All professionals responded that they require low mental demand to recall their password (Very low: 12; Low: 6).

FCRB baseline (patients)

Mixed responses on password memorability were received in the FCRB case study with 11 users having very low or low mental demand to recall their password, 5 users a moderate demand and 5 users high or very high demand.

FCRB (feedback from professionals)

A total of 9/19 professionals require low mental demand during password recall, 6 professionals rated mental demand as moderate while 4 users require a high mental demand during password recall.

Trial measurement:

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Trial		***4.09***	***4.16***	***4.12***

ZMC PoC (patients)

The majority of patients from the ZMC case study responded positively to perceived password memorability after their interaction with the Serums user authentication system. The majority of users reported a very low or low mental demand (21/31; moderate: 5/31) in recalling their password. In addition, 25/31 users could effectively recall their password.

ZMC (feedback from professionals)

All ZMC professionals (4) believe that the login task will require low mental demand from patients, 3 believe that patients will easily remember their password while 1 professional believes that patients will have difficulties to login.

FCRB PoC (patients)

Similar to the FCRB case study, the majority of patients responded positively to perceived password memorability after their interaction with the Serums user authentication system. The majority of users reported a very low or low mental demand (19/24) in recalling their password. In addition, 19/24 users could effectively recall their password. Nonetheless, 4 patients reported that they found the authentication system as mentally demanding

FCRB (feedback from professionals)

A total of 3 professionals believe that the login task will require low mental demand from patients (1 rated moderate mental demand), 2 believe that patients will easily remember their password while 3 professionals believe that patients will moderately remember their passwords.

Commentary on results:

Overall, in the ZMC case, users were positive towards perceived memorability in both the baseline and PoC user authentication system with the ZMC baseline system scoring higher levels of memorability. In the case of FCRB, results reveal a significant increase of perceived memorability for the PoC system compared to the baseline system (4.16 *vs.* 3.63). Results are encouraging for further investigating the proposed flexible and personalized user authentication system since in both PoC case studies, patients reported high levels of perceived memorability. Nonetheless, further research is needed to investigate the proposed system over time in order to increase external validity of the proposed approach.

	TOTAL
Baseline	***0.62***
1 Trial	***0.78***

KPI 3.3: Perceived Security	**PUA**

For perceived security, we have asked participants questions on whether they believe the user authentication system is secure, whether they believe their password is strong, etc. Users rated the statements through a 5-point Likert scale (*e.g.*, 1: Not at all - 5: Absolutely).

Baseline measurement:

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline		***3.82***	***3.59***	***3.71***

ZMC baseline (patients)

The majority of the ZMC participants perceived the baseline user authentication system as secure (Very secure: 6; Secure: 10; Medium: 3) and commented that their password is strong (Very strong: 4; Strong: 6; Medium: 8; Weak: 1). Finally, with regards to the password reset process, 6 users find the process very secure, while the majority of users (13) believe that the password reset process has a moderate security.

ZMC (feedback from professionals)

Professionals perceive the baseline user authentication system as secure (14/19) while 4 professionals perceive it as moderately secure. With regards to password strength, 10/19 professionals believe their password is strong, while 8 professionals believe it has medium strength. Similarly, 14/19 professionals find the reset process as secure, while 4 professionals believe it has medium security.

FCRB baseline (patients)

The majority of the FCRB participants perceived the baseline user authentication system as secure (Not secure at all: 1; Not secure: 2; Medium: 5; Secure: 11; Very secure: 2) and commented that their password is strong (Very weak: 1; Weak: 0; Medium: 8; Strong: 10; Very strong: 2). Similarly, with regards to the password reset process, the majority of users believe that the password reset process is secure (Not secure at all: 1; Not secure: 1; Medium: 7; Secure: 9; Very secure: 3).

FCRB (feedback from professionals)

Mixed responses were received from professionals with regards to perceived security. A total of 4/19 users perceive the system as not secure, 8 as moderately secure and 7 as secure. The majority of professionals believe their password has medium strength (12/19), 2 believe it is weak while 5 believe it is strong. Similarly, the majority of professionals believe that the password reset process has medium security (11/19), 2 believe it is weak while 6 believe it is strong.

Trial measurement:

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Trial		***4.02***	***3.75***	***3.88***

ZMC PoC (patients)

The majority of ZMC participants perceived the Serums user authentication system as secure (25/31) while 5 users and 1 user rated it to have moderate and limited security. With regards to password strength, 25 users believe that their password in the Serums user authentication is strong.

ZMC (feedback from professionals)

Mixed responses were received on perceived security; 2 professionals find the system as secure, while 1 user believes it has medium security and another 1 believes it is not secure. With regards to password strength, 2 professionals believe the passwords are strong, while another 2 believe the passwords have medium strength.

FCRB PoC (patients)

The majority of FCRB participants perceived the Serums user authentication system as secure (17/24), 2 participants rated it to have moderate security, while 5 participants believe the system is not secure. With regards to password strength, 16 users believe that their password in the Serums user authentication is strong, 4 participants believe it has moderate strength and 4 participants believe the generated passwords are weak.

FCRB (feedback from professionals)

All FCRB professionals (5) perceive the authentication system as secure as well as the passwords as strong.

