

ITEA-20050 - Secur-e-Health

Privacy preserving cross-organizational data analysis in the healthcare sector

HARDWARE-BACKED CRYPTOGRAPHIC IDENTITY & MEDICAL SENSORS


Deliverable: List of physical wearables, sensors and devices compatible with the software system to enable secure user identification

Due date of deliverable: (31-03-2023)
 Actual submission date: (06-04-2023)

Start date of Project: November 2021

Duration: 36 months

Responsible WP2: Kelvin Zero

Dissemination level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Service	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (excluding the Commission Services)	

DOCUMENT INFO

Author

Author	Company	E-mail
Sharmila Raveendra	Kelvin Zero	s.raveendra@kzero.com
Finn Siegel	OFFIS	finn.siegel@offis.de
Sophia Tatiyosyan	Stryker	sophiaanais.tatiyosyan@stryker.com
Ricarda Merfort	UKAC	rmerfort@ukaachen.de

Documents history

Document version #	Date	Change
V0.1	March 31 st , 2023	Starting version
V1.0	April 5 th , 2023	First version

Table of Contents

1	INTRODUCTION.....	5
1.1	Expected results	5
2	LIST OF PHYSICAL WEARABLES, SENSORS AND DEVICES COMPATIBLE WITH THE SOFTWARE SYSTEM TO ENABLE SECURE USER IDENTIFICATION	6
2.1	Biometrics Smart Card	6
2.1.1	DESCRIPTION.....	6
2.1.2	INTEGRATION WITH WORK PACKAGE.....	7
2.2	Mobile application for Biometrics card.....	8
2.2.1	DESCRIPTION.....	8
2.2.2	INTEGRATION WITH WORK PACKAGE.....	8
2.3	Hardware Security Modules	9
2.3.1	DESCRIPTION.....	9
2.3.2	INTEGRATION WITH WORK PACKAGE.....	10
2.4	ADAPT system	11
2.4.1	DESCRIPTION.....	11
2.4.2	INTEGRATION WITH WORK PACKAGE.....	11
2.5	Complete Wearable	12
2.5.1	DESCRIPTION.....	12
2.5.2	INTEGRATION WITH WORK PACKAGE.....	13
2.6	Sensors used in the Wearable.....	14
2.6.1	DESCRIPTION.....	14
2.6.2	INTEGRATION WITH WORK PACKAGE.....	15
2.7	Xsens Motion Tracking Sensor	16
2.7.1	DESCRIPTION.....	16
2.7.2	INTEGRATION WITH WORK PACKAGE.....	16
5	CONCLUSIONS	17

Objective of WP2

- To fully integrate the project's core software infrastructure to specific hardware components for added security, capabilities and functionalities.
- To promote system general adaptability to various consumer wearables, commercial terminals, medical equipment interfaces.

1 Introduction

This document defines the list of physical wearables, sensors and devices compatible with the software system to enable secure user identification.

Such devices can be (for example):

- compact cards
- mobile devices (including types and/or models)
- real-time data gathering and monitoring with onboard processing (tested, functional and evaluated).

1.1 Expected results

- Secure cryptographic key management through Hardware Security Modules (HSM).
- Implementation of commercial wearables for secure and privacy-preserving collaborative data gathering with medical center software.
- Development of seamless integration with computer-assisted surgery navigation system (ADAPT) and other medical devices for improved feedback control.
- Physical device embodiment of digital identity for authentication and authorization purposes.

2 List of physical wearables, sensors and devices compatible with the software system to enable secure user identification

2.1 Biometrics Smart Card

2.1.1 Description

- Multi-Pass is an authenticator with on-board biometric that allows support for multiple use-cases in a single credit card form factor.
- It's an interoperable way of accessing any digital or physical environment in a passwordless authentication.
 - Leverages NFC and biometrics.
 - Offline biometric storage.
 - MFA by default.
- The most secure way to identify yourself.
 - Card cannot be broken into (if tried, the data will be destroyed).
 - Card cannot be used by anyone else except for the individual.
 - If someone steals/takes-away their card, they will not have access to their account due to biometrics integrated.
 - Identity recovery is possible if card is lost (Multi-Pass SaaS).



- Simple enrolment process: Using the provided sleeve, press on the biometric sensor 5 times.
- Easy usage: Put finger on the fingerprint sensor and tap the card on the terminal, phone, or NFC reader.

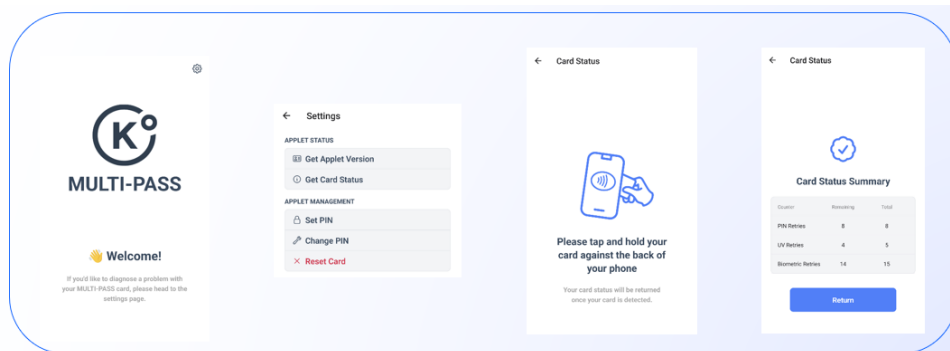
2.1.2 Integration with Work Package

- The biometrics card can be used to identify the patient when using a medical device.
- The card can also be used to ensure trust by making sure the access to medical data can only be done by authorized personal.
- The card can also be used to sign patient consent for medical documents.

2.2 Mobile application for Biometrics card

2.2.1 Description

- Mobile application is used to support the biometrics card for the following use cases:
 - Verify card status for security.
 - Set PIN: used to set the initial card fallback PIN.
 - Change PIN: used to change card PIN.
 - Reset card: used to remove all credentials and card PIN.
 - Future:
 - Update the software on the biometrics card.
 - Use the mobile app as an NFC reader.
- Currently, the app is available on the App Store (Apple phones) and Play Store (Android phones)



2.2.2 Integration with Work Package

- Using the mobile app with the biometric card will enable the user to self-manage the card for updates card reset, and troubleshooting.
- In addition, with the ability to use the mobile device as an NFC reader, this will greatly reduce the dependency on external NFC readers during user authentication.

2.3 Hardware Security Modules

2.3.1 Description

- In order to protect consent provided by patient during clinical trials, Kelvin Zero will provide system cryptographic key management capabilities.
- The following Hardware Security Modules were used to store and manage cryptographic keys:
 - Thales Luna Network HSM 7



Feature	Details
OS Support	<ul style="list-style-type: none"> • Windows, Linux, Solaris, AIX • Virtual: VMware, Hyper-V, Xen, KVM
Cryptography	<ul style="list-style-type: none"> • Full Suite B support • Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES) with named, user-defined and Brainpool curves, KCDSA, and more • Symmetric: AES, AES-GCM, DES, Triple DES, ARIA, SEED, RC2, RC4, RC5, CAST, and more • Hash/Message Digest/HMAC: SHA-1, SHA-2, SM3, and more • Key Derivation: SP800-108 Counter Mode • Key Wrapping: SP800-38F • Random Number Generation: designed to comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A compliant CTR-DRBG
Cryptographic APIs	<ul style="list-style-type: none"> • PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL • REST API for Administration
Reliability	<ul style="list-style-type: none"> • Dual hot-swap power supplies • Field-serviceable components • Mean Time Between Failure (MTBF) 171,308 hrs
Certifications	<ul style="list-style-type: none"> • FIPS 140-2 Level 3 –passwordand multi-factor (PED)Certificate #3205 • QSCD for eIDAS compliance • Common Criteria Certification (PP 419 221-5)
Compliance	<ul style="list-style-type: none"> • UL, CSA, CE • FCC, CE, VCCI, C-TICK, KC Mark • RoHS2, WEEE • TAA

2.3.2 Integration with Work Package

- MHICC (Montreal Health Innovations Coordinating Center) currently has a process for collecting “Informed consent” during clinical trials. To ensure the information collected is safely stored, we developed a solution (SoLID) to digitally sign those consent and leverage HSMS (Hardware Security Modules) to generate and store cryptographic keys.

2.4 ADAPT system

2.4.1 Description

- Made up from:
 - ADAPT tablet usable in the OR
 - associated ADAPT software
 - 3D-printed reference bodies
- Usage requires a C-arm connected to the tablet to generate fluoroscopic intra-op images.
- Serves as a base to be extended, providing intra-op fluoroscopy-based navigation for exact screw placement in fractures.
- As an extension of this system, it will be investigated whether intraoperatively fracture fragments can be reconstructed in 3D with simple fluoroscopy images by using AI to perform a better repositioning of the fracture by matching its shape, rotation and length with the healthy limb.
- Possible output: x-rays and patient-specific measurements regarding the fracture (bone length and rotation angle before and after the fracture repositioning).

2.4.2 Integration with Work Package

- Corresponding task: Sensors & wearables (WP2 T1)
- Serves as a sensor which is integrated in the smart fracture care patient pathway to improve patient healing.

2.5 Complete Wearable

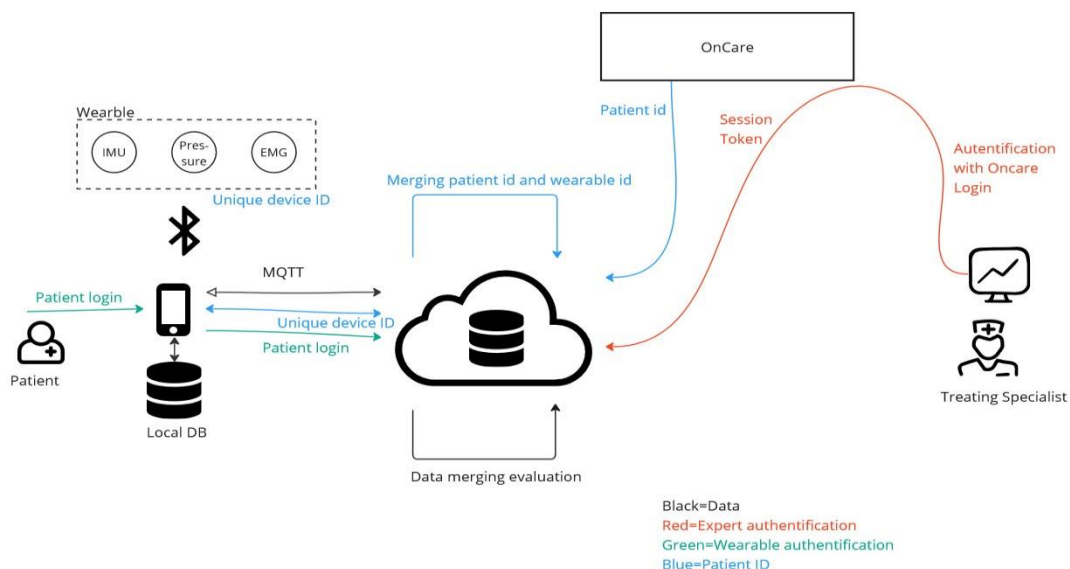
2.5.1 Description

A major problem in follow-up is inadequate information density. Which would be necessary to achieve an optimal outcome. We have developed a concept to digitize rehabilitation and increase the density of information. In the following figure, a part of this concept is shown.

On the one hand, the wearable is visible that monitors the patient and is managed by the device Api, generating additional Information about recovery. On the other hand, the OnCare system is visible, which enables digitalization of rehabilitation.

There are two places where patients or experts have to authenticate.

- 1) The specialist must log on to the system in order to virtually assign the wearable to the patient. This access is solved via the patient management system Oncare. A specialist logs into the Oncare platform via 2-factor authentication and is thus enabled to control the wearable. For this purpose, a session token will be exchanged between the two systems (Device API and OnCare).
- 2) A system for the patient authentication is necessary in order to interact with the wearable. So far, the wearable is supposed to communicate via Bluetooth with the mobile device of the patient, therefore this way is secured via the general cell phone lock.



2.5.2 Integration with Work Package

A device that requires developed solution of identification and authentication is presented. First suitable solutions are presented in addition, but improvements can be integrated.

2.6 Sensors used in the Wearable

2.6.1 Description

The wearable consists of different sensors. The final structure is not yet fixed. So far, an electromyography study has been conducted with a Delsys system. Other sensors that are already available are pressure sensors built into a sole and IMUS on an Arduino.

EMG:

- Here, a product approved as a medical device is currently being used to test how EMG sensors can be used for monitoring rehabilitation



- This system is great for first tries but not usable for everyday use, so will be replaced in the following

Pressure sensors:

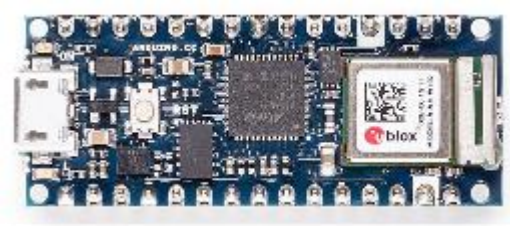
- The pressure sole is a sensor that changes its internal conduction characteristics when pressure is applied from the outside



- These sensors are read out by the Arduino

IMU:

- The IMUs are mounted on the Arduino and can be read out directly



All in all, the various sensors are to be connected to an Arduino, which then connects via Bluetooth to a mobile device running an instance of the device api. The communication is secured via a unique ID.

2.6.2 Integration with Work Package

The different sensors that are combined in the wearable are secured via the concept presented in 2.5 with regard to user identification.

2.7 Xsens Motion Tracking Sensor

2.7.1 Description

Xsens system (Xsens, Enschede, Netherlands) is a system for the measuring and recording peoples' movements in real time, based on the technology of inertial sensor technology. Inertial sensors consist of a position sensor, which is aligned with the earth's magnetic field, and three acceleration and rotation rate sensors. The acceleration sensors record the translational movement, while rotation rate sensors are used for recording the rotatory rotation components. With this, a reliable and non-invasive method for motion analysis has been developed with the advantages of flexible test environment and not influence by the light sources.

MVN Awinda Intermediate performance



Range	~50m
Update rate	60hz
Battery life	6h
Comms	Radio protocol (Awinda)
Receiver	Awinda station
Hardware	17(+1) wireless sensors T-shirt + straps
Charging	Charging station

2.7.2 Integration with Work Package

The XSens system will be used for validation of the wearable which will be developed by OFFIS.

5 Conclusions

As detailed out above, the team is advancing greatly towards the expected results of this work package.

- HSM are being used to secure cryptographic keys for the use case of “Siteless clinical trials”.
- Commercial wearables are progressively being developed and continuously improved for the use case of “Wearables for rehab”.
- Integration with ADAPT is evolving meticulously to support the use case of “Computer assisted surgery”.
- Biometric cards are being used to securely identify and authenticate users.

In addition, we are collaborating to see how our respective devices can benefit from each other’s technologies and expertise in the domain.