SUNRISE

Strategies and Technologies for **Un**ited and **R**esilient Critical **I**nfrastructures and Vital **S**ervices in Pandemic-Stricken **E**urope

D4.2 Access control tool and training guide V1

Document Identification			
Status	Final	**Due Date**	30/09/2023
Version	1.0	**Submission Date**	29/09/2023

Related WP	WP4	**Document Reference**	D4.2
Related Deliverable(s)	D4.1, D3.1, D3.2	**Dissemination Level (*)**	PU
Lead Participant	AIT	**Lead Author**	Daniel Slamanig
Contributors	IMA, UKC, INS, UoW, SZ, CAF, TS	**Reviewers**	Rodrigo Diaz, Antonio Alvarez (ATS)
			Nikolay Zherdev (LSE)

Keywords:
Physical Access Control, GDPR, Critical Infrastructures, Pandemic, Privacy protection

Document Information

List of Contributors	
Name	Partner
Name Surname	Beneficiary short name
Daniel Slamanig, Stephan Krenn, Julia Mader	AIT
Jan Orlicky, Tomas Trpisovsky, Karel Neuwirt, Jiri Ochozka, Vlastimil Benes	IMA
Matjaž Tavčar	UKC
Gilda de Marco	INS
Tom Sorell	UoW
Tomaž Ramšak	SZ
Daniele Fabro	CAF
Andreja Markun	TS

Document History			
Version	Date	Change editors	Changes
0.1	25/06/2023	IMA	ToC drafted
0.2	26/07/2023	IMA	ToC finalized, D4.2 skeleton drafted
0.3	03/08/2023	IMA	Chapter 2 included
0.4	04/08/2023	IMA	Chapter 2 reviewed
0.5	26/08/2023	IMA	Chapter 3 content added
0.6	14/09/2023	AIT	Chapter 1 content added, document reviewed
0.7	14/09/2023	IMA	Pilot contributions and CI user guide reviewed
0.8	22/09/2023	IMA	Review comments addressed
1.0	27/09/2023	IMA	Final version after 2nd round review

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Daniel Slamanig (AIT)	27/09/2023
Quality manager	Juan Andrés Alonso (ATS)	29/09/2023
Project Coordinator	Antonio Álvarez (ATS)	29/09/2023

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
ABC	Attribute-based Credential
ACS	Access Control System
ADC	Analog to Digital Converter
AI	Artificial Intelligence
BLE	Bluetooth Low Energy
CI	Critical Infrastructure
D4.2	Deliverable number 2 belonging to WP 4
DHC	Digital Health Certificate
EC	European Commission
EUDCC	European Digital Covid Certificate
GDPR	General Data Protection Regulation
HW	Hardware
IDM	Identity Management
IAM	Identity and Access Management
IPS LCD	In-plane Switching Liquid Crystal Display
ML	Machine Learning
NFC	Near Field Communication
NN	Neural Network
PMOS	P-type Metal-Oxide Semiconductor
PPE	Personal Protective Equipment
RC circuit	Resistor-capacitor Circuit
RiBAC	Risk-Based Access Control
SW	Software
TRL 5, TRL 6	Technology Readiness Level 5 resp. 6
WP	Work Package

Executive Summary

The Risk-based Access Control (RiBAC) tool is one of the tools of the SUNRISE project. It aims to provide so-called RiBAC components that can be used to augment access control system for critical infrastructure sites with access control decisions based on pandemic-specific factors (e.g., the presence of protective gear such as masks, body temperature or vaccination status). The RiBAC tool pays special attention to privacy protection, security, and compatibility with GDPR and meets specific requirements for both scalability of physical access control and economic efficiency.

The concept of RiBAC – as a new tool for increasing the security of critical infrastructures – was presented in private deliverable D4.1. The following document describes the implementation of the RiBAC tool at a modular level (the components of the RiBAC tool) as well as information about the pilot trial execution. Further future progress will be presented in subsequent iterations (D4.3-D4.6). The results of the first validation of the RiBAC tool in laboratory conditions are also described.

The development status of the software/hardware solutions of the RiBAC modules aligns with the expectations and achieves a TRL of 5 or higher. Furthermore, a first laboratory integration of the RiBAC modules has been conducted. The outcomes from these lab tests indicate that the tool can address the challenges that appear in real-world settings. Furthermore, the document includes a first user guide for CIs on how to operate RiBAC components.

With all the content provided, D4.2 establishes a solid foundation upon the RiBAC components that can be further improved and developed and an integrated version can be demonstrated in the real-world environment of CI operators.

1 Introduction

1.1 Purpose of the document

The SUNRISE project is designed to bolster the resilience of essential services within Europe's Critical Infrastructure (CI) by equipping CI operators and authorities with the necessary tools to handle situations similar to those encountered during the recent COVID-19 pandemic. The main aims are *"to ensure greater availability, reliability, and continuity of critical infrastructures in Europe including transport, energy, water, and healthcare"*.[1] To achieve this, the project proposes the development of a strategy and a set of tools. Included in this set of tools is the risk-based access control (RiBAC) tool developed within WP4. This tool primarily focuses on ensuring a reduced risk for access to critical infrastructure in a scalable and privacy-preserving way.

In this context, the main goal of D4.2, "Access control tool and training guide V1", is to outline the approach and the initial steps taken during the development of the tool and corresponding modules designed to equip (existing) access control systems with the capability to integrate additional factors into the access control decision. Additional pandemic-specific factors are for instance whether an individual subject to access control wears protective measures (e.g., a face mask) or health parameters of the individual (e.g., body temperatures as well as the status from a digital health credential).

This document provides a description of the first phase of the implementation of the RiBAC tool at the level of individual functional modules (mask detection, temperature measurement and digital health credential check) on the TRL5 level. It also describes the results of RiBAC validation in a laboratory setting. In addition, the principles of using RiBAC by individual CI operators are described. It also provides an overview of CI sites with proposed piloting schedules. Finally, it presents a user manual and training guide for CI operators on how to use the RiBAC tool.

1.2 Relation to other project work

This deliverable D4.2 "Access control tool and training guide V1", represents the second output from WP4 and includes work related to the tasks: T4.1 Privacy aspects in access control techniques; T4.2 Architecture for privacy-friendly risk-based access control; T4.3 UI (user interface) for privacy-friendly risk-based access control to critical facilities; T4.4 Continuous integration and testing; and T4.5 Demonstration, training, evaluation, and validation. Like all other tool WPs (WP4-WP7), WP4 is interconnected with collaboration (WP1), strategy (WP2), and design (WP3), as well as management (WP9), dissemination and exploitation (WP8), ethical requirements (WP10). From a technical perspective, the primary connection is with WP3, which gathers requirements and serves as a hub for the development of all the tools in the respective work packages.

When it comes to concrete documents that have either been already submitted or are currently written, D4.2 has a strong relationship with D4.1 as well as D3.1 and D3.2. More precisely, D4.1 " Access control conceptualization" covers the (conceptual) foundations for the RiBAC tool, its architecture, and the developments of the RiBAC modules. It provides an extensive discussion of potential RiBAC architectures that – depending on the prerequisites – can be considered, its requirements as well as security and privacy guarantees along with a first introduction to the pilots. Moreover, the deliverables D3.1 and D3.2 represent (an iteration of) the requirements that are coming from CI stakeholders and a technical overview of the approach towards the RiBAC tool.

[1] https://sunrise-europe.eu/

1.3 Structure of the document

This document is structured in 5 major chapters and annexes.

Chapter 1 presents the purpose of this deliverable (D4.2), its relation to other project work, and its structure.

Chapter 2 presents the overview of the RiBAC Tool. The focus is on the architecture and deployment of the four modules.

Chapter 3 presents the evaluation results of lab experiments of individual modules and especially in an environment whose parameters can be changed.

Chapter 4 presents the CI pilot trials within the Italian and Slovenian clusters as well as the Czech pilots.

Chapter 5 provides a summary of the main findings of this deliverable and presents conclusions.

Annex I shows a template of informed consent intended for the pilot participants.

Annex II provides an overview of privacy measures adopted within the pilot testing phase of the RiBAC tool and offers a user manual for the terminal integrating the modules presented in previous chapters.

1.4 Glossary adopted in this document

EUDCC

To facilitate safe free movement during the COVID-19 pandemic, the European Union established the EU Digital COVID Certificate (also known as the COVID Pass, Digital Green Certificate, Digital COVID Certificate, or also the Certificate).
On 1 July 2023, the World Health Organization (WHO) took up the *"EU system of digital COVID-19 certification to establish a global system that will help protect citizens across the world from on-going and future health threats, including pandemics"*.[2]

EUDCC in the Czech Republic

This certificate has been issued since July 1 2021 and is in addition used as proof of having undergone a test/vaccination or survived a COVID-19 infection within a EU member state. As for other countries than the EU member states, the conditions set by the respective country (page in Czech only) apply.

There are two applications constituting the safe and sound proving principle - one containing a QR code (from the certificate) and the other that reads the code and shows whether the vaccination or COVID-19 test is performed at the required interval - either according to the rules of cross-border movement or within the entrance to stores, establishments, for cultural or sports events, etc. The same applies for having survived a COVID-19 infection as well.[3]

[2] Source: https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

[3] Source: https://covid.gov.cz/en/situations/vaccination/validation-applications-ctecka-and-tecka

2 Risk-Based Access Control Tool

As the follow up of the RiBAC concept presented in the D4.1 document the functional implementation on TRL5 level has been accomplished. IMA was responsible for the implementation of this phase. The phase included the development of the basic HW and SW parts of RIBAC and the preparation of the RIBAC base version on TRL5.

The result is a graphical touch-screen terminal equipped with an RFID card reader for interaction with supervised persons. The terminal is also equipped with a number of data interfaces for connecting the peripherals needed to perform the physical access control. These peripherals include e.g., an infrared camera, an optical camera, a QR code scanner and a graphic accelerator. Furthermore, the terminal contains interfaces for controlling entrance doors or turnstiles. The terminal is equipped with an Ethernet interface or a WiFi module for communication with a higher-level system.

RiBAC upgrade to TRL6 level, integration with other components of the access system used by the CI operator and validation at pilot sites will be continuously ensured during the next stages of SUNRISE.

The RiBAC terminal was implemented with partial use of the results of the previous national project: Automated detection of protective equipment and status indicating disease (ADOPSIO[4]) with identification code VI04000069 co-financed with the contribution of the Ministry of the Interior of the Czech Republic. Specifically, during the first year of the SUNRISE solution, we established an ADOPSIO terminal designed for the Czech national environment. It was modified in terms of replacing obsolete HW components and related SW equipment. The RiBAC terminal also has a modified mechanical design. Furthermore, the AIT partner is preparing a completely new EUDCC module in accordance with the European standard.

2.1 General Architecture

The RiBAC terminal consists of IMA's proprietary HW/SW solution housed in a unique plastic box. This enables simple, scalable integration with legacy access control systems already in use by CI operators.

A simplified description of the device follows.

[4] https://starfos.tacr.cz/en/projekty/VI04000069

2.1.1 Terminal hardware solution

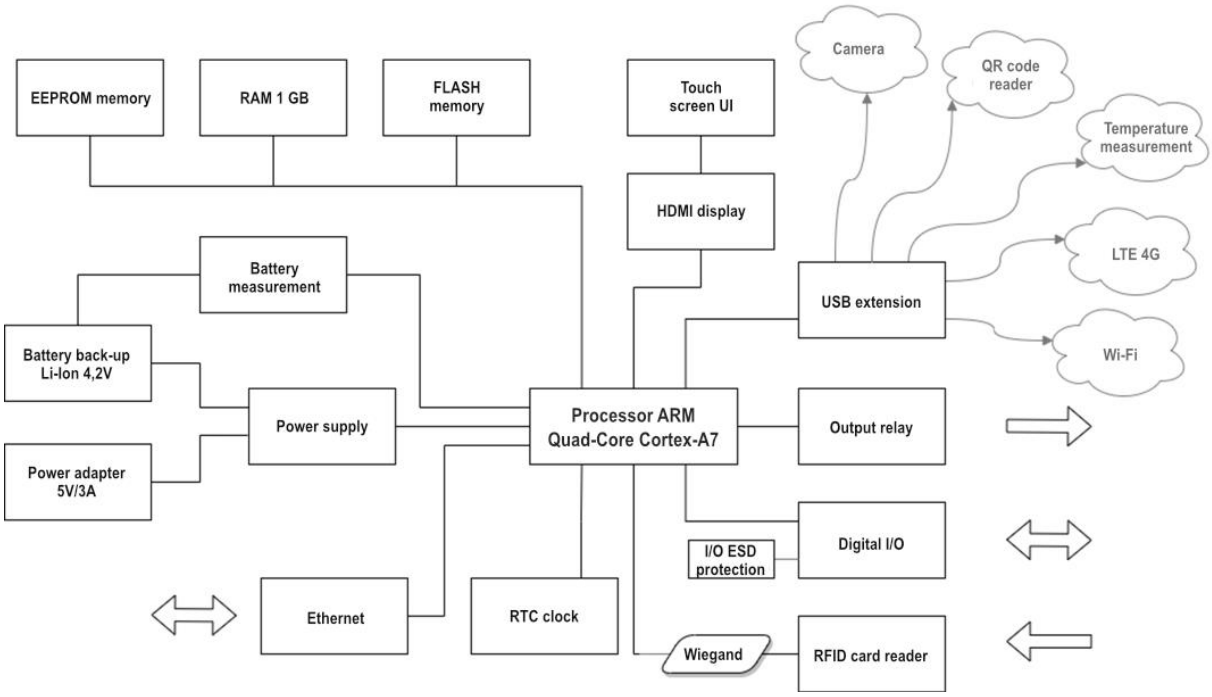


Figure 1: X block diagram of the terminal

The terminal serves as an end device for access control, data collection and communication with the user. It is equipped with a capacitive LCD touch screen (7 inches). The design of the displayed messages can be programmed according to the operator's needs. The terminal contains a powerful Quad-Core Cortex-A7 ARM CPU with 1GB RAM and expandable FLASH memory up to 128GB. This allows an extensive database of the list of enabled cards and the number of recorded events to be stored offline. The terminal is equipped with a universal RFID card reader. Supported card standards are Mifare, Desfire, LEGIC and HID.[56]

[5] Mifare and Mifare DESFire: https://www.nxp.com/products/rfid-nfc/mifare-hf:MC_53422

[6] LEGIC: https://www.legic.com/products/smartcards/legic-smartcard-ics

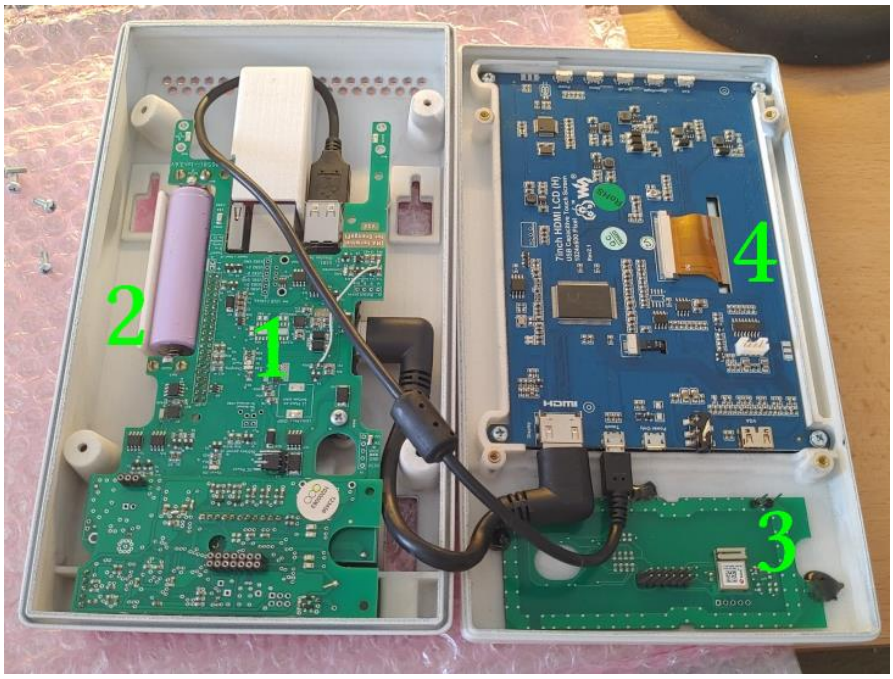


Figure 2: Internal layout of terminal hardware components

The terminal contains four In/Out pins and one output relay, allowing the connection of many input and output devices (door locks and contacts, control buttons, turnstiles, etc.). Connection to security and anti-fire systems is also available.

The terminal is equipped with an integrated Ethernet communication interface. The communication interface can be extended by external USB converters, providing alternative communication with the parent system such as LTE or Wi-Fi modules.

2.1.2 Computing module

The module with the main Quad-Core Cortex-A7 ARM CPU also contains the basic computer peripherals. The module directly contains a USB controller, Ethernet, GPIO, HDMI, memory card reader and other peripherals not used in the terminal. The CPU itself runs at 1.6GHz, has 4 cores and uses 1GB of DDR3 RAM. The processor has a passive heatsink on it and there are ventilation holes in the terminal cover for heat dissipation. In Figure 2, the computing module is hidden under the motherboard at the location labeled "1".

2.1.3 Motherboard

The heart of the motherboard is the computing module described above. There is also a power supply block on the board, including the battery charging circuit. The battery itself is then also stored directly on the terminal's motherboard. The board is further extended with a universal RFID card reader, an output relay and a terminal block for connecting the terminal.

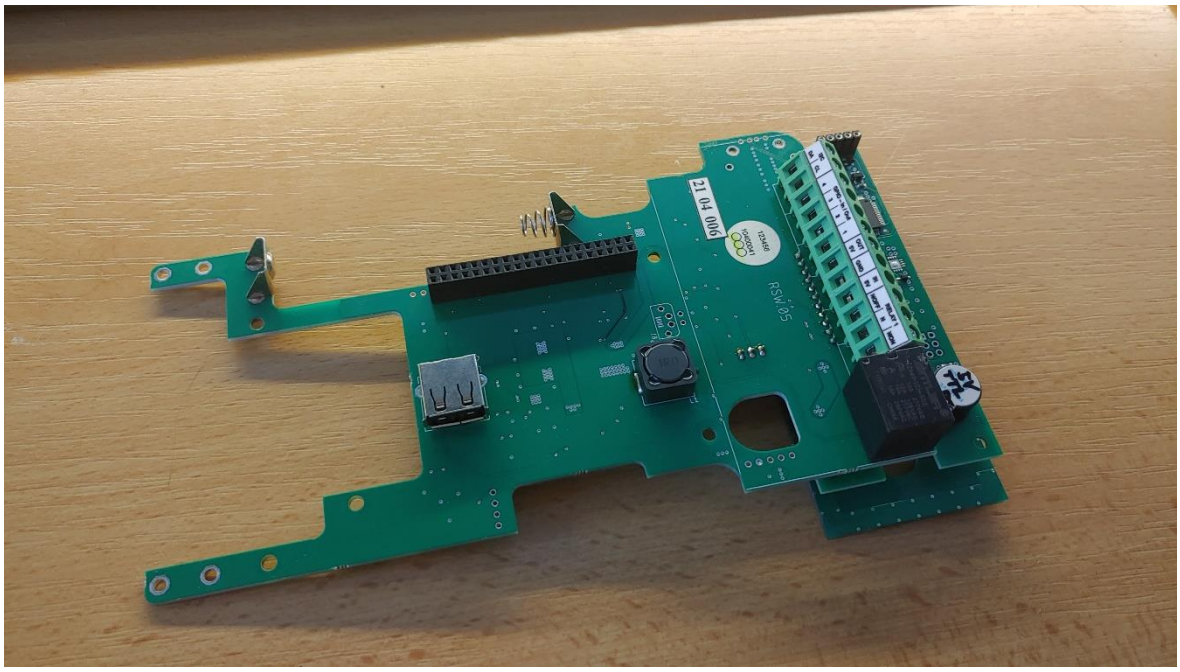


Figure 3: Internal layout of terminal hardware components

2.1.4 Power supply block

The power supply is provided by an external 5V/3A DC adapter. The consumption of the whole terminal during normal operation is 5 to 10W. The adapter is connected to the terminal block at the back of the terminal. The power supply is backed up by a battery due to the risk of damaging the SD card in the event of a power failure. In the event of a failure, the RC circuit starts to discharge and the comparator then disconnects the PMOS transistor through which the battery is connected to the circuit. To protect the battery itself, an additional comparator is used to disconnect the battery should its voltage drop below 3V.

In order to power the entire device from a Li-Ion battery that has a voltage between 3.3 and 4.2V, a boost converter is required. The voltage from both the adapter and the battery is fed into the inverter via diodes so that they do not affect each other and so that the battery remains disconnected when the external adapter is connected (the voltage from the battery will always be lower than that from the adapter). The voltage converter is capable of maintaining a 5V/2.8A output as long as there is at least 2.5V at the input, which even a nearly discharged battery reduced by the 0.7V drop across the diode will provide.

An integrated circuit is used to charge the battery, which is capable of delivering up to 2A current to the battery. To check the battery status, an analogue ADC is fitted, which can measure the state of charge of the battery. If everything is working properly, there will still be approximately 4.2V on the battery thanks to the charging circuitry that maintains this value. The battery itself is an 18650 size and is labeled "2" in Figure 2.

2.1.5 Real Time Circuit

If the terminal is not connected to the Internet, it should not have the current time after reboot. This is a very unlikely situation, but if this happens, the terminal will keep the current time. The terminal's functionality will not be impaired. The RTC circuit is powered directly from the battery, so a failure of

the primary power supply will not stop the clock. After a reboot, the computing module downloads the current time and continues to run as standard inside the Linux operating system.

2.1.6 EEProm memory

The EEProm memory is connected to the terminal via the I2C bus to store basic information about the motherboard. This is the type of board and the MAC address of the specific piece. This will later differentiate between the pieces and ensure that no two identical terminals are in operation.

2.1.7 USB port control

The motherboard allows to switch on and off 2 USB ports via power PMOS transistors. This feature is useful when the primary power supply goes down, so that the display or other peripherals can be switched off immediately, thus placing less demand on the battery capacity.

2.1.8 RFID card reader

The terminal has an integrated RFID card reader produced by IMA. It is marked "3" in Figure 2. It is a universal reading device that, thanks to the support of NFC and Bluetooth technologies, allows identification by a wide range of media. It is based on RFID technology support at 13.56MHz or 125kHz. Support for Bluetooth or NFC communication with mobile phones is added.

Supports cards and cryptographic keys:

- LEGIC PRIME, ADVANT (standard 14443, 15693),
- Mifare and Desfire cards,
- HID cards (15693 standard),
- Legic Connect virtual keys,
- Virtual keys BLE + NFC platform Openmobile,
- Variant for 125kHz cards (e.g. EM-MARINE).

2.1.9 Touch screen display

The display is connected to the system via HDMI and USB. The display is powered via USB and the data from the touch layer is transmitted at the same time. The display is capacitive and multi-touch. The display dominates the front of the terminal, where it takes up most of the surface. The display is covered by a thin, transparent, plastic film with black borders. In Figure 2Figure 2, the display can be seen from the inside of the terminal labelled "4".

Basic display parameters:

- Size: 7 inches diagonal.
- Resolution: 1024x600 pixels.
- Technology: IPS LCD.
- Touch layer: Capacitive multi-touch, up to 5 points simultaneously.

2.1.10 Inputs, outputs and peripherals

2.1.10.1 I/O terminals

The terminal is designed for permanent installation on the wall; therefore, the connection of peripherals is solved via the terminal block. This connection is reliable and saves space in the terminal. In the base, only a DC 5V/3A voltage source will be connected to the terminal block.

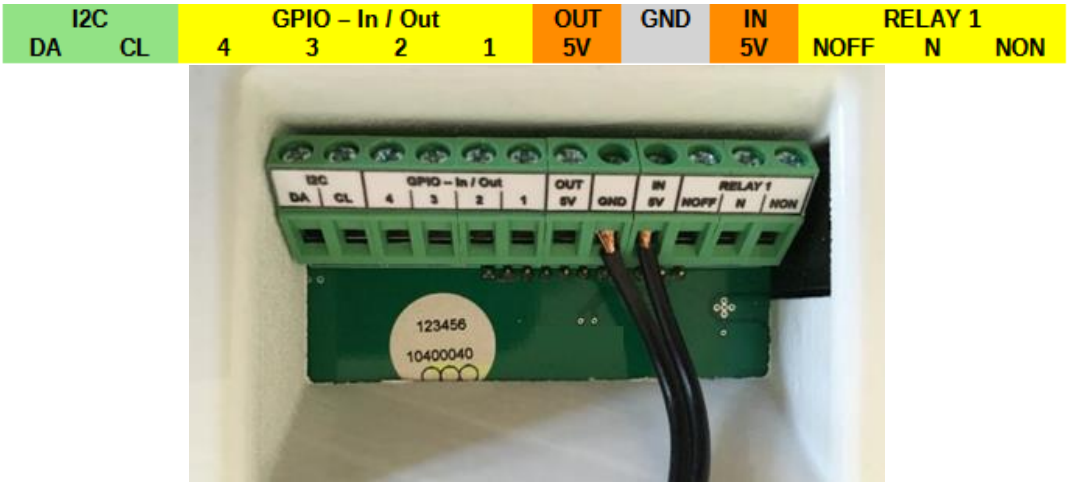


Figure 4: Wiring the terminal block on the back of the terminal

2.1.10.2 Galvanically isolated switch

The terminal can control, for example, a door lock or a turnstile. It is a device with a high current consumption, often inductive in nature, powered by different voltages. A galvanically isolated relay is used in the terminal for this purpose. The maximum current and voltage values at the relay terminals are: 10A at 250VAC.

2.1.10.3 Wiegand interface

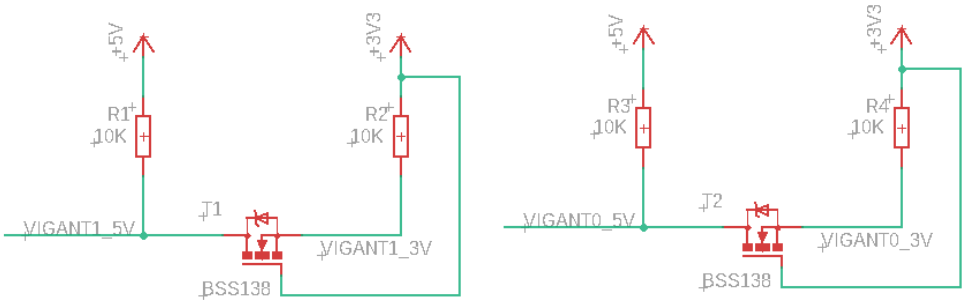


Figure 5: Wiring diagram of the level converter from 5V Wiegand to 3.3V for the calculation module

The Wiegand interface is a de facto wiring standard. It is commonly used to connect a card swipe mechanism to the rest of an access control system.

2.2 Tool Modules Description

2.2.1 Main loop

Within the stage, modules for facial temperature detection, face mask detection, protective equipment detection, RFID card reading, QR code reading of the Tečka application (CZ official info on personal vaccination) and anonymous COVID PASS reading were integrated into the main loop of the program.

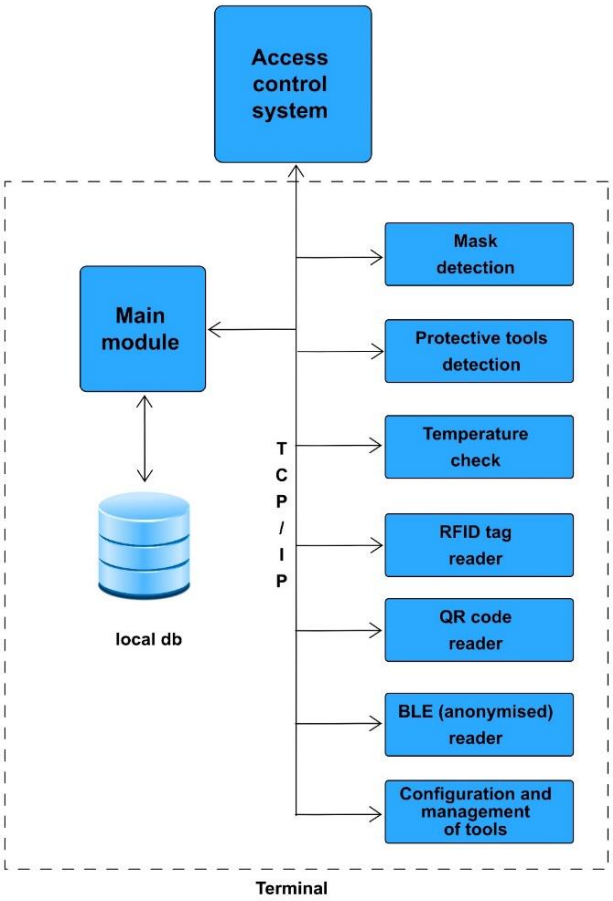


Figure 6: RiBAC tool modules

2.2.1.1 Program initialization

Before the GUI starts, a configuration file is loaded that is created through the web interface. This specifies which interfaces are connected to the terminal. After the file is loaded, the TCP servers for each service are started. If an RFID card reader is present, processing is also started for this interface, which is connected directly via the Wiegand interface (see Figure 5).

2.2.1.2 Communication between services

All services communicate with each other in JSON format, where each message is preceded by 2 bytes of information about the size of the received message.

2.2.2 Terminal user interface

The terminal user interface consists of several parts. The major part is the display with a capacity touch panel. Next are visual and infrared cameras. Then RFID reader is used for reading the user identifiers.

The display shows the actual status of the terminal, the protective tools verification status and the final result as access granted or rejected. Optionally the instructions for better protective tools recognition in the form of instructions for a person can be displayed. The display is also able to optionally show a camera image of the user's face for better positioning during verification.

2.2.3 Communication Interface - API

Communication Interface -API is a REST interface for operating access terminals. The interface provides the following services:

- getting a version of the service,
- obtaining the current configuration sequence number and blocked cards,
- obtaining simplified access rights to foreign sensors,
- obtain incremental changes to access rights,
- obtain incremental changes to blocked cards,
- get details for the specified card number,
- obtaining a photo of the person for the card number entered,
- entering passes on foreign sensors into the legacy system.

For deployment, it is assumed that individual functions are called sequentially. The terminal can call the version at any time to verify the basic connection to the service.

If any internal error occurs that prevents the function from executing, the http code 500 (internal server error) is returned. Furthermore, unless otherwise specified, http code 200 (OK) is returned on success.

2.2.4 Access Control Module

The Access control module is dedicated to the reading of staff badges for access rights evaluation. Nowadays the mostly used badges are RFID tokens and mobile phones equipped with Bluetooth interface. The terminal is equipped with the reader, which enables communication with standard RFID tokens and mobile phones via Bluetooth. The reader communicates with the terminal processor unit via Wiegand interface.

The reader is equipped with 16 - bit processor MICROCHIP 24FJ256 with 256 kbit memory[7]. The RF interface is made by LEGIC chip SM6300[8]. This configuration can operate with cards according to standards ISO 14443 and ISO 15693. And mobile phones with Bluetooth 4.0 and above.

The reader is powered up by 5V. The consumption is about 200 mA. Figure 7 shows the RFID reader main board.

[7] https://www.microchip.com/en-us/product/pic24fj256da106

[8] https://www.legic.com/fileadmin/user_upload/Flyer_Broschueren/SM-6300_flyer_en.pdf

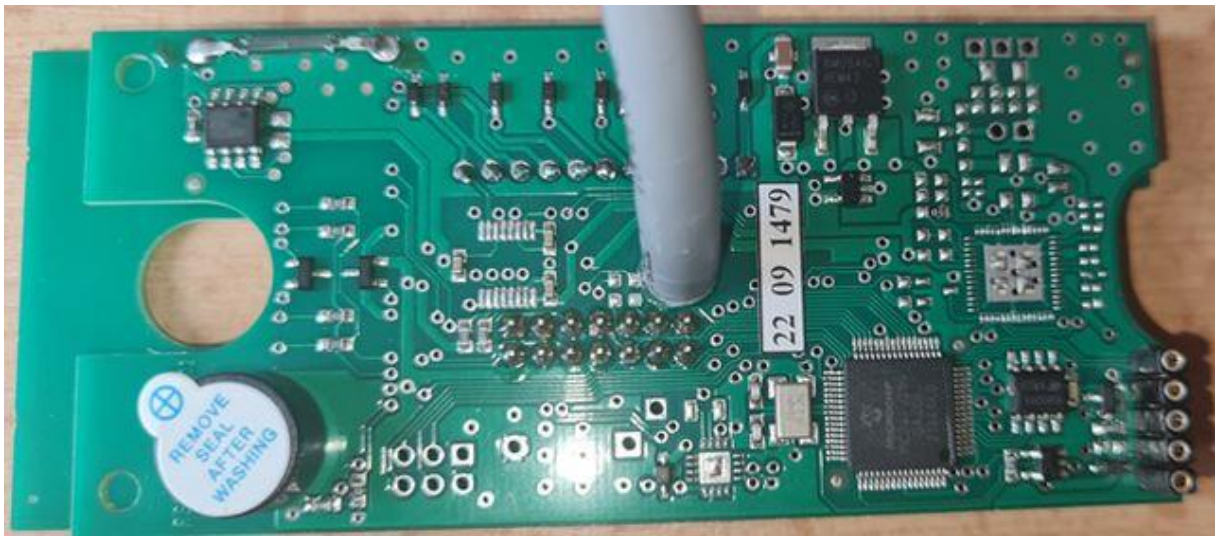


Figure 7: RFID reader main board

To achieve the best communication performance (distance) the reader is equipped with a separate antenna board. There are antenna wires, RF circuit SM6300 and indication LEDs, typically red and green. The antenna board is shown in Figure 8.

Figure 8: Antenna board

2.2.5 Protective Tools Detection Module

The protective tools detection module consists of two parts. On one side, there is a RGB visual camera for monitoring of the place in front of the terminal, and on the other side there is a computer acceleration module for data evaluation (Neural Compute Stick 2).

The camera Arducam 2Mpx[9] is connected to the computer via USB port. It provides data transition and power supply. The camera parameters are:

- Plug & Play USB camera compatible with UVC.
- 2Mpx CMOS sensor Sony IMX291 with dynamic range 80 dB.
- Lens M12 with 100° viewing angle and IR filter.
- 30fps @ 1920x1080 video.

The viewing angle 100° enables optimum protective tools detection in 1m distance. The camera module is on the Figure 9.

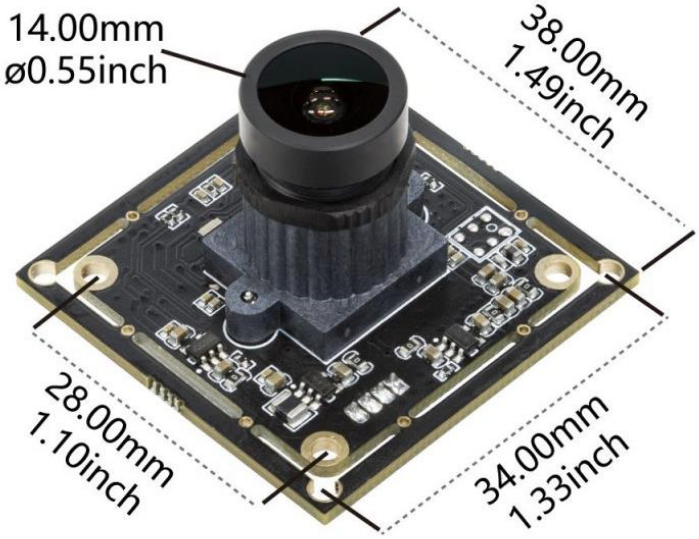


Figure 9: Camera module

The computing power of the Raspberry Pi can be considered sufficient for most of the expected operations. However, it is no longer sufficient for the proposed real-time convolutional neural network image processing. Achieving real-time performance is problematic for these algorithms even with desktop performance. Fortunately, these are operations that can be efficiently parallelized to transfer the computational load to devices with less powerful processors, but with a large number of them (typically a graphics card). In the project at hand, these calculations will not be performed on the Raspberry GPU, which is not very powerful, but on an external device that is adapted for these operations. In our case, a product from Intel was chosen, namely the NCS2 (Neural Compute Stick 2)[10] module, which can be connected directly to the Raspberry via USB. This module is based on an Intel® Movidius™ Myriad™ X VPU[11] with 16 programmable shave cores and a dedicated computational engine for hardware acceleration of neural network computations. The advantages of this module are

[9] https://www.arducam.com/product/arducam-2mp-spi-camera-b0067-arduino/

[10] https://www.intel.com/content/www/us/en/developer/articles/tool/neural-compute-stick.html

[11] https://www.intel.com/content/www/us/en/products/details/processors/movidius-vpu/movidius-myriad-x/products.html

low acquisition cost, sufficient computational power optimized for convolutional neural networks, and low-power direct USB power supply. The module is described in Figure 10.

Figure 10: Neural Compute Stick 2

NCS2 parameters:

- Processor: Intel Movidius Myriad X Vision Processing Unit (VPU).
- Power 4 TOPS (Trillion Operations Per Second).
- Connectivity USB 3.1, USB 2.0.
- Supported operating systems Raspbian, Windows 10, Ubuntu 16.04, CentOS 7.4.
- Dimensions Width 72.5 mm, depth 27 mm, height 14 mm.
- Consumption 1 to 2 W.

2.2.6 Temperature Detection Module

During 2023, two samples of the body temperature measurement module were constructed: one for easy experimentation during development and the other whose design was already suitable for practical field deployment. The mechanical design of the development sample is clearly visible in Figure 11.

In both samples, the RGB camera is a Leopard Imaging LI-OV5640-USB-AF[12], the IR camera is a Seek Thermal S304SP[13], and the TEC controller is an Analog Devices LTC1923[14] (kit DC491A).

The temperature reference target is again placed above the IR camera on an aluminium angle, which is firmly connected to the cabinet by an aluminium prism (55×30×20 mm). As the outer walls of the cabinet are slightly beveled, it was necessary to mill a 30 mm wide groove in the top wall for it. This makes the prism perpendicular to the front wall of the camera cabinet. Both the angle and the prism serve to dissipate heat from the Peltier cell. The angle in Figure 11 (width 30 mm, arm lengths 25 and 80 mm) has only about 1/2 the area of the angle in the development sample. The aluminium prism compensates for this, i.e. contributes to better heat dissipation to the surroundings. The target was set to a temperature of 37.3 °C, corresponding to the threshold body temperature at which a person is considered ill.

[12] https://www.leopardimaging.com/product/usb20-cameras/5m-usb-af-camera/li-ov5640-usb-af/
[13] https://www.thermal.com/mosaic-core-320x240-4mm.html
[14] https://www.analog.com/en/products/ltc1923.html

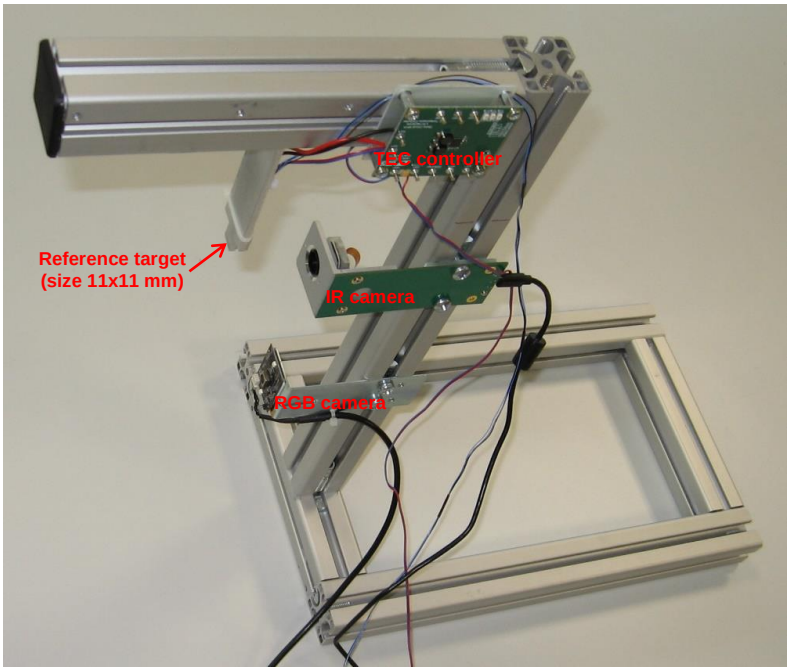


Figure 11: Development sample of the Al profile temperature measurement module

Figure 12: External view of a working sample of the temperature measurement module

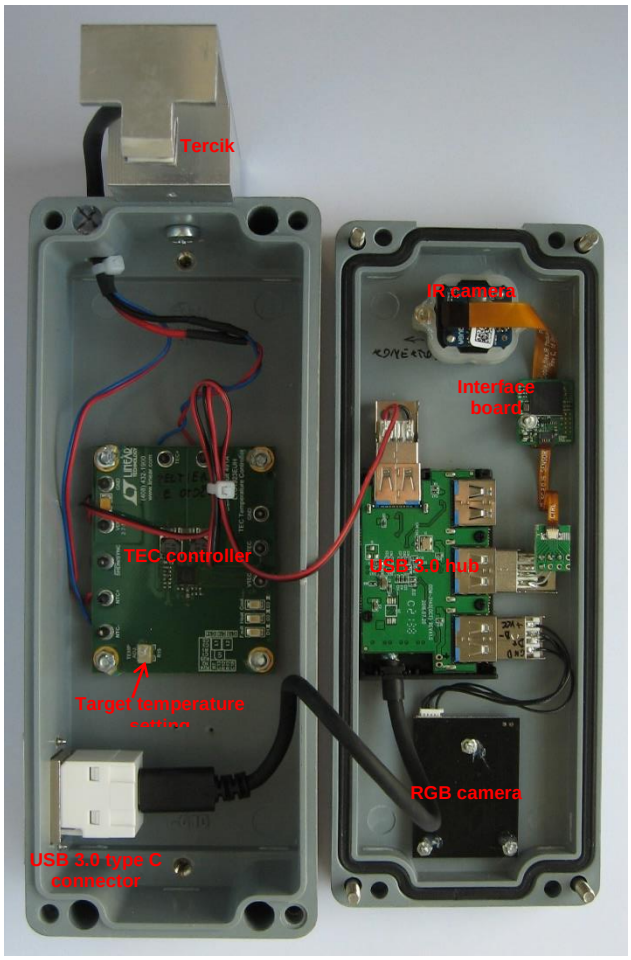


Figure 13: Internal layout of the functional sample of the temperature measurement module

The size and design of the reference target was also experimented with during the research. See Figure 14 that shows two examples of the practical implementation.

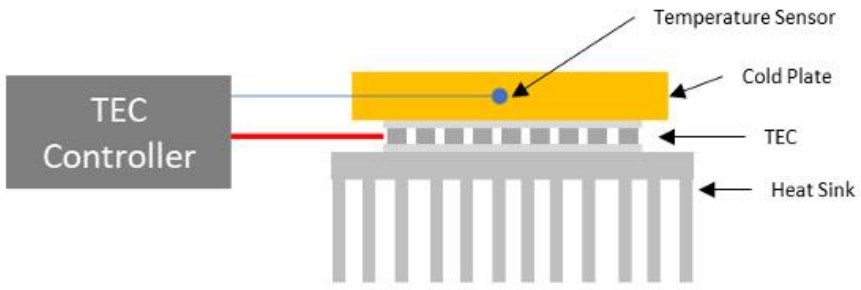


Figure 14: Block diagram of the reference target

2.2.7 Vaccine Credential Detection Module

In terms of vaccination detection, two principals were tested. The first was based on the Czech application TECKA, which allows the mobile phone owner to safely download their own sensitive

information in the form of a QR code. This code is discoverable using the official application, however sensitive information is exposed.

The second tested principle is fully compliant with GDPR and allows you to preset rules (valid for the country, website, time period) that will be evaluated and only general information about their fulfillment is generated in the form of GO/NOGO. This vaccination test is described as follows.

In the coming phase of the SUNRISE project this module is envisioned to be rebuilt or replaced by the module designed by AIT in order to fully comply with EU standards. The latter will be based on the open-source EUDCC framework[15] and will also be made available open-source.

The Vaccine Credential Detection Module is dedicated to the verification of desired administrative condition for access allowance. An example of such a system was integrated into the system. The main advantage of the solution is revealing only the minimum necessary information for access control rights evaluation. The CovidPass architecture with privacy protection is shown in Figure 15.

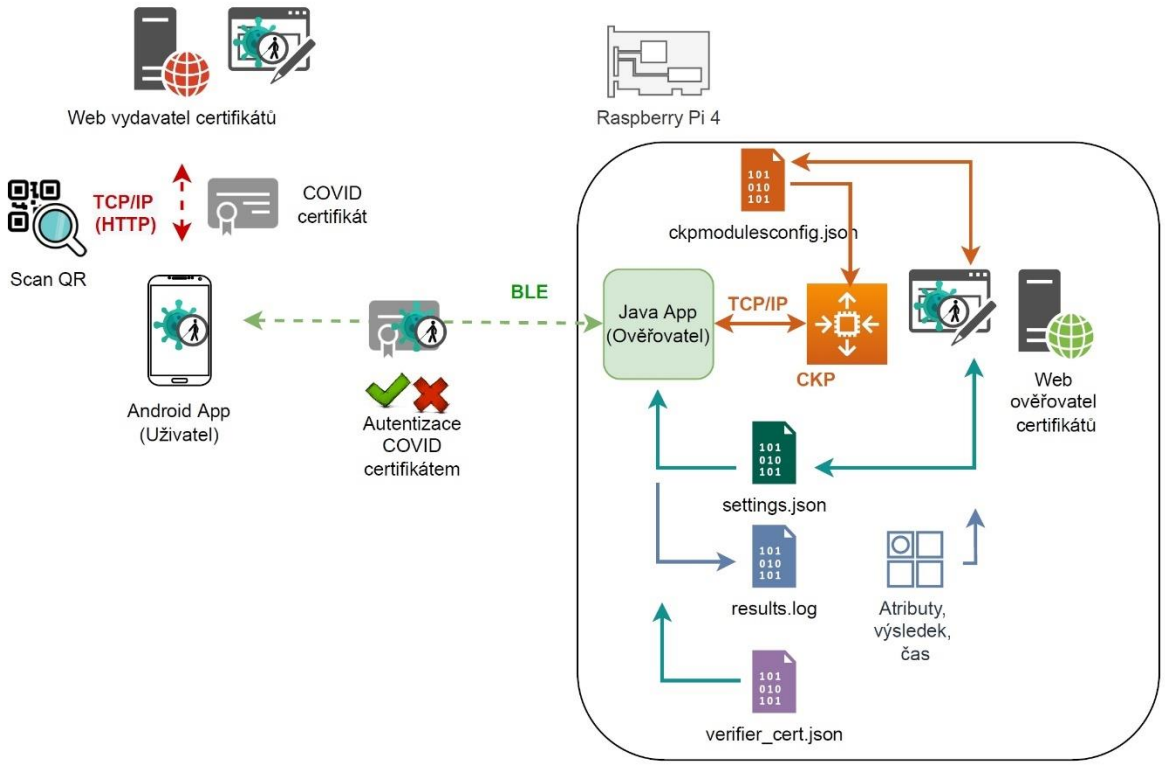


Figure 15: CovidPass verification system

The system consists of the following applications:

- **Certificate Issuer Web**: the CovidPass certificate issuer Web application. The application allows the management of system users (Admin role), certificate issuance and management (role Issuer) and downloading them to users' phones (User role).
- **Android App** (User): an Android application for a mobile phone with support for technology Bluetooth Low Energy (BLE). The app allows you to download CovidPass certificates using generated

[15] https://github.com/eu-digital-green-certificates

QR codes in the Web certificate issuer app and then use them for authentication against the Java App (Verifier). Communication between the Android App (User) and the Web Certificate Issuer is provided via the protocol Hypertext Transfer Protocol (HTTP).

- **Java App** (Verifier): a Raspberry Pi application that enables CovidPass authentication certificates presented by the user (using a mobile app) via the BLE communication interface. App 1) uses the "settings.json" file for custom configuration, 2) writes the logs of the authentication process to the file "results.log"(containing the read attributes, authentication result and authentication time), 3) reads the verifier certificate “cert.json” with authentication attributes enabled, which is signed by the certificate issuer, 4) sends the retrieved attributes and the authentication result to the terminal authorization module via the interface TCP/IP to localhost.
- **Web certificate verifier**: a Raspberry Pi application that allows graphical management of the authentication terminal, i.e. 1) reading/writing to the "settings.json" file, 2) authentication, authentication logs from the "results.log" file, 3) reading/writing to "ckpmodulesconfig.json" defining the active data source modules (CovidPass, reader, Temperature Detector, Detector Tag Detector, Mask Detector) for the CKP authorization module.
- **CKP**: A Raspberry Pi application that evaluates and displays data from connected modules (CovidPass, reader, Temperature Detector, Tag Detector, Mask Detector) according to the file "ckpmodulesconfig.json" and performs the actual user authorization based on these data.

Application Mobile phone screen is shown in Figure 16.

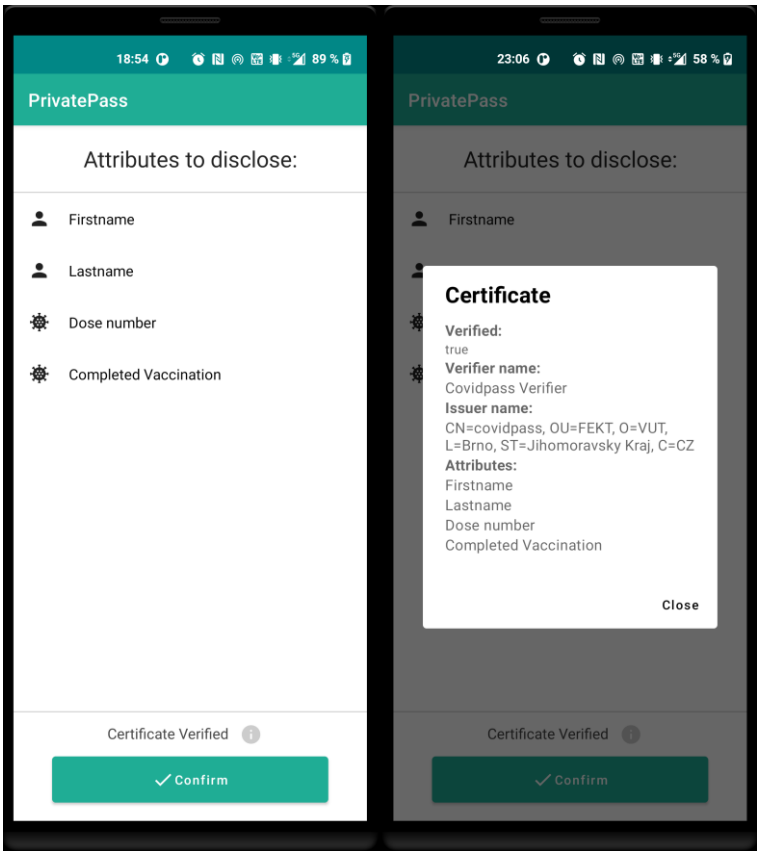


Figure 16: Mobile phone CovidPass application

2.2.8 RiBAC Cryptographic Module

As described in more detail in D3.2 and D4.1, this module is envisioned to provide privacy-preserving cryptographic mechanisms to realize RiBAC. In particular, it should provide the core cryptographic functionalities required for a privacy-enhancing equivalent of the European Digital Covid Certificate (EUDCC).

The key ingredients for such a privacy-enhancing certificate can be summarized as follows:

- Firstly, the cryptographic libraries underlying the EUDCC need to be replaced by privacy-preserving equivalents such as attribute-based credentials in order to allow for selectively revealing only the information that is necessary to prove one's vaccination status.
- Secondly, when aiming for the highest privacy guarantees while still ensuring the integrity of the vaccination proof, certificate sharing needs to be avoided, e.g., by using biometrics to bind certificates to physical users.

Within SUNRISE, the following advancements to those two issues have been achieved:

- Regarding cryptographic libraries, we build upon and together with partners from OLYMPUS[16] the team has contributed to the OLYMPUS open-source project for attribute-based credentials. Specifically, while the existing library only supported selective disclosure of attributes, the team has contributed extended functionalities that are required to realize privacy-preserving health certificates:
    - **Range proofs**: these proofs allow, e.g., to show that the validity period of the Covid test has not yet expired. Also, they are important when proving that biometric measurements are consistent with each other;
    - **Inspection**: to revoke anonymity in case of abuse of a certificate;
    - **Pseudonyms**: for scoped and user-controlled linkability;
    - **Revocation**: in case of fraudulent certificates or in case, e.g., of a positive Covid test despite a vaccination.

  The extensions have been extensively tested under lab conditions to demonstrate the practical efficiency and usability of the extensions.[17]

[16] https://olympus-project.eu/

[17] Jesus Garcıa-Rodrıguez, Stephan Krenn, Jorge Bernal Bernabe, Antonio Skarmeta: *Extension of multi-signature based privacy-ABC system with commit-and-prove techniques*. Technical report, 2023 (currently under submission)

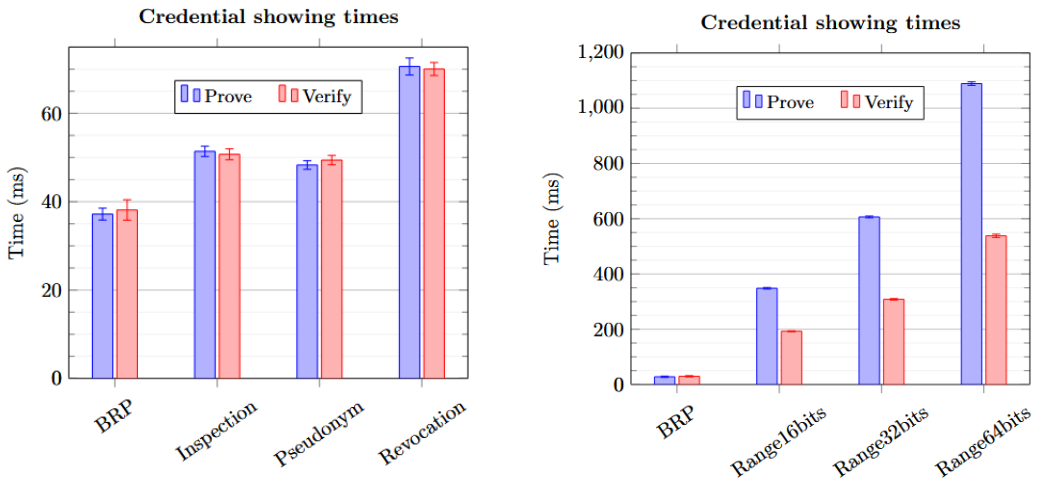


Figure 17 : Running times of necessary extensions of the OLYMPUS attribute-based credential library compared to a basic reference policy (BRP)

- Regarding the binding of physical identities to human beings, the team has developed all necessary protocols and cryptographic primitives.[18] The protocols allow to embed the physical identity based on facial biometrics into the credential, and later prove that the biometrics of the user in front of an entry gate correspond to the biometrics encoded in the credential – without ever having to reveal them in the plain.

  Similar to the above, the feasibility of this approach has been demonstrated under lab conditions, resulting in a running time of slightly above 3 seconds on commodity hardware (i.e., smart phone for the user, a Raspberry Pi 3 for the biometric reader, and a standard laptop for the verifier).

  The development of a full-fledged standalone demonstrator is currently ongoing.

Finally, in a parallel effort, we are planning to investigate in detail the existing reference architecture of the EUDCC to analyse the precise changes that need to be made in order to integrate the above results into the EUDCC.

[18] Jesus Garcıa-Rodrıguez, Stephan Krenn, Daniel Slamanig: *To Pass or Not to Pass: Privacy-Preserving Physical Access Control.* Technical Report, 2023 (currently under submission)

2.3 Deployment

The terminal runs a full-fledged Linux operating system based on the Ubuntu distribution. When the terminal is switched on, other services that are needed for the main program are initialized. For example, the graphical environment, loading all HW drivers, etc. Once all the necessary components are loaded, the main application is launched and runs in full-screen mode. This makes it impossible to run any other application on the terminal, which protects it from unauthorized use or tampering.

2.3.1 Initializing and configuring the terminal

2.3.1.1 Preparing firmware for SD card

To prepare the SD card for the terminal, an image is prepared for this particular type of HW with the operating system, and basic configuration. The system image is loaded onto the SD card in a normal computer.

The terminal uses the ext4 format, which does not have direct support for Windows, so direct editing of a file on an SD card is only possible if the SD card is inserted into a PC with a Linux-type OS.

If the user has only Windows for the initial configuration, he must use SSH. The terminal has DHCP in its default settings. To make it easier to find devices, the terminal is set up with the Avahi program[19], which allows you to find devices on the network using a hostname.

2.3.1.2 Terminal configuration

The configuration of the terminal takes place in two phases.

The initial, unchanged configuration is saved to the terminal at the beginning using a .ini file directly in the terminal repository. It is assumed for this setting that it will only be set during the initial installation. These are for example IP addresses or the graphical interface of the terminal.

User settings that can be performed online by the parent system. Flashing, terminal type, fire alarm or security system activation, etc.).

2.3.1.3 Remote management

In case of a failure or configuration change that cannot be done through the parent system, it is possible to connect to the terminal using SSH. The terminal is secured by allowing access only to those who have an SSH key enabled on the device. Password login is disabled for security reasons.

2.3.2 Graphical interface

The GTKmm library is used to display the graphics on the terminal. This library allows you to design a layout using an external Glade program. This program can easily define buttons, image positions, etc. The output of this program is a .xml file that is easily imported into the terminal program. It processes the elements and adds their functions. The program can then be conveniently controlled via the touch screen.

[19] https://www.avahi.org/

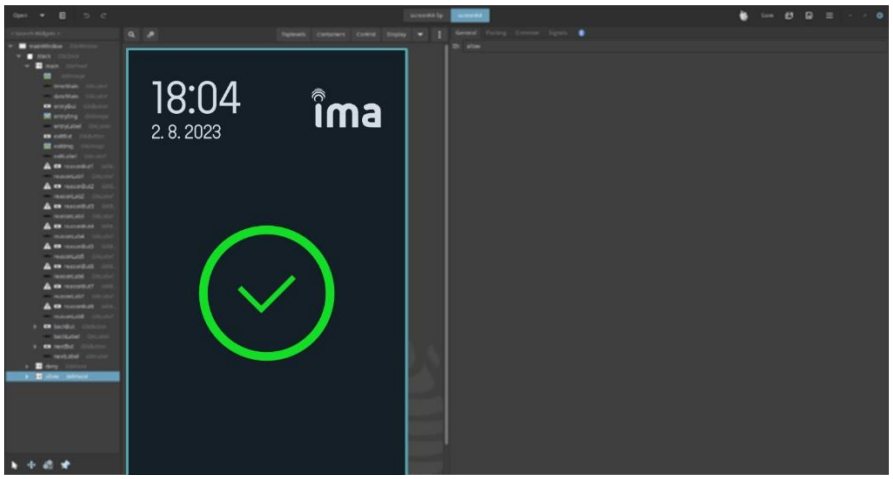


Figure 18: Screenshot from the application GUI builder

So far, the terminal program has a simple user interface with three screens. The reasons on the initial screen are downloaded from the parent system. After evaluating the card privileges, either a permit screen or a deny screen is displayed. All screens are shown in Figure 19.

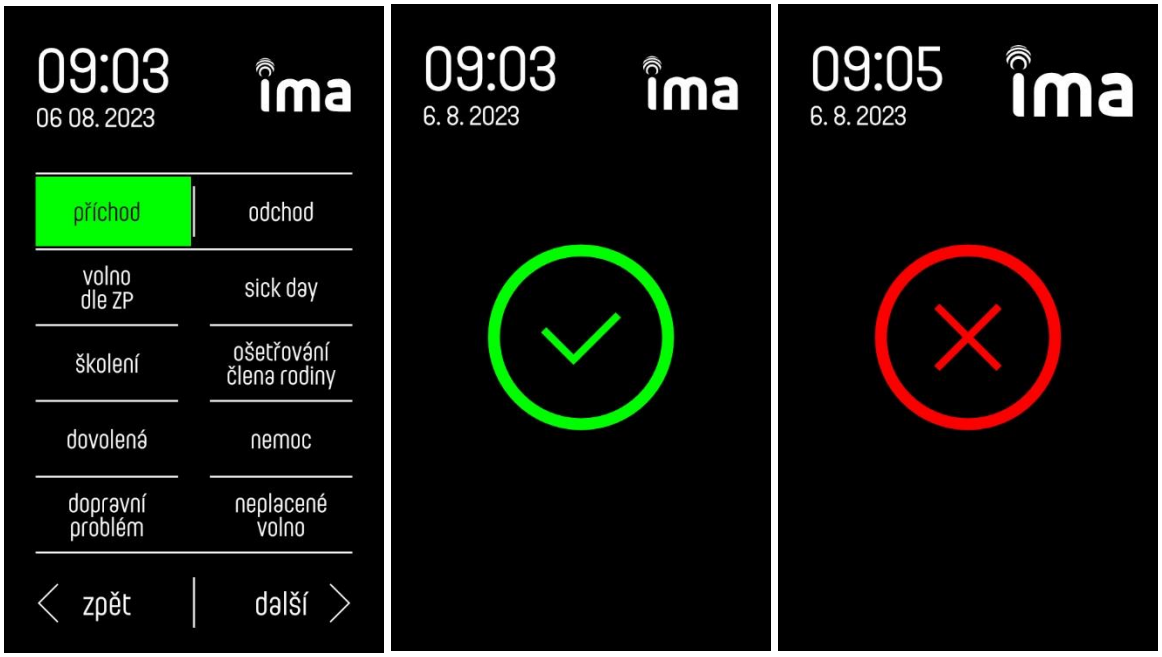


Figure 19: Screenshots from the terminal - Default screen with reasons, permissions, rejections

2.3.3 Power failure protection

The SD card is used as the main storage for the terminal. If an unexpected power failure occurs, the entire SD card may be damaged, rendering the entire terminal inoperable.

The ext4 format, which is a journaling format, is used to eliminate this problem. That is, it takes the data it wants to save to a log (backup) and only after the write is successful does it delete the log. In case the device shuts down during the write, after rebooting the OS detects that the transaction was not completed and starts restoring or repairing the data.

Even if ext4 is used, the SD card controller may be damaged by a sudden power failure. Therefore, the terminal has a backup battery that will hold the terminal for long enough to write everything and complete the terminal properly in the event of a power failure.

2.3.4 Communication interface

2.3.4.1 Communication with the legacy system

The connection to the parent system is established using the UDP protocol. Since this protocol is stateless, the terminal periodically broadcasts the status of whether it is online. The status information is shown on the terminal display. If the user is not using special functions (PINs, the random person checking, etc.), the terminal operates in off-line mode as if it were online. After reconnection to the higher-level system, all passes are uploaded to the server.

2.3.4.2 Wiegand communication

An RFID card reader is connected to the computing module via the Wiegand interface. This is a standard protocol for readers, so the terminal can also handle readers from other manufacturers. A universal reader of IMA's own production is integrated into the base.

The protocol transmission is handled over two signal wires. These signals are typically called D0 and D1. At rest, these wires are held in LOG 1 and their level is 5V. In the case of communication, the corresponding signal is pulled down to LOG 0. Communication is done in such a way that each bit is transmitted sequentially. For bit = O, the pulse on the signal is DO. For bit = 1, the pulse is on signal D1. The pulse length is in the order of 10us, the distance between pulses is in the order of milliseconds.

On the terminal, Wiegand communication is handled via an interrupt on the arrival of the first bit. At that point, a timer is started. With each subsequent pulse, the timer is reset. If the timer expires, the program stops waiting for the next bits and sends the received card number for evaluation.

2.3.5 Access rights

The terminal waits in its own thread for information from the card unit whether a card has been attached. If it has been attached, it starts processing it immediately. Before the card itself is sent for rights evaluation, it has to go through a function to modify the card number (trimming, bit rotation). The output of this function is a card that is sent to the terminal for evaluation. The rights in the terminal are sorted from smallest to largest number to allow a search using the binary halving method.

If the card is found, the system still has to check whether it can evaluate the rights itself, or it has to send the card to a higher-level system for processing (PIN, random person check). After evaluation, the action is performed (relay closure, send to parent system) The selected reason from the terminal display (doctor, lunch) is also packed to the sent pass.

2.3.6 Mechanical solution

The requirements for the form of the terminal were chosen for demanding practical use, including an interesting appearance and robust construction. It was necessary to design a custom box as none of the industrial ones were suitable. For example, it was not compact enough, and especially the internal layout was not suitable for the use of the selected components. Subsequent production had to be taken into account already in the design. The main design challenge was the solution of mounting the terminal on the wall so that it was robust and unobtrusive. All the requirements eventually led to the creation of a two-piece box, joined together by four screws. The internal space was tailored to the

electronics used, the necessary ventilation holes were created and a special wall mounting system was created on the back using a mounting frame.

Figure 20: Contents of delivery of the terminal with mounting frame

2.3.6.1 External cover design

The size of the terminal is based on the display used and the space required around it for mounting, connectors and RFID card reader placement. The thickness of the terminal is determined by the computing module, motherboard, battery and display used. The main dominating feature on the front of the housing is the large 7-inch display. Below it is a texture in a circle, marking the RFID card attachment point. The sides are smooth, with only the two parts of the terminal cover showing. On the bottom, there is an inconspicuous ventilation grille that hides 2 slots for mounting screws to the mounting frame. The back and interior are then designed only for practicality, as it is no longer visible after installation.

Figure 21: View of the bottom of the terminal with the screws ready for mounting

2.3.6.2 Space for electronics

The lower part of the terminal cover is adapted for mounting the base board with the computing module. Posts of the correct height for screwing in the electronics are formed at suitable locations. The battery holder is mechanically designed directly in the cover, which saves space and production costs. To simplify assembly, the battery contacts are directly in the motherboard so. Thus, the holder

in the housing is only an additional mechanical fixing, the main one is the PCB itself. To reduce thickness, the battery axis passes approximately through the plane of the PCB. As a result, a commercially available 18650 Li-Ion rechargeable battery can be used.

2.3.6.3 Display

The display is primarily made for landscape orientation and therefore has asymmetrical long sides of the bezel. For the needs of the terminal, the display needed to be placed in portrait orientation. It was then necessary to cover the asymmetrical bezel with Plexiglas. To maintain the functionality of the touch layer, a Plexiglas of 0.6mm thickness was chosen. It was glued to the terminal box in a groove using double-sided tape.

The display is attached with four screws behind the PCB of the display from the inside of the top part of the terminal. The connectors protruding from the display use the space between the electronics and the reader antenna. This is a complication in terms of assembly, as the antenna must be plugged into the electronics when the two parts of the terminal are assembled. However, this is a one-time issue during assembly because the terminal is not made for user opening.

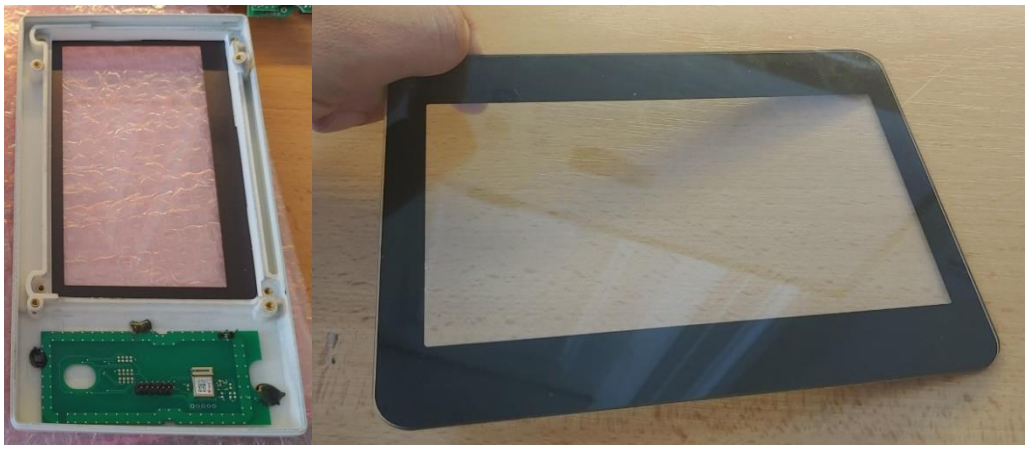


Figure 22: Slot in terminal cover for display, plexiglass with black frame

2.3.6.4 Mounting frame

Once the frame is mounted on the wall, the terminal slides onto the frame tabs and snaps onto the frame with a downward motion. The cables connected to the terminal block and the Ethernet network cable can be routed inside the frame, see Figure 23.

Once the terminal is firmly on the frame, (even at the bottom it cannot be swung away from the wall) the next step is to screw the two M3 screws that are attached to the mounting frame from the bottom of the terminal.

Figure 23: Terminal from the back, mounting frame, mounted frame on the terminal

3 RiBAC Tool Validation in Lab Conditions

In the previous stage of the project, the general concept of the RIBAC system was designed, which consisted of the following parts: detection frame, control terminal, camera sensor, proximity temperature sensor, authentication object reader, display panel and data interface. In addition, the concept of three modules for:

- Non-contact body temperature measurement,
- detection of protective equipment,
- personal authentication and security.

Based on the requirements placed on these modules and the initial experiments carried out, the individual parts of the system were specified in this phase to take into account the needs required by the above modules.

3.1 Risk Assessment

The testing took place in laboratory conditions and especially in an environment whose parameters can be changed. Demonstrators within the SUNRISE project will be installed in a real environment. Fluctuations in temperature at the access points can be expected, as well as uneven lighting due to possible real sunlight at the access points.

Due to IMA's many years of experience with the installation of access systems, measures will be proposed to eliminate these disturbing phenomena.

Similarly, functional verification of RiBAC will take place only on a selected sample of employees, so we avoid overloading the access systems. However, the stress measurements will take place so that future operators have information about the projected throughput of RiBAC during acute deployment during the pandemic.

3.2 Tool Modules Validation

Testing of individual modules was done on the test metal frame with dimensions of 200 × 105 centimetres. The assembly is shown in Figure 24.

Figure 24: The test setup

The tested modules were:

- Mask protection detection.
- Temperature measurement.
- Identification of a person using a RFID identifier.
- Privacy Covid pass.

3.2.1 Mask protection detection

Tests were carried out under a combination of daylight and artificial light with an illumination intensity of 280 - 400 lx. A sample is shown in Figure 25.

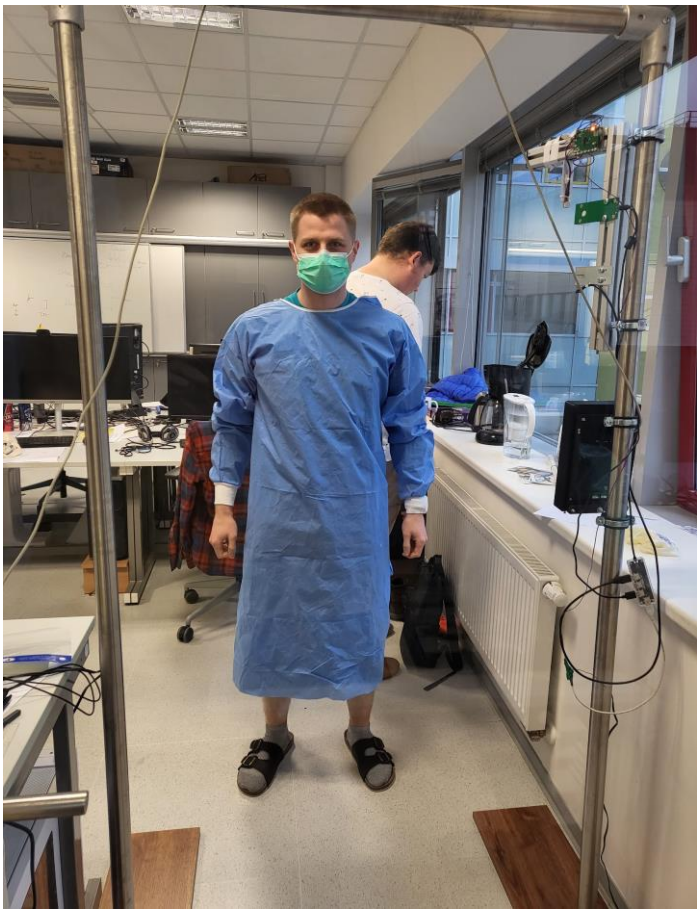


Figure 25: The test setup with user

Respirators and surgical drapes in different colours were used to control the respiratory protective equipment (respirators and respirators) deployed (see Figure 26).

Figure 26: Example of surgical drapes used for airway protection detection testing

Fifty people took part in the testing, some of them more than once. The height of the subjects ranged from 160 to 190 cm, they were adults of different ages, both sexes, with and without beards, with and

without glasses, with different types of clothing with the possibility of influencing the results of the measurements (scarves, hoods, etc.). For the sake of clarity, the following tables (Table 1, Table 2, Table 3, Table 4, and Table 5) show the results for the first 20 to 25 measurements (depending on the variability of the resulting data). All the results obtained are then shown graphically.

3.2.1.1 Measurement of detection sensitivity as a function of distance from the frame

The aim of the measurement was to determine the optimal distance of the person from the detection unit to determine all necessary attributes. This measurement was carried out for a person with a mask on. For individual distances of 1 - 2 m from the frame, 10 measurements were successively taken each time, where either a positive detection (TP - true positive) or a missed detection (FN - false negative) was recorded for the following classes: person and veil.

The experiment shows the sensitivity of the detector as a function of the distance of the objects from the frame, and for each class the sensitivity in % was determined as

$$SENS = \frac{TP}{TP+FN} * 100. \quad (1)$$

A distance of less than 1 m from the frame is not considered, as cameras set at this distance will not capture the entire object. Also, the maximum distance was set to 2 m, as this is the distance where recognition no longer works. The resulting sensitivities (SENS) are written in Table 1 and plotted graphically in Figure 27.

Table 1: Effect of the distance of the person from the detection unit on the detection sensitivity

Class			
Person detection	1	1,5	2
1	TP	TP	TP
2	TP	TP	TP
3	TP	TP	TP
4	TP	TP	TP
5	TP	TP	TP
6	TP	TP	TP
7	TP	TP	TP
8	TP	TP	TP
9	TP	TP	TP
10	TP	TP	TP
SENS [%]	**100**	**100**	**100**
Veil detection			
1	TP	TP	TP
2	TP	TP	TP
3	TP	TP	TP
4	TP	TP	FN
5	TP	TP	TP
6	TP	TP	TP
7	TP	FN	FN
8	TP	FN	TP
9	TP	TP	FN
10	TP	TP	TP
SENS [%]	**100**	**80**	**70**

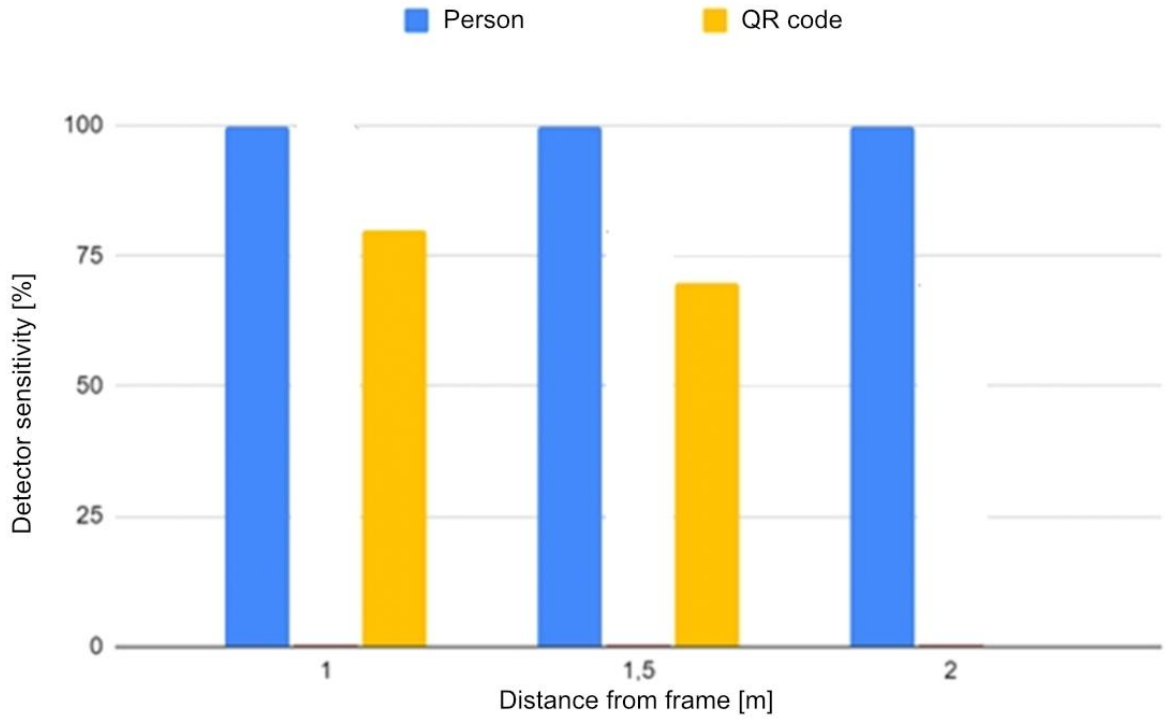


Figure 27: Measurement of the detector sensitivity as a function of the distance of the object from the frame.

As can be seen from the results obtained, the optimal distance of a person from the detection unit is approximately 1 meter, when the sensitivity of the detector is at a very good level.

3.2.1.2 Testing the task of detecting the use of respiratory protection

In this case, the persons were successively approached in front of the detection frame within a distance of 1 m either without respiratory protection or with the use of a respirator or a mask of a different colour. This testing corresponds to a respiratory protection testing scenario, therefore by the nature of the scenario, the persons do not linger in front of the frame but walk away smoothly. In order to verify the robustness of the system against persons with beards in the case of unfitted respiratory protection, special attention was paid to this category during testing. The ratio of persons with respiratory protection to persons without protection was set at 4:3. The results are presented in Table 2 and graphically illustrated in Figure 28.

Table 2: Results of respiratory protection detection testing

Person	Beard	Respirator/ Drape (colour)	TP	TN	FP	FN
1	No	No	0	1	0	0
2	No	No	0	1	0	0
3	No	Black	1	0	0	0
4	No	Black	1	0	0	0
5	No	Black	1	0	0	0
6	Yes	No	0	1	0	0
7	Yes	No	0	1	0	0
8	Yes	Blue	1	0	0	0
9	Yes	Blue	1	0	0	0
10	Yes	Blue	1	0	0	0
11	No	No	0	1	0	0
12	No	No	0	1	0	0
13	No	Green	1	0	0	0
14	No	Green	1	0	0	0
15	No	Green	1	0	0	0
16	No	No	0	0	1	0
17	No	No	0	1	0	0
18	No	Green	1	0	0	0
19	No	Green	1	0	0	0
20	No	Green	1	0	0	0

The A_{CC} (accuracy) of the detector was determined from equation 2

$$A_{CC} = \frac{TP + TN}{TP + TN + FP + FN}, (2)$$

For the whole course of testing then $A_{CC} = 0{,}985$, expressed as a percentage of approximately **98.**5%. Importantly, in no case was a person with respiratory protection incorrectly identified as unprotected. This is important in view of the deployment of the systems in practice, where the existence of false alarms is one of the main reasons why particular systems cease to be used after some time. The fact that the person had a beard or not had no effect on the detection of the face shroud. It was also shown that none of the standard colours of respiratory protective equipment had a negative effect on the detection success rate.

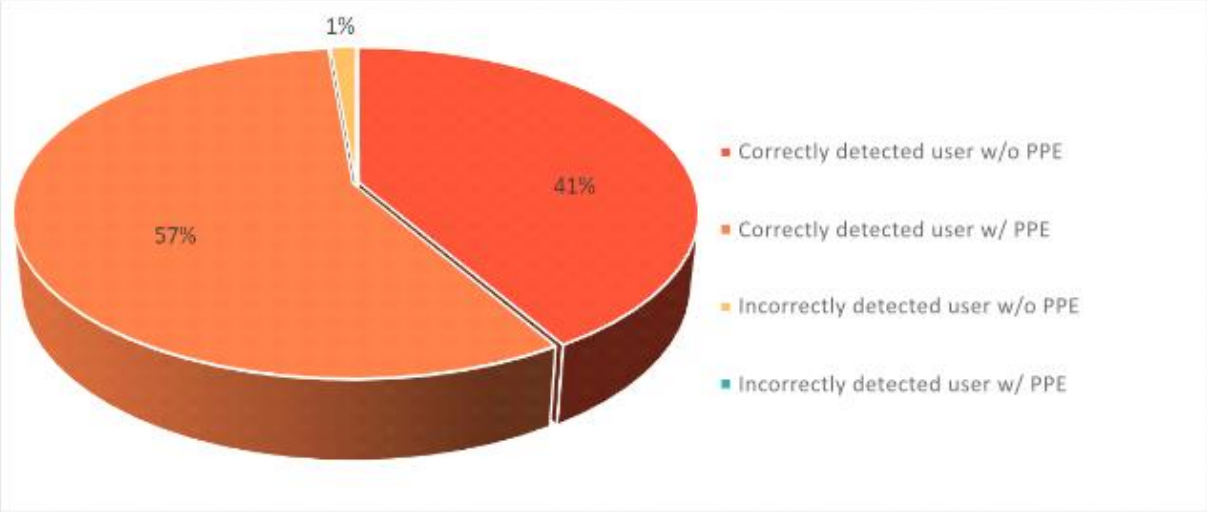


Figure 28: Test results of the task of detecting the use of respiratory protection.

Figure 29: Sample of the respiratory protection detection testing process.

3.2.2 Temperature measurement

Measurement of the temperature deviation detected by the SUNRISE thermal imaging camera from the reference temperature, which is measured by a non-contact thermometer.

The TrueLife Q7[20] non-contact thermometer was purchased for the purpose of controlling body temperature measurement, which is generally reported to be relatively accurate - the manufacturer's claimed accuracy is ± 0.2 °C (although, as it became apparent during initial testing, this claimed accuracy is not entirely adequate). Although generally non-contact thermometers are not considered to be the most reliable, they were deliberately chosen for the control measurements because they measure human skin surface temperature at roughly the same location as the SUNRISE system and are commonly used in healthcare settings due to the ease of handling.

Figure 30: TrueLife Q7 non-contact thermometer for measuring human skin temperature.

The subject was first measured with a non-contact thermometer in the middle of the forehead, then stood in front of the detection frame at a distance of 1 m, and the temperature was read from the unit's display on the SUNRISE system's display panel. It was problematic to secure persons with elevated body temperature during this testing (testing was conducted in full operation on university premises), fortunately one person with signs of acute illness presented during the testing. This person was included in the test group before leaving the site and their elevated temperature was demonstrated by both the reference thermometer and the SUNRISE system. The results of the testing are presented in Table 3 and plotted graphically in Figure 31.

[20] https://eshop.truelife.eu/en/health-care/875-truelife-care-q7-blue-8594175354911.html

Table 3: Test results of automated temperature measurement of persons

Measurements	Reference thermometer	SUNRISE system	Deviation
1	36,5 °C	33,87 °C	2,63 °C
2	36,4 °C	33,73 °C	2,67 °C
3	36,3 °C	33,9 °C	2,4 °C
4	36,5 °C	33,82 °C	2,68 °C
5	36,5 °C	33,77 °C	2,73 °C
6	36,6 °C	33,29 °C	3,31 °C
7	36,5 °C	33,46 °C	3,04 °C
8	36,4 °C	33,71 °C	2,69 °C
9	36,5 °C	33,46 °C	3,04 °C
10	36,5 °C	33,41 °C	3,09 °C
11	36,6 °C	34,14 °C	2,46 °C
12	36,4 °C	33,9 °C	2,5 °C
13	36,6 °C	34,15 °C	2,45 °C
14	36,7 °C	34,1 °C	2,6 °C
15	36,7 °C	34 °C	2,7 °C
16	36,5 °C	33,65 °C	2,85 °C
17	36,2 °C	33,75 °C	2,45 °C
18	36,3 °C	33,55 °C	2,75 °C
19	37,7 °C	35,56 °C	2,14 °C
20	37,8 °C	35,68 °C	2,12 °C

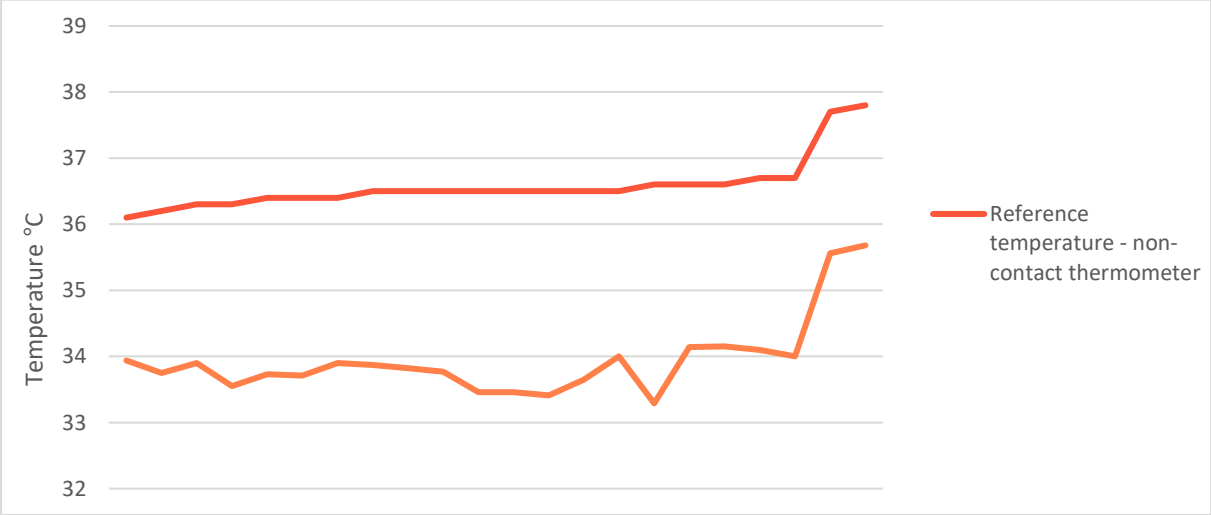


Figure 31: Comparison of body temperature measured with a non-contact thermometer and tested termocamera.

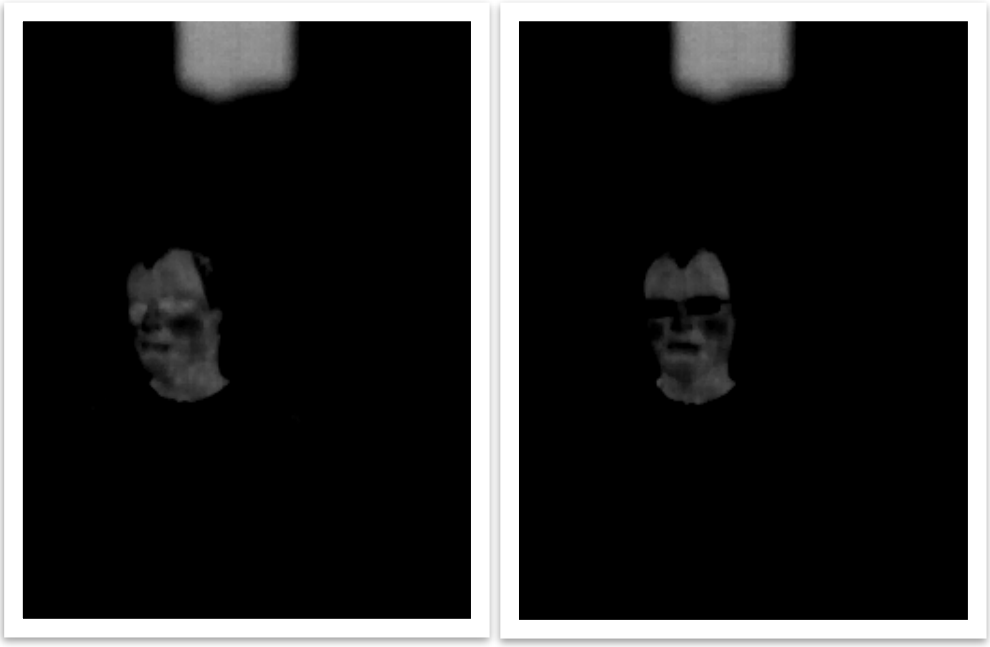
Based on the obtained data, the average value of the difference of temperatures measured by SUNRISE TA system compared to the temperatures obtained by the non-contact thermometer TR was then determined based on (3) and the standard deviation (4):

$$\Delta T_{AVG} = \frac{1}{N} \cdot \sum_{n=1}^{N} T_R - T_A, \quad (3)$$

$$\Delta T_{STDEV} = \sqrt{\frac{1}{N-1} \cdot \sum_{n=1}^{N} \left((T_R - T_A) - T_{AVG}\right)^2} \quad . \quad (4)$$

The resulting value is 2.52 +- 0.41 °C. Thus, for a temperature range of 36.0 - 37.8 °C, the detection system gives an average temperature statistically about 2.52 °C lower than the temperature obtained by the thermometer. This value corresponds to a scientific study from 2022, which compared temperature values obtained by different measurement methods (rectal, oral, underarm, non-contact ear, non-contact forehead). The authors of this study noted an average difference between the forehead surface temperature and the per-value temperature. This value corresponds to the average difference between the temperatures read by the SUNRISE system and the non-contact thermometer. It appears that the thermometer manufacturers deliberately add a correction factor to the actual face surface temperature so that the readings correspond to the temperatures measured in a manner to which ordinary users are accustomed.

Since the body temperature is measured in the upper part of the face (according to the literature, the highest body temperature is in the facial area near the inner corners of the eyes), wearing glasses whose glasses reflect thermal radiation can have a negative effect on the measurement (see Figure 32). For this reason, attention has been paid in this section to persons wearing glasses. The results of this experiment are presented in Table 4.



a) b)

Figure 32: Illustration of the effect of wearing glasses on the measurement of emitted thermal radiation, a) face without glasses, b) face with glasses.

Table 4: Test results of automated temperature measurement of people with a focus on the presence of glasses.

Measurements	Glasses	Reference thermometer	SUNRISE system	Deviation
1	No	36,6 °C	34,85 °C	1,75 °C
2	No	36,7 °C	34,6 °C	2,1 °C
3	No	36,7 °C	34,45 °C	2,25 °C
4	No	36,5 °C	34,63 °C	1,87 °C
5	No	36,5 °C	34,21 °C	2,29 °C
6	No	36,5 °C	34,74 °C	1,76 °C
7	No	36,5 °C	34,72 °C	1,78 °C
8	No	36,5 °C	34,73 °C	1,77 °C
9	No	36,5 °C	34,47 °C	2,03 °C
10	No	36,5 °C	34,5 °C	2 °C
11	Yes	36,4 °C	34,09 °C	2,31 °C
12	Yes	36,6 °C	34,07 °C	2,53 °C
13	Yes	36,5 °C	34,08 °C	2,42 °C
14	Yes	36,4 °C	33,93 °C	2,47 °C
15	Yes	36,5 °C	33,98 °C	2,52 °C
16	Yes	36,5 °C	34,11 °C	2,39 °C
17	Yes	36,5 °C	33,81 °C	2,69 °C
18	Yes	36,5 °C	34,16 °C	2,34 °C
19	Yes	36,5 °C	33,82 °C	2,68 °C
20	Yes	36,4 °C	34,09 °C	2,31 °C

If we determine the average temperature difference between the SUNRISE system and the reference non-contact thermometer and its standard deviation, we obtain the following values for persons with and without glasses: 1.96 +- 0.21 °C (persons without glasses) and 2.47 +- 0.14 (persons with glasses). Shown in Figure 33 are the temperatures measured by the reference thermometer and the temperatures measured by SUNRISE after correcting the values by the calculated average value for persons with and without glasses. In general, it can be concluded that wearing glasses can reduce the temperature measured by the SUNRISE system by about 0.43 to 0.62 degrees. For more accurate measurements, it is therefore advisable to ask persons to remove their glasses for a short time.

Figure 33: Comparison of body temperature measured with a non-contact thermometer and SUNRISE with correction of the resulting temperature.

For corrected values of measured temperatures T_{Ak}we then determined the absolute value of the average difference between the temperature measured with the non-contact thermometer and the SUNRISE system according to (5) $\Delta T_{|AVG|} = 0{,}14\ ^{o}C$.

$$\Delta T_{AVG} = \frac{1}{N} \cdot \sum_{n=1}^{N} |T_R - T_{Ak}|,$$

3.2.3 Testing the COVID PASS application

Testing the use of the developed attribute-based COVID passport validation application was aimed at measuring the response speed of the detection unit to user-triggered initiation of communication via *Bluetooth* interface. The speed of communication using BLE was measured using the *measureTimeMillis()* function. First, an attempt was made to measure the time interval from ViewModel initialization to the detection of the verifier terminal. These times varied on the order of a few seconds, but usually fell in the interval 0 - 10 *s*. In some cases, the device was found immediately, in others it took a few seconds to find the device. Another measured interval was the receipt of the authenticator's prompt from the button press to initiate communication; this time was measured to be in the interval from 4.2 *s* to 4.3 *s*, with minimal dependence on the number of attributes detected. The last measurement step was the time from confirmation of sending the requested attributes, after receiving the authentication result. The measured time for this exchange ranged from 4.7 *s* to 5.7 *s*, with a lower value with a higher number of revealed attributes. The total communication time using BLE was measured to be about 9 to 10 *s*. Including the search for nearby devices, this value is at most about 20 *s*. These times can be considered feasible. To reduce them, it would be possible to change the wait intervals within the *waitForMessage()* function within the code, but this could compromise the reliability of the communication. Table 5 and the graph in Figure 34 describe the dependency of the message exchange time on the number of detected attributes.

Table 5: Effect of the number of detected attributes on communication

Attributes	0	2	4	6	8	10	12	14	16	18	20
Challenge [ms]	4265	4259	4261	4164	4364	4367	4273	4370	4283	4381	4385
Verification [ms]	5775	5622	5631	5420	5430	5206	5033	5133	4914	4711	4718

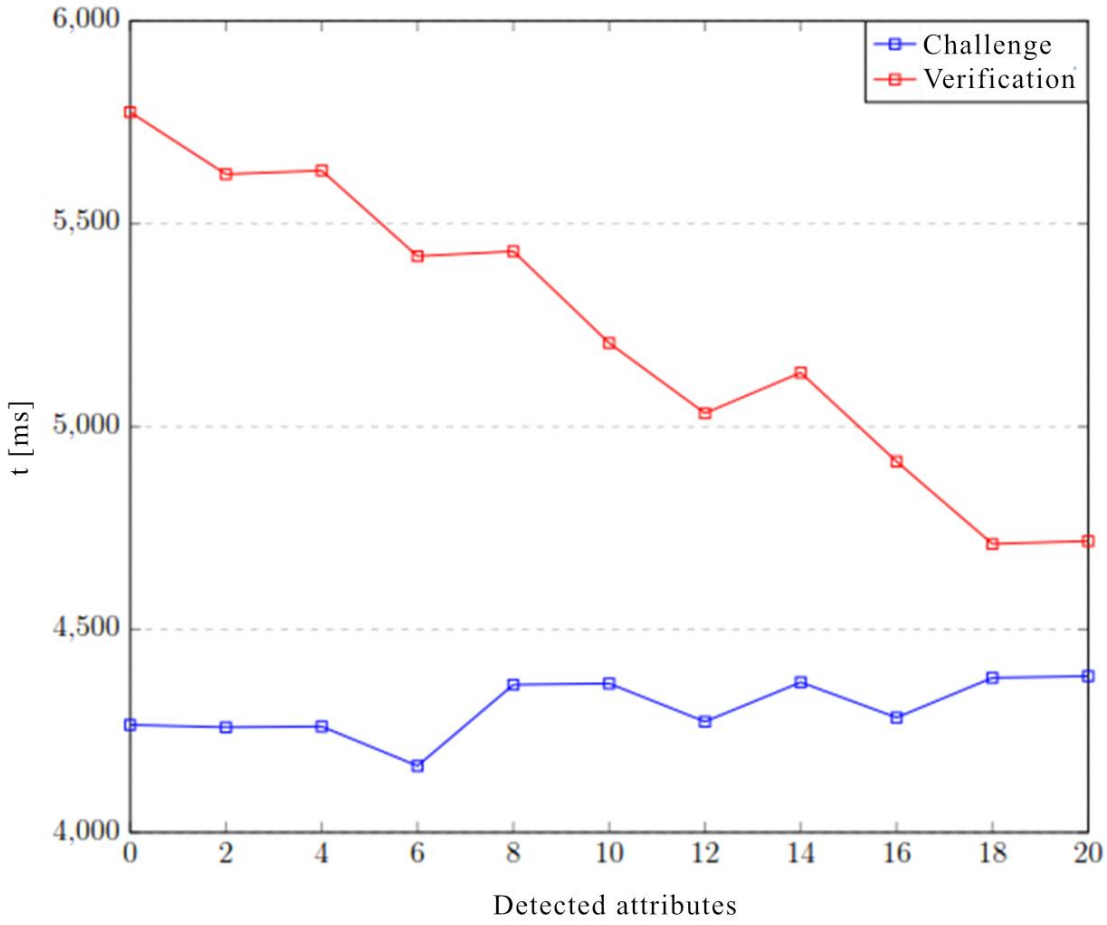


Figure 34: Effect of the number of detected attributes on communication.

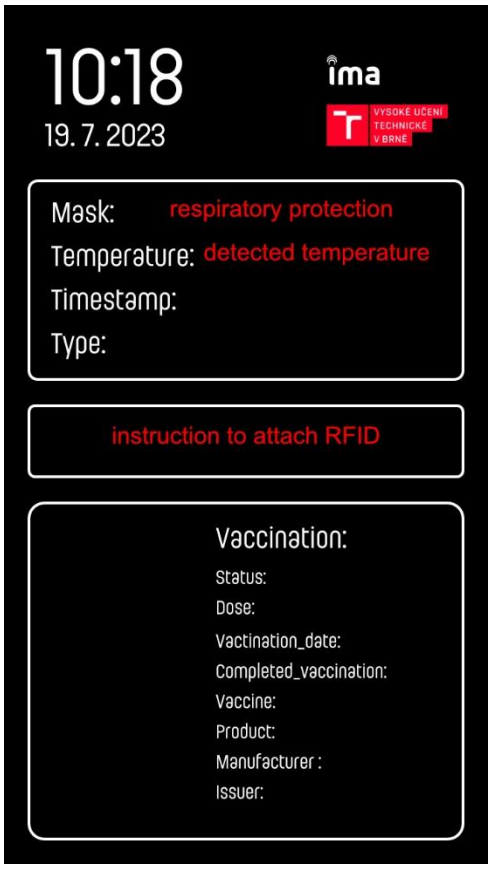


Figure 35: Information on the display.

3.3 Integrated RiBAC Validation

The whole system validation has been done on set with access control turnstile to achieve the experience of real person's passes. The setup is shown in Figure 36.

Figure 36: The test setup with turnstile.

Thus, the total time was measured in this testing, which consisted of the following parts:

- The person stood 1 m in front of the detection frame - time measurement started,
- Temperature and respiratory protection,
- The person attached an RFID chip,
- The system has signalled safe entry of a person - the timer has stopped ticking.

The results are presented in Table 6 and plotted graphically in Figure 37.

Table 6: Total clearance time of the detection frame

Person	1	2	3	4	5	6	7	8
Time [s]	15	8,324	10	7,707	7,985	7,1787	10,273	12,218
Person	9	10	11	12	13	14	15	16
Time [s]	6,942	6,571	10,296	8,002	7,664	9,833	8,108	6,997
Person	17	18	19	20	21	22	23	24
Time [s]	8,961	11,222	5,974	5,233	7,224	13,632	14,023	9,156

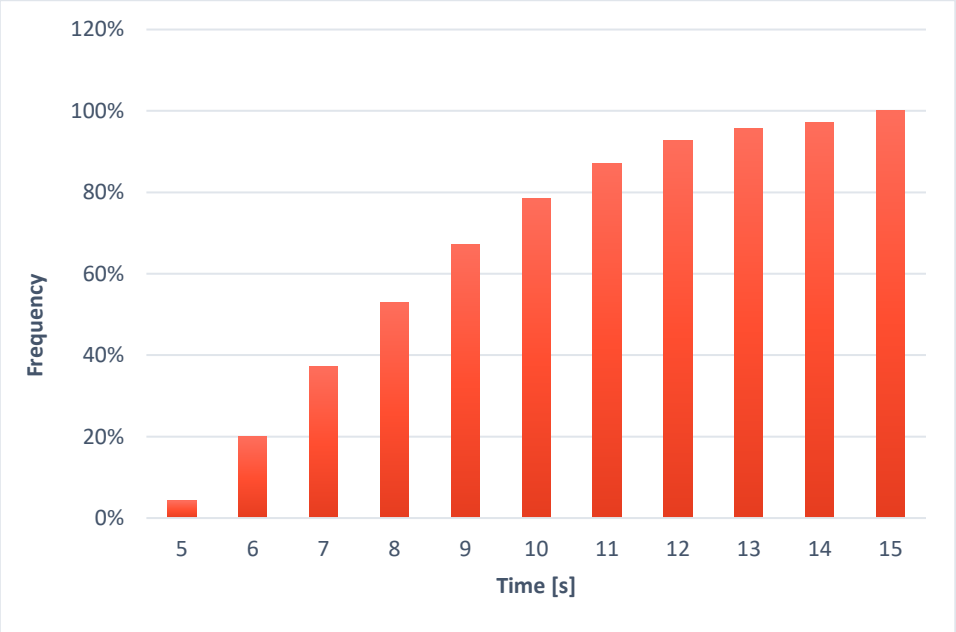


Figure 37: Cumulative histogram of the total clearance time of the co-located detection frame.

From the results obtained, the average time required for a person to pass through the detection frame was calculated:

When checking then T_{AVG} **= 10,09 +- 4,14** s

Based on the cumulative histogram, we can then conclude that:

In a check, 96% of persons pass through the detection frame within 13 seconds.

In general, the greatest delays in passage were caused by 2 factors:

1. Slow response of people to the prompt for attaching the RFID tag - this was particularly evident when people first passed through, when they did not know exactly what the prompt to attach looked like visually. Recommendation: improve the visual response of the system.
2. Auto focusing of the capture device - the capture device automatically adjusts the sharpness of the captured image. In the case of a new arrival, it sometimes takes time to find the optimal image sharpness. In the original design of the camera module, a camera with manual focus was to be integrated and fixed at the desired distance. However, when

the device was designed, these cameras were not currently available and an autofocus camera was used instead. Recommendation: replace the autofocus with manual focus.

3.3.1 Extended testing

Further testing experimented with respiratory protection and temperature detection for different types of head and face coverage. Test subjects wore:

- Hood - had no effect on respiratory protection detection, nor demonstrable effect on temperature detection.
- Cap - had no effect on respiratory protection detection, nor demonstrable effect on temperature detection.
- Face scarf - The face scarf was detected as respiratory protection, it had no demonstrable effect on temperature detection.

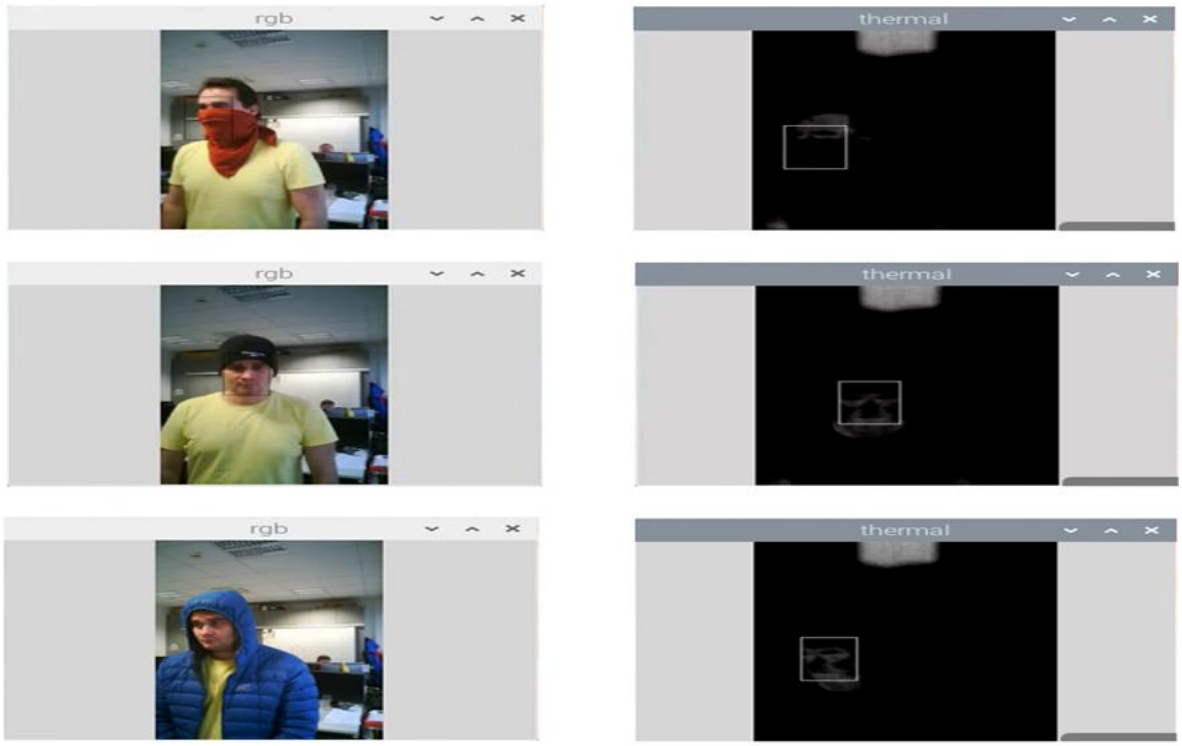


Figure 38: Example of experimental testing.

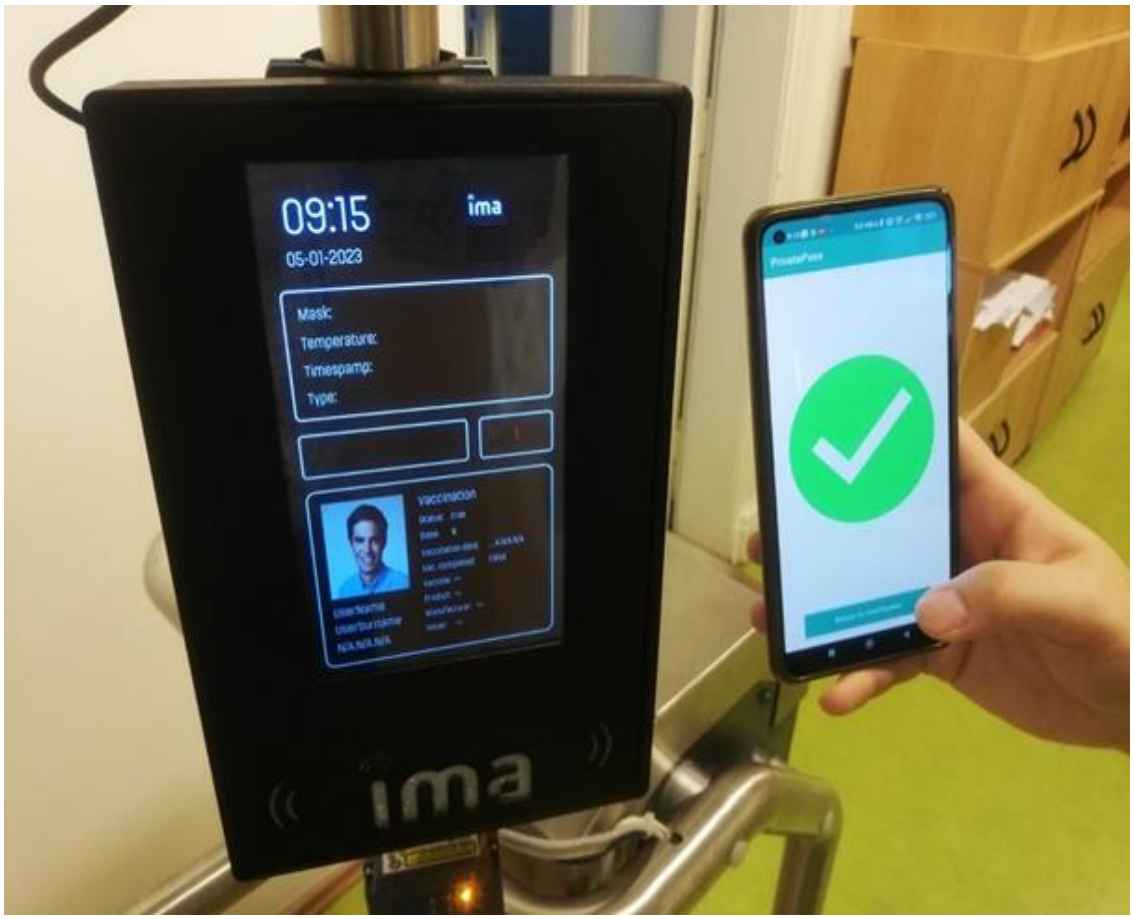


Figure 39: Vaccine credential verification

4 Pilot trials execution (feasibility analysis)

4.1 Proofs of concept

Background Controlling physical access to critical infrastructure and facilities during pandemics is an important measure to reduce workforce exposure to infectious diseases and to maintain the business continuity of critical infrastructures. Going forward, we will use the term risk-based access control (RiBAC) for such measures. One well-known and widely used RiBAC measure has been the introduction of digital health credentials in the form of the EU Digital COVID-19 Certificate in the context of the COVID-19 pandemic. This and similar solutions use digital signatures (from an authority) to sign a document linking an individual's identification data (name, date of birth, etc.) to their health status, (vaccinated, recovered, tested, date of vaccination/recovery/test, type of vaccine, etc.). Verification is then typically done by scanning a QR code containing the dates and his/her signature and checking personal attributes against a physical ID (e.g. passport, driver's license, etc.). However, this current technology has some drawbacks. First, the need to rely on physical identity documents in RiBAC makes the verification process time consuming and less scalable than desired. Second, the disclosure of all the data contained in this certificate (personal and health data of the individual) for RiBAC purposes violates the privacy of individuals. Privacy is often adapted to a decentralized approach, i.e., certificate verification is not done at a central location, (e.g., at the issuer of these credentials), but locally. However, during authentication, all information written in the certificate is revealed, although not all of this information is necessary to decide whether access should be granted or denied. One important aspect is that disclosure of the vaccinated/renewed/tested state is not necessary for the access decision: it is sufficient to know that one of these criteria is met. This is important in cases where vaccination information is sensitive or controversial.

Ambition the project aims to develop a new architecture and software component for RiBAC that takes scalability and privacy into account (as shown below). Identity data exchange involves several privacy-related aspects, especially in cases of personal data sharing. The aim is to enable the secure and trusted exchange of this information between multiple parties involving multiple actors (government agencies and open datasets, including for commercial use) and with different objectives and requirements in terms of security, data protection and trust issues, as well as compliance with applicable legislation and the EU policy framework for cross-border data flow. In this context, the project will address four important aspects:

(i) compliance with the GDPR regulatory basis,

(ii) the concept of Privacy by Design,

(iii) Privacy by Default settings; and

(iv) guidelines for compliance with the GDPR.

The aim of the project is to take privacy aspects into account when designing the solution, not only from a technical point of view, but also from a sociological, ethical and legal point of view, and to offer a solution that is modular and can be integrated into existing physical access control solutions. It is also important to closely monitor the development of the European Digital Identity Wallet to allow for future interoperability. In addition, the design will be made to be suitable for different types of access control scenarios that have different requirements with regard to privacy and scalability, e.g. closed critical infrastructure with access only for employees or open critical infrastructure to which everyone has access (hospitals, public transport, etc.). The developed scalable platform for RiBAC will consist of the following building blocks: an ID management server with interfaces suitable for incorporating privacy enhancing technologies (e.g. anonymised login credentials), mobile apps and HW

accessories/readers. RiBAC is partially based on the results of the SACON, CyberSec4Europe and OLYMPUS European projects[21].

4.2 Description of piloting activities

This section follows up on information described In Deliverable D4.1 Access Control Conceptualization; which provided a high level overview of possible WP4 piloting activities.

Information below serves as a confirmation of the selected CI sites for the pilots; together with new information received and bilaterally agreed with the corresponding CI operators.

4.2.1 Czech pilots – IMA

IMA has been a long-term supplier of a robust access control system (AC system) called IMAporter Pro[22] to the two selected Czech CI operators, taking part in the piloting activities in the Czech Republic. These CI operators process tens of thousands of identification transactions in their daily operation. Especially during the morning and afternoon rush hours and the change of work shifts, the throughput of the AC system is critical.

The RiBAC tool, as a crisis measure for the time of the pandemic, would therefore unnecessarily prolong the screening of employees, therefore it is not desirable to deploy it in full operating conditions. The proposed piloting schedule therefore entails several phases, the first one will involve the usage of an autonomous RiBAC tool device.

4.2.1.1 Military University Hospital in Prague (health)

- Long-standing operation of IMAporter Pro AC system, 6.000 RFID 13,56 MHz Mifare identifiers in daily operation.

Figure 40: Military University Hospital in Prague

[21] SACON: https://starfos.tacr.cz/en/projekty/7D19001; CyberSec4Europe: https://cybersec4europe.eu/; OLYMPUS: https://olympus-project.eu/

[22] https://www.ima.cz/products/access-control-systems/imaporter-pro/?lang=en

- Proposed piloting phases will be as follows:
  - Phase 1: Autonomous device (M14-M17).
  - Phase 2: Partial integration – parallel architecture scenario (M18+).
  - Phase 3: Full integration – if possible (M30+).

4.2.1.2 Czech Technical University in Prague (education)

- Long-standing operation of IMAporter Pro ACS. 40.000 RFID 13,56 identifiers in daily operation.

Figure 41: Rectoracy of the CTU in Prague

- Proposed piloting phases will be as follows:
  - Phase 1: Autonomous device (M14-M17).
  - Phase 2: Partial integration – parallel architecture scenario (M18+).
  - Phase 3: Full integration – if possible (M30+).

4.2.2 Italian cluster

Piloting activities concerning the two envisioned pilots within the Italian cluster are planned and discussed in close cooperation with partner INS, who is the lead representative of the cluster.

It is envisioned that one autonomous RiBAC device will be used subsequently in the first stage of the two Italian cluster pilots – INS/FVG and CAF.

4.2.2.1 Insiel HQ offices in Trieste (digital)

Insiel has its headquarters in Trieste, Via San Francesco d'Assisi 43, and other offices on the territory of Friuli Venezia Giulia. The test of RiBAC device will take place in Trieste and in particular at the main entrance.

The physical access control is structured in two parts, the main door (picture 1), is open from 7:00 to 19:00 and open on request the rest of the day.

Figure 42: Insiel HQ entrance

Visitors must be registered and authorized by security staff. Insiel employees have to go through a second access point and identify themselves using a company card. The following picture shows the second step access, where employees have to use a company card; while visitors use a temporary visitor card provided by the security staff, after registration.

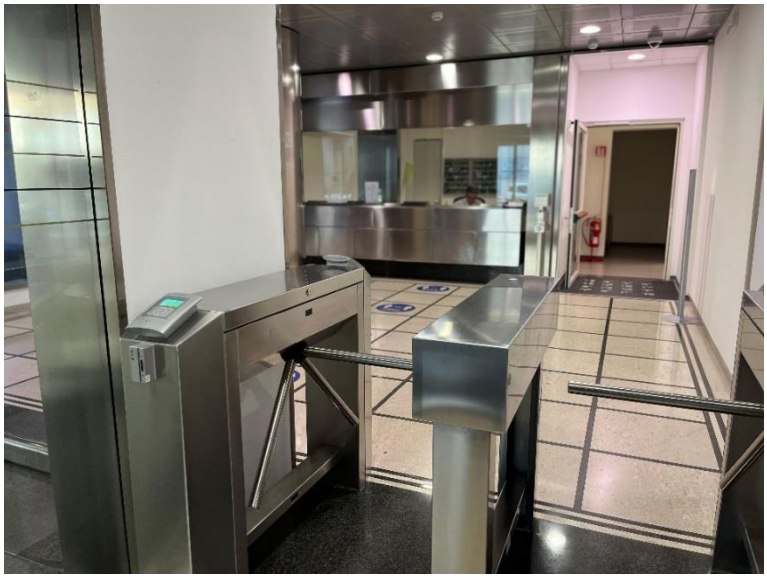


Figure 43: Insiel HQ - turnstile

The Ribac tool will be positioned in the entrance, between the security staff and turnstiles.

Currently, the implementation of a new access system is ongoing. The new access system will be composed by hardware and software components, in particular LBX 2910 terminal with Rfid 2xMifare, LBX 2901 reader to be connected to CCN7210 to open the gate, customized RFID Mifare cards and access control cards system[23].

[23] https://www.solari.it/solutions/other-solutions/access-control/

The reader LBX 2910 has been tested by our Cybersecurity Team, with the aim to improve the gate's security posture. Each gate permits access to a specific bureau, and each employee is provided with a smartcard to identify and authorize the worker.

The tests have been done using specific tools, in order to emulate a new smartcard from reader sniffed data flow; read, clone and emulate employee's smartcards, and spoof the employee's identity to access the building and the Organization's bureau.

- Proposed piloting phases will be as follows:
  - Phase 1: Autonomous device; using a visual sign by a dashboard or a sound to validate the access control (M14-M17).
  - Phase 2: Partial integration – integration test environment with the new Insiel access system, involving about 20-30 employees (M18+).

4.2.2.2 CAFC HQ offices in Udine (water/digital)

- The existing AC System adopted by CAFC is composed of per-floor building devices, each consisting in an RFID device coupled with an extra mask detection/temperature measuring device.
- Proposed piloting phases will be as follows:
  - Phase 1: Autonomous device; using a visual sign by a dashboard or a sound to validate the access control (M14-M17).
  - Phase 2: Partial integration – integration test environment with the new CAFC access management system, involving about 20-30 employees (M18+).

4.2.3 Slovenian cluster

Piloting activities concerning the two envisioned pilots within the Slovenian cluster are planned and discussed in close cooperation with partner ICS, who is the lead representative of the cluster.

It is envisioned that one autonomous RiBAC device will be used subsequently in the first stage of the three Slovenian cluster pilots – UKC, SZ and TS; as there will be be three devices initially constructed in total for all piloting activities in the Phase 1.

4.2.3.1 UKC City Children Hospital in Ljubljana (health)

- Existing AC system adopted in City Children Hospital of the UKC is supporting access control without any other control functions.
- The unit has three entrances; one dedicated to patients and visitors, and two for employees. All three are equipped with ACS that unlocks the doors.
- At present, UKC is using four different AC systems. Therefore, there is a large potential for integration of the different systems and RiBAC tool will play an important role in the future integration.
- Proposed piloting phases will be as follows:
  - Phase 1: Autonomous device with selected employees and entrances (M14-M17).
  - Phase 2: Partial integration with the existing infrastructure using a test integration environment (M18+).

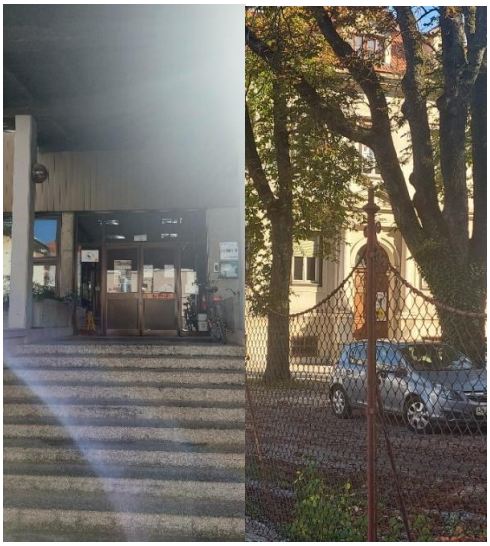


Figure 44: UKC Ljubljana Old City Children Hospital

4.2.3.2 SZ – Main railway station building in Ljubljana (transport)

- The main railway station building has three entrance points. The access to the railway platforms is possible through an underpass at two of the main entrances.
- Proposed piloting phases will be as follows:
  - Phase 1: Autonomous device installed at an office of the railway station; with selected employees to validate the access control and other RiBAC modules (M14-M17).
  - Phase 2: Partial integration (if possible) – integration test environment with existing infrastructure (M18+).

Figure 45: Main railway station in Ljubljana

4.2.3.3 TS - Office building of Telekom Slovenije (digital)

- RIBAC tool used will be used to control the access to the relaxation space for TS employees called “Brihta Plac” in Cigatelova street office building of Telekom Slovenije.
- Proposed piloting phases will be as follows:

- Phase 1: Autonomous device with selected employees to