Commentary on results:

Overall, users' responses with regards to perceived security were positive towards both user authentication systems (baseline and PoC). A comparison between the two systems reveal that in both case studies, users perceived the PoC system as more secure than the baseline system.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline		***3.82***	***3.59***	***0.67***
1 Trial		***4.02***	***3.75***	***0.72***

KPI 3.4: Trust in the proposed PUA scheme **PUA**

For perceived trust, we have asked participants questions that relate to their trust towards the user authentication system technology, its ability to protect their data privacy, their trust on security and trust to keep their data safe from cybercriminals. Users rated the statements through a 5-point Likert scale (*e.g.*, 1: Not at all - 5: Absolutely).

Baseline measurement:

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline		***4.01***	***3.56***	***3.78***

ZMC baseline (patients)

The majority of ZMC participants indicated that they trust the baseline user authentication system. Specifically, 15/19 trust the authentication technology while 4 participants have moderate trust towards the technology. With regards to trust on privacy, 16/19 participants trust the authentication system to protect their data privacy, 2 users have moderate trust while 1 user has no trust towards the system with regards to privacy. With regards to trust towards security, 13/19 participants are not worried about the security of the authentication system while 3 participants are mildly worried, and another 3 participants are worried about the authentication system security. Finally, when participants were asked on whether they trust the authentication system to protect their account and data from cybercriminals, 15/19 participants trust the system, while 2 participants indicated moderate trust and another 2 indicated not trust.

ZMC (feedback from professionals)

Overall, professionals trust the baseline authentication technology (17/19), as well as trust the system to protect their privacy (13/19). However, in the case of trust towards its security and safety against cybercriminals, a considerable number of professionals (6) commented that they are worried about the security of the authentication technology (12/19 trust the security), and 5 professionals do not trust that their data is safe. Nonetheless, 11/19 professionals showed trust towards the system to keep their data safe against cybercriminals.

FCRB baseline (patients)

The majority of FCRB participants indicated that they trust the baseline user authentication system. Specifically, 14/21 trust the authentication technology while 5 participants have moderate trust towards the technology, and 2 participants do not trust the technology. With regards to trust on privacy, 13/21 participants trust the authentication system to protect their data privacy, 4 users have moderate trust while 4 users have no trust towards the system with regards to privacy. With regards to trust towards security, 13/21 participants are not worried about the security of the authentication system while 4 participants are mildly worried, and another 4 participants are worried about the authentication system security. Finally, when participants were asked on whether they trust the authentication system to protect their account and data from cybercriminals, 13/21 participants trust the system, while 5 participants indicated moderate trust and another 3 indicated not trust.

FCRB (feedback from professionals)

Mixed responses were received from professionals with regards to perceived trust. A total of 12/19 users trust the technology, 5 show moderate trust and 4 do not trust the technology. With regards to trust towards protecting their privacy, 8/19 professionals trust the system, 6 show moderate trust and 5 do not trust the system. A total of 9/19 professionals (9/19) are somewhat worried about the security of the authentication system, while 9 trust the system, 1 user does not trust the system. Finally, 10/19 professionals trust the system to keep their data safe against cybercriminals, 7 have moderate trust while 2 professionals do not trust the system.

Trial measurement:

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Trial		***3.96***	***4***	***3.98***

ZMC PoC (patients)

The participants of the ZMC PoC study responded positively with regards to trust towards the Serums user authentication technology. With regards to trust towards the technology, 22/31 trust the Serums authentication technology, 7 have moderate trust while 2 users do not trust the technology. Furthermore, 22/31 participants have trust towards the Serums authentication system to protect their privacy, while 8 users have moderate trust and 1 user has no trust. A total of 18/31 users are not worried about the security of the authentication system, 8 participants are somewhat worried while 5 users are worried about the security. Finally, 21/31 users trust the authentication system to keep their data safe against cybercriminals, 8 have moderate trust while 2 users do not trust the system.

ZMC (feedback from professionals)

Mixed responses were received on perceived trust; 2 professionals trust the technology, while 2 users do not trust the technology. With regards to trust to protect privacy, 3 professionals trust the system and 1 does not trust the system. A total of 2 professionals are not worried about the system's security, while another 2 professionals are worried. Finally, 3 professionals trust the authentication system to keep the patients' data safe against cybercriminals, and 1 professional does not trust the system.

FCRB PoC (patients)

The participants of the FCRB PoC study similarly responded positively with regards to trust towards the Serums user authentication technology. With regards to trust towards the technology, 18/23 trust the Serums authentication technology, 2 have moderate trust while 3 users do not trust the technology. Furthermore, 18/23 participants have trust towards the Serums authentication system to protect their privacy, while 2 users have moderate trust and 3 users have no trust. A total of 16/23 users are not worried about the security of the authentication system, 2 participants are somewhat worried while 5 users are worried about the security. Finally, 16/23 users trust the authentication system to keep their data safe against cybercriminals, 4 have moderate trust while 3 users do not trust the system.

FCRB (feedback from professionals)

All FCRB professionals trust the Serums authentication technology across all trust dimensions (technology, privacy, security, safety). In the case of trust with regards to safety against cyber criminals, 1 professionals rated moderate trust.

Commentary on results:

Overall, participants in both evaluation studies (baseline and PoC) at both end-user organizations (ZMC and FCRB) trust the user authentication technologies. A comparison between system versions suggest that in the case of the FCRB study, patients scored higher trust levels for the PoC authentication system compared to the baseline, while in the case of the ZMC case, trust levels were similar for both systems.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline		***4.01***	***3.56***	***0.69***
1 Trial		***3.96***	***4***	***0.74***

KPI 3.5: Patient Trust	**SPR**

Questionnaire:

USTAN: N/A

ZMC: 19 Respondents

FCRB: 19 Respondents

Baseline Measurement: We provided two questions to the end users to be asked that were graded on a scale of 1 - 5. These were designed to measure the patients' trust in the current system. These questions were asked in conjunction with a series of other questions related to other KPIs throughout this deliverable. Both participating hospitals were able to ask 19 patients which gave a maximum potential score of 190 and a minimum of 38.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline	***N/A***	***136***	***128***	***132***

Commentary on results: As expected, the patients exhibited a high trust in the current system. From speaking to the patients, it became clear that this is based on a lifetime of using the hospitals and the in-built assumption that the data within the hospitals' systems is safe. This is an area we may not be able to improve upon with the Serums system. These figures were then applied to the AMPI method to give the following result.

	USTAN	***ZMC***	***FCRB***	***TOTAL***
Baseline	***N/A***	***0.64***	***0.59***	***0.62***

KPI 3.6: Data Analytics Model Utility **PDA**

Metrics:

To measure the Data Analytics Model Utility we compare the accuracy of state-of-the-art privacy preserving machine learning approaches with the accuracy of the approaches developed in WP3 for a given level of privacy. To measure the level of privacy we use the mathematical framework of (e; δ)-differential privacy.

- **Metric:** This will be defined in the second version of this Deliverable (D7.4).

Trial Measurements:

The trial measurements are initially performed using only established publicly available benchmark datasets. In particular we are using the MNIST Dataset and the Freiburg Groceries. As soon as the models have been integrated into the system and are therefore available for our use case partners, we will perform the measurements also on the selected use cases.

Both approaches, state-of-the-art and our novel approach, are able to achieve any level of privacy, from very high to zero. The achievable privacy and accuracy of a model are always competing properties. Therefore, this KPI is strongly connected to KPI2.3. To measure the difference in utility between those approaches we compare the achieved testing accuracy of the competing models for a given level of privacy.

In this first trial we evaluate the utility of our distributed deep-learning models that uses our novel optimal noise adding mechanism in comparison the state-of-the-art approach that uses Gaussian noise.

Details about the datasets, the setup of the experiments and the results have been explained in chapter 2 of deliverable D3.1.

Baseline Measurements:

For the baseline measurements we performed several experiments with the given datasets. In every experiment we changed the variables of the privacy metric and calculated the testing accuracy. The results are described in detail in chapters 2.4.1 for the MNIST and 2.4.2 for the Freiburg Groceries Dataset. Looking the results, we can see that for a given level of privacy our novel approach achieves a higher or the least the same accuracy in the models output.

How Impact on the Success Indicator will be measured

KPI 4.1 Higher utility of the models leads to better diagnostics thus resulting in improved patient safety.

S4) Quantifiable improvement in patient safety (at least a factor of 2), evidenced by reduced risk of harm through incorrect treatments or medicines mediated by reduced risk of tampering with medical records, and measured vulnerabilities of connected medical systems.

SERUMS’ Technologies Contributing in Achieving the Success Indicator - **Privacy-preserving Data Analytics (PDA)**	
KPI 4.1: Data Analytics Model Utility	**PDA**

Metrics:

To measure the Data Analytics Model Utility we compare the accuracy of state-of-the-art privacy preserving machine learning approaches with the accuracy of the approaches developed in WP3 for a given level of privacy. To measure the level of privacy we use the mathematical framework of (e; δ)-differential privacy.

- **Metric:** This will be defined in the second version of this Deliverable (D7.4).

Trial Measurements:

The trial measurements are initially performed using only established publicly available benchmark datasets. In particular we are using the MNIST Dataset and the Freiburg Groceries. As soon as the models have been integrated into the system and are therefore available for our use case partners, we will perform the measurements also on the selected use cases.

Both approaches, state-of-the-art and our novel approach, are able to achieve any level of privacy, from very high to zero. The achievable privacy and accuracy of a model are always competing properties. Therefore, this KPI is strongly connected to KPI2.3. To measure the difference in utility between those approaches we compare the achieved testing accuracy of the competing models for a given level of privacy.

In this first trial we evaluate the utility of our distributed deep-learning models that uses our novel optimal noise adding mechanism in comparison the state-of-the-art approach that uses Gaussian noise.

Details about the datasets, the setup of the experiments and the results have been explained in chapter 2 of deliverable D3.1.

Baseline Measurements:

For the baseline measurements we performed several experiments with the given datasets. In every experiment we changed the variables of the privacy metric and calculated the testing accuracy. The results are described in detail in chapters 2.4.1 for the MNIST and 2.4.2 for the Freiburg Groceries

Dataset. Looking the results, we can see that for a given level of privacy our novel approach achieves an higher or the least the same accuracy in the models output.

How Impact on the Success Indicator will be measured

KPI 4.1 Higher utility of the models leads to better diagnostics thus resulting in improved patient safety.

4.4 Summary

Success Indicator	KPI	Technology	Baseline	Trial
S1	**1.1: Guessability**	PUA		
	1.2: Password Leaks	PUA		
	1.3: System Vulnerability	SPR	0.39	
S2	**2.1: Password Cracking Resistance**	CH		
	2.2: Data Breaches	SPR	0.44	
	2.3: Enhanced Model Privacy	PDA		
	2.4: Granular access to patient record	DLT	0	
	2.5: Authorisation Data Integrity	DLT	0	
S3	**3.1: Perceived Usability**	PUA	0.68	0.71
	3.2: Perceived Memorability	PUA	0.62	0.78
	3.3: Perceived Security	PUA	0.67	0.72
	3.4: Trust in the proposed PUA scheme	PUA	0.69	0.74

	3.5: Patient Trust	SPR	0.62	
	3.6: Data Analytics Model Utility	PDA		
S4	**4.1: Data Analytics Model Utility**	PDA		

5 Conclusions

As can be seen in the Evaluation summary (Section 4.4) some improvements can be already reported, but the fact that the integration of the technologies has not been achieved means that the overall or in some cases individual improvement or success it is not easily evaluated. Needless to say the evaluation in the First Trial (PoC 1) is quite reduced due to this great amount of unmeasured Metrics and KPIs. In addition, the fact that in the Use Case Organizations the technologies developed in the Serums project have no similar counterparts in most of the cases makes leaves either a difficultly evaluable situation or a very obvious improved one, like in the case of the Distributed Ledger Technology. This leaves the main conclusion that until at least the next Proof of Concept, when all the technologies have been integrated or at least more individually mature, a full evaluation and a report of the improvement won't be possible.

The main findings with regards to the Serums PoC authentication technology are encouraging for further investigating the suggested flexible and personalized user authentication approach since users were positive with regards to all four dimensions (perceived usability, memorability, security and trust) towards the Serums authentication technology. In particular, the majority of users in both case studies like the flexible and personalized authentication paradigm (40/56 extremely and very much like the paradigm) and commented that they would be willing to adopt the authentication technology as their main authentication method. In comparison to the baseline system, in the majority of cases, the PoC system scored higher values of security *(baseline practical entropy .31 vs. PoC practical entropy .38)*, perceived usability *(baseline .68 vs. PoC .71)*, memorability *(baseline .62 vs. PoC .78)*, security *(baseline .67 vs. PoC .72)* and trust *(baseline .69 vs. PoC .74)*. Next steps entail improving the interaction design of the picture password system based on feedback received from users as well as investigate different policy effects on usability and security of the picture password system.

In regards to the system vulnerability, the current system is perfectly adequate as it is already similar to the systems used by the end users today. The backend especially is completely in line with what we would expect from something used to store highly sensitive data. A key area which Serums will be able to improve upon however is the continuous improvement in security technology. By utilising cutting edge practices, hardware, and software, we will be able to harden many of the potential vulnerabilities, without a noticeable downgrade in performance.

Furthermore, it is clear that the hospitals have systems in place to minimise potential data breaches, whilst at the same time ensuring that data is readily available in an emergency to whomever, wherever, within the hospital's internal system. This only breaks down through either nefarious use of the systems, made possible by the readily available access to printing or removable media at many of the stations throughout the hospital, or when the patient is transporting data themselves to an external healthcare provider. Whilst Serums will have some impact on the first of these two scenarios through the stricter access controls placed on their data, it is the second scenario that we will make a huge impact on.

6 References

[1] De Muro, P., Mazziotta, M. & Pareto, A. Composite Indices of Development and Poverty: An Application to MDGs. *Soc Indic Res* 104, 1–18 (2011). https://doi.org/10.1007/s11205-010-9727-z

[2] Burr, W., Dodson, D., Polk, W. (2006). Electronic authentication guideline. Technical report, NIST

[3] Komanduri, S., Shay, R., Kelley, P., Mazurek, M., Bauer, L., Christin, N., Cranor, L., Egelman, S. (2011). Of passwords and people: measuring the effect of password-composition policies. In ACM CHI '11, ACM Press, 2595-2604

[4] Microsoft Developers' Blog. Signing in with a picture password. https://docs.microsoft.com/en-us/archive/blogs/b8/signing-in-with-a-picture-password

[5] Zhao, Z., Ahn, G., Seo, J., Hu, H. (2013). On the security of picture gesture authentication. In USENIX Security (SEC'13), USENIX Association, 383–398

[6] Sun, C., Wang, Y., Zheng, J. (2014). Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. Journal of Information Security and Applications, 19(4-5), 308-320.

Appendix 1 Documents of the PoC 1

This appendix contains:

1- User Authentication First Proof of Concept Study - Guidelines for Study with Patients
2- User Authentication Study - Instructions for Participants
3- User Authentication First Proof of Concept Study - Guidelines for Semi - structured Interviews with Professionals and Security/IT Experts
4- Baseline Questionnaire DigiD English
5- PoC Questionnaire ZMC English

User Authentication First Proof of Concept Study

Guidelines for Study with Patients

Objective

The main purpose of this study is to demonstrate to the patients the FlexPass paradigm and the system, and elicit their opinions, preference and likeability with regards to FlexPass using a questionnaire.

About FlexPass

FlexPass is a user authentication system that allows users to create secret picture passwords. Instead of remembering complex text passwords, the only thing you need to remember is 3 secret spots on an image by drawing them on the image.

In order to make your graphical password more memorable and easier to use, FlexPass provides images tailored to each user's prior daily life activities and experiences to make them more memorable and secure.

In addition, in case you like to use textual passwords, you can also create a secret passphrase which you can use to flexibly switch between your graphical password in order to login.

Unique Incremental User IDs

In order to relate the user interactions among the different components of the FlexPass system and their feedback with the questionnaire, we suggest printing a small sheet with a unique incremental User ID (*e.g.*, 1, 2, 3, etc.). The user will enter this unique identification code when required in different forms of the system (*i.e.*, Registration Form, Push Notification Form, and Questionnaire).

Links to Access the System

(1) Landing Page: This is the main link for the desktop/laptop device:

http://serums.cs.ucy.ac.cy:9000/web_app

This is the landing page for the end-users, from which they can read instructions about the FlexPass approach, as well as get access to the following:

a) **Demo:** The demo page on which they can experiment by drawing gestures on a background image
b) **Video Demo:** A video demo we created that shows a dry-run of the password creation and login tasks
c) **Sign Up button:** Redirects to the registration form

(2) Push Notification: This is the link that simulates the push notification for the mobile device:

http://serums.cs.ucy.ac.cy:9000/web_app/push_notification

Study Procedure Instructions

The study procedure is split in four main phases as follows:

Phase A – Explain the FlexPass Paradigm

In the very beginning, it is important to explain the FlexPass paradigm to the end-users and get their first impressions about the suggested authentication approach. As soon the participants understand the paradigm, we have included a drop-down list asking the participants whether they like the idea (or not) of creating picture passwords with personalized images tailored to their prior daily life activities and experiences. Before proceeding with Phase B, we suggest that the participant also goes through the Demo page to experiment and get an initial idea of how the picture password system works, as well as see the Video Demo.

Phase B – Password (Picture and/or Text) Creation Process

In this phase, participants will start going through the whole authentication process by initially creating a picture password and/or textual password. The participants start by clicking on the Sign Up button which redirects them to the registration form. Participants will enter their unique User ID provided by the researchers in the beginning of the study. Participants are then redirected to a page that illustrates 6 images from public locations of their hospital and then select one preferred image that will be used to draw 3 secret spots on that image. Upon creating their picture password, users can then create a secret passphrase (with minimum 16 characters, not restrictions applied) by reflecting their secret story used in the picture password.

Phase C – Login Process and Push Notification

In this phase, participants are required to choose their preferred authentication method (picture or text) and accordingly provide their secret picture password or passphrase to login. Upon successful login, users are then required to approve a push notification on a mobile device (tablet or smartphone). For this purpose, we have implemented a medium-fidelity prototype of the push notification process which will be available to the participants on the mobile device for approval or rejection.

Important Note: In order to relate the push notification action with the current user's session, the push notification form requires the participant's User ID to be filled. We suggest that the researcher already enters the participant's User ID in this form in the beginning of the participant's session.

As soon the user approves the notification, the interaction with the system is completed and a relevant success message is shown to the user. In addition, a link is shown that redirects the users to a questionnaire aiming to get qualitative feedback about their interactions with FlexPass.

Phase D – Questionnaire

In the final step, users are required to fill in a questionnaire to elicit their opinions, preference and likeability with regards to FlexPass.

Other Important Remarks

- Keep track of end-users User ID, so you assign the next number to each new end-user. If a User ID is already used, the system will not allow it, therefore, you will have to provide a different User ID.
- After an end-user creates a picture password (and an optional passphrase), they will be redirected to the login page (or they could use the navigation links at the top of the page to go to the login page).
- During the login task, once they enter their assigned User ID and click the Next button, the flexible paradigm takes place, *i.e.*, it will either present two alternative ways of authenticating (*e.g.*, text, graphical) if the passphrase has been previously set, or present only the graphical way if the passphrase has not been previously set.
- If the login credentials are successful, they will be redirected to a page that presents the message about the two-factor authentication. At this point, you will have to prepare the mobile device (*i.e.*, go to link (2) above and enter their User ID). If they reject the notification, nothing will happen. You could re-enter their User ID and they accept it. The login will be considered successful only if they accept the push notification on the mobile device. If they accept the notification, they will be redirected to the final screen that contains the external link to the Google Forms questionnaire.
- Once a patient is finished with the entire task (password interaction and questionnaire), it is a good idea to ask them to logout by pressing the logout button at the top right of any PoC page (or feel free to do it yourself) before a new patient arrives at the same device. This is recommended mostly for clearing cookies and any cached information.

User Authentication Study

Instructions for Participants

Thank you for participating in this user study for the EU Horizon 2020 research project Serums.

The main purpose of this study is to elicit the end-users opinions, preference and likeability with regards to FlexPass, a novel authentication system that aims to improve usability and memorability of passwords and at the same time preserve security.

About FlexPass

FlexPass is a user authentication system that allows users to create secret picture passwords. Instead of remembering complex text passwords, the only thing you need to remember is 3 secret spots on an image by drawing them on the image.

In order to make your graphical password more memorable and easier to use, FlexPass provides images tailored to each user's prior daily life activities and experiences to make them more memorable and secure.

In addition, in case you like to use textual passwords, you can also create a secret passphrase which you can use to flexibly switch between your graphical password in order to login.

Study Procedure Instructions

Please find below the main steps you need to follow for completing the study:

Step 1 – Create Picture Password

1) A set of background images will be displayed on the screen. The images will depict content that you are familiar with. You are required to select one image from the set of images, on which you will then create your picture password.

2) Next, you will create a picture password by drawing 3 gestures on an image. You could use any combination of circles, straight lines and taps (clicks).

3) Memorize the size, the position, the directionality, and the ordering of your gestures. These gestures will be your secret picture password.

Step 2 – Create Textual Password (optional)

In case you like to use textual passwords, you can also create a secret passphrase (minimum 16 characters long) which you can use to flexibly switch between your graphical password in order to login.

In order to make your password more memorable, we suggest reflecting the secret you created in the graphical password as your passphrase. For example, *"the day I had lunch with my friends at the cafeteria"*.

Step 3 – Login and Approval

In order to login you need to choose your preferred authentication method (picture or text) and then proceed to login by entering your secret password.

To increase the security of the login process, you also need to approve your login through a notification that will show up on your tablet device.

Last Step 4 – Questionnaire

In the last step, please answer a questionnaire to indicate your opinions, preference and likeability with regards to FlexPass.

Thank you for participating in this user study and help us improve FlexPass!

User Authentication First Proof of Concept Study

Guidelines for Semi-structured Interviews with Professionals and Security/IT Experts

Objective

The objective of the study with the professionals (*i.e.*, doctors, nurses, caregivers), and the security and IT experts is to get feedback about their preference and opinion about the FlexPass system, get insights and discuss various aspects on usability, security, user acceptance and trust, and whether they believe it would be a good alternative authentication method for patients.

About FlexPass

FlexPass is a user authentication system that allows users to create secret picture passwords. Instead of remembering complex text passwords, the only thing you need to remember is 3 secret spots on an image by drawing them on the image.

In order to make your graphical password more memorable and easier to use, FlexPass provides images tailored to each user's prior daily life activities and experiences to make them more memorable and secure.

In addition, in case you like to use textual passwords, you can also create a secret passphrase which you can use to flexibly switch between your graphical password in order to login.

Study Procedure Instructions

Please find below the main steps you need to follow for completing the study:

Step 1 – Demonstrate the FlexPass System

For each professional, it is important to *i)* explain the idea of FlexPass; and *ii)* demonstrate all the components of FlexPass (*i.e.*, password creation, login, push notification, reset process) and then provide them the questionnaire.

Please use the following links for demonstrating the system:

(1) Information about the FlexPass approach and starting point of the FlexPass system:

http://serums.cs.ucy.ac.cy:9000/web_app

(2) This is the link that simulates the push notification for the mobile device:

http://serums.cs.ucy.ac.cy:9000/web_app/push_notification

Step 2 – Semi-structured Interview

In order to get feedback from the professionals and the security/IT experts, we suggest following a semi-structured approach when conducting the interviews based on a set of predefined questions. For this purpose, we have prepared a questionnaire that should be used as a guideline and basis for the discussions with the professionals and the security/IT experts.

You may access the same questionnaire for each end-user organization from the links below:

ZMC-Professionals-English: https://forms.gle/xhvaY4ZELzaDPv8p7

FCRB-Professionals-English: https://forms.gle/TusZoPwyBxXzNY9h6

USTAN-Professionals-English: https://forms.gle/CYMG1DXYpoRFzonG7

User Authentication Study

Thank you for participating in this user study for the EU Horizon 2020 research project Serums.
The main purpose of this study is to identify end-user behaviors and opinions with regards to the DigiD user authentication system and common practices they follow. DigiD is an identity management platform which government agencies of the Netherlands, including the Tax and Customs Administration, can use to verify the identity of Dutch residents on the Internet.
Before taking part in this study please read the information below. When you are finished, click on the "I consent" option at the bottom of this page if you understand the statements and freely consent to participate in this study.

*Required

About Serums and Contact Information

The Serums project (Securing Medical Data in Smart Patient-Centric Healthcare Systems) deals with security and privacy of future-generation healthcare systems, putting patients at the center of future healthcare provision, enhancing their personal care and maximizing the quality of treatment they receive.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826278.

For more information about the project, please visit the project’s official Website: http://serums-smartpatient.com

How to contact us:
Department of Computer Science, University of Cyprus

Prof. Andreas Pitsillides
Andreas.Pitsillides@ucy.ac.cy

Dr. Marios Belk
belk@cs.ucy.ac.cy

Information about the User Study

The user study will take about 15 minutes. Your answers will be treated confidentially and anonymously.

Participation in the study is voluntary and can be cancelled at any time. You can terminate your participation at any time. In doing so, you also object to the use of your data collected up to that point.

The data collected as part of this study and described above will be treated confidentially. Furthermore, the results of the study will be published in anonymous form, i.e., without your data being personally identifiable.

There are no risks to individuals participating in this study beyond those that exist in daily life.

For further questions about this study, the project or about the way your contribution will be used, please feel free to contact us.

Thank you for taking your time to support this project!

Consent
By clicking the "Next" button you declare that you
1) understand the purpose of the study,
2) are over 18 years old,
3) voluntarily participate in this study, and
4) have taken note and understand the study information presented above.

1. **I consent to the processing of my personal data in accordance with the information provided herein** *

Mark only one oval.

○ I consent

○ I do not consent *Skip to "Thank you."*

General Background

Please provide some information with regards to your educational background and computer literacy

2. **What is your Age range (in years)?** *

Mark only one oval.

○ 18-25
○ 26-35
○ 36-45
○ 46-55
○ 56-65
○ 66 and above

3. **What is your highest degree of education?** *

Mark only one oval.

○ Ph.D. Studies
○ Master Studies
○ Bachelor Studies
○ High School
○ Primary School

4. **How would you rate your computer literacy?** *

Mark only one oval.

	1	2	3	4	5	
Beginner	○	○	○	○	○	Advanced

5. **Do you currently have regular access to a computer?** *

Mark only one oval.

○ Yes

○ No

Password Usage and Behavior

Please provide some information with regards to your general usage and behavior with the DigiD authentication system

6. **Which are the most common types of password systems you use to access your DigiD?** *

Tick all that apply.

□ Textual password

□ Textual password with SMS verification

□ DigiD app

□ Other: ____________________

7. **Which one is the common interaction device you use to access government services with your DigiD?** *

Mark only one oval.

○ Desktop

○ Tablet

○ Smartphone

8. **How many government services (e.g., municipality, pension, etc.) do you access with your DigiD?** *

Mark only one oval.

○ 1

○ 2

○ 3

○ 4

○ 5

○ 6

○ More than 6

9. **How many times per month do you login with your DigiD?** *

Mark only one oval.

○ 1
○ 2
○ 3
○ 4
○ 5
○ 6
○ More than 6

10. **How often do you need to reset your DigiD password because you cannot remember your password?** *

Mark only one oval.

○ Once every week
○ Once every month
○ Once every three months
○ Once every six months
○ Never
○ Not applicable

11. **Do you use the same password on multiple accounts?** *

Mark only one oval.

○ Yes
○ No
○ Sometimes

12. **Do you save your DigiD password in your Web browser?** *

Mark only one oval.

○ Yes
○ No
○ Sometimes

13. **Do you write down your DigiD password?** *

Mark only one oval.

○ Yes
○ No
○ Sometimes

14. **Which memorability practices do you employ for building your password? In other words, what practices do you follow to memorize more effectively your password (e.g., includes names, birth dates, etc.)?** *

Password Creation

Please rate your experience and perceptions with regards to the password creation system and process of DigiD

15. **Overall, how difficult or easy do you find the password creation task?** *

Mark only one oval.

	1	2	3	4	5	
Very difficult	○	○	○	○	○	Very easy

16. **Overall, how secure do you find the DigiD authentication system?** *

Mark only one oval.

	1	2	3	4	5	
Very insecure	○	○	○	○	○	Very secure

17. **How strong do you believe your current DigiD password is?** *

Mark only one oval.

	1	2	3	4	5	
Very weak	○	○	○	○	○	Very strong

Password Login

Please rate your experience and perceptions with regards to the DigiD login system

18. **Overall, how difficult or easy do you find the DigiD login task?** *

Mark only one oval.

	1	2	3	4	5	
Very difficult	○	○	○	○	○	Very easy

19. **How mentally demanding is the DigiD login task?** *

Mark only one oval.

	1	2	3	4	5	
Very low	○	○	○	○	○	Very high

Password Reset

Please rate your experience and perceptions with regards to the DigiD password reset system and process

20. **Overall, how difficult or easy do you find the password reset process of DigiD?** *

Mark only one oval.

	1	2	3	4	5	
Very difficult	○	○	○	○	○	Very easy

21. **Overall, how secure do you find the password reset process of DigiD?** *

Mark only one oval.

	1	2	3	4	5	
Very insecure	○	○	○	○	○	Very secure

22. **How would you prefer to reset your password in the DigiD system?** *

Tick all that apply.

□ Call helpdesk
□ Email notification
□ Smartphone application
□ Password reset tool
□ Answer security questions
□ Receive a new password through traditional mail
□ Visit the organization's helpdesk and provide an Identification Document (ID)
□ Other: ____________________

Trust

Please rate your trust towards the current DigiD password system

23. **I trust in the technology the DigiD password system is using** *

Mark only one oval.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

24. **I trust in the ability of the DigiD password system to protect my privacy** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

25. **I am not worried about the security of the DigiD password system** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

26. **I trust the DigiD password system to protect my account and data from cybercriminals** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

Password Experience and Preference

Please explain your overall experience, preference and opinions with regards to the DigiD password system and authentication systems in general

27. **What have been your best experiences when interacting with the DigiD password system? (example: "I like that I can quickly login using the DigiD app")**

28. **What have been your worst experiences when interacting with the DigiD password system? (example: "One day, I had to urgently login to access some important files and I was locked out of my account because I forgot my password")**

29. **Would you be willing to use an alternative user authentication type to login to your user account?** *

Mark only one oval.

○ Yes

○ No

30. **If you answered "Yes" to the previous question, which of the following alternative user authentication schemes would you prefer to login?**

Tick all that apply.

□ Picture passwords (require users to memorize images or draw secret patterns as their secret key)

□ Biometrics (e.g., fingerprint)

□ Object-based authentication (e.g., card)

□ Traditional textual passwords

□ Other:

31. **Explain the reasoning behind your answer in the previous question**

32. **How would you imagine the perfect password system?**

Trust in healthcare provider

Please rate the trust you have in healthcare providers handling your medical data.

33. **How capable or incapable do you consider healthcare providers in handling medical data securely?**

Mark only one oval.

	1	2	3	4	5	
Very incapable	○	○	○	○	○	Very capable

34. **Please rate your agreement with the following statement: “I trust my healthcare provider to handle my medical data in a safe and secure manner”**

Mark only one oval.

	1	2	3	4	5	
Stronly disagree	○	○	○	○	○	Strongly agree

Stop filling out this form.

Thank you

No data has been processed

Powered by
Google Forms

User Authentication Study

Thank you for participating in this user study for the EU Horizon 2020 research project Serums. The main purpose of this study is to elicit the end-users opinions, preference and likeability with regards to FlexPass, a novel user authentication system that aims to improve usability and memorability of passwords and at the same time preserve security.
Before taking part in this study please read the information below. When you are finished, click on the "I consent" option at the bottom of this page if you understand the statements and freely consent to participate in this study.

*Required

About Serums and Contact Information

The Serums project (Securing Medical Data in Smart Patient-Centric Healthcare Systems) deals with security and privacy of future-generation healthcare systems, putting patients at the center of future healthcare provision, enhancing their personal care and maximizing the quality of treatment they receive.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 826278.

For more information about the project, please visit the project’s official Website: http://serums-smartpatient.com

How to contact us:
Department of Computer Science, University of Cyprus

Prof. Andreas Pitsillides
Andreas.Pitsillides@ucy.ac.cy

Dr. Marios Belk
belk@cs.ucy.ac.cy

Information about the User Study

The user study will take about 15 minutes. Your answers will be treated confidentially and anonymously.

Participation in the study is voluntary and can be cancelled at any time. You can terminate your participation at any time. In doing so, you also object to the use of your data collected up to that point.

The data collected as part of this study and described above will be treated confidentially. Furthermore, the results of the study will be published in anonymous form, i.e., without your data being personally identifiable.

There are no risks to individuals participating in this study beyond those that exist in daily life.

For further questions about this study, the project or about the way your contribution will be used, please feel free to contact us.

Thank you for taking your time to support this project!

Consent
By clicking the "Next" button you declare that you
1) understand the purpose of the study,
2) are over 18 years old,
3) voluntarily participate in this study, and
4) have taken note and understand the study information presented above.

1. **I consent to the processing of my personal data in accordance with the information provided herein** *
Mark only one oval.

○ I consent
○ I do not consent *Skip to "Thank you."*

General Background

Please provide some information with regards to your educational background and computer literacy

2. **What is your Age range (in years)?** *
Mark only one oval.

○ 18-25
○ 26-35
○ 36-45
○ 46-55
○ 56-65
○ 66 and above

3. **What is your highest degree of education?** *
Mark only one oval.

○ Ph.D. Studies
○ Master Studies
○ Bachelor Studies
○ High School
○ Primary School

4. **How would you rate your computer literacy?** *
Mark only one oval.

	1	2	3	4	5	
Beginner	○	○	○	○	○	Advanced

5. **Do you currently have regular access to a computer?** *
Mark only one oval.

○ Yes
○ No

Password Creation

Please rate your experience and perceptions with regards to the FlexPass password creation system and process

6. **Overall, how difficult or easy do you find the password creation task in FlexPass?** *

Mark only one oval.

	1	2	3	4	5	
Very difficult	○	○	○	○	○	Very easy

7. **Overall, how slow or fast do you find the password creation task in FlexPass?** *

Mark only one oval.

	1	2	3	4	5	
Slow	○	○	○	○	○	Fast

8. **How long (in seconds) did you need to create your password in FlexPass?**

9. **Overall, how secure do you find the FlexPass password system?** *

Mark only one oval.

	1	2	3	4	5	
Very insecure	○	○	○	○	○	Very secure

10. **How strong do you believe your FlexPass password is?** *

Mark only one oval.

	1	2	3	4	5	
Very weak	○	○	○	○	○	Very strong

11. **Did the image scenery impact your password selections (i.e., did you create a certain story when selecting points on the image, did you consider any past experiences as part of your selections)? If yes, please explain how the image scenery impacted your password selections** *

12. **How did you decide where to draw the gestures on the image?** *

13. **How did you decide which gesture (tap, line, or circle) to draw?** *

14. **What strategy did you follow to create your password?** *

15. **What type of background image would you prefer?** *

Password Login

Please rate your experience and perceptions with regards to the FlexPass login system

16. **Overall, how difficult or easy did you find the login task in FlexPass?** *
Mark only one oval.

	1	2	3	4	5	
Very difficult	○	○	○	○	○	Very easy

17. **How mentally demanding was the login task?** *
Mark only one oval.

	1	2	3	4	5	
Very low	○	○	○	○	○	Very high

18. **I could easily log on to the FlexPass password system** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

19. **I effectively remembered my password** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

Password Reset

Please rate your experience and perceptions with regards to the FlexPass password reset system and process

20. **Overall, how difficult or easy do you find the password reset process of the FlexPass system?** *
Mark only one oval.

	1	2	3	4	5	
Very difficult	○	○	○	○	○	Very easy

21. **Overall, how secure do you find the password reset process of the FlexPass system?** *
Mark only one oval.

	1	2	3	4	5	
Very insecure	○	○	○	○	○	Very secure

Trust

Please rate your trust towards the FlexPass password system

22. **I trust in the technology the FlexPass password system is using** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

23. **I trust in the ability of the FlexPass password system to protect my privacy** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

24. **I am not worried about the security of the FlexPass password system** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

25. **I trust the FlexPass password system to protect my account and data from cybercriminals** *
Mark only one oval.

	1	2	3	4	5	
Strongly disagree	○	○	○	○	○	Strongly agree

Password Experience and Preference

Please explain your overall experience, preference and opinions with regards to the FlexPass password system

26. **What are the positive aspects you like in the FlexPass password system?**

27. **What are the negative aspects you do not like in the FlexPass password system?**

28. **Would you be willing to use the FlexPass password system as an alternative user authentication system to login to your user account?** *
Mark only one oval.

○ Yes
○ No

29. **Explain the reasoning behind your answer in the previous question**

Thank you

No data has been processed

Powered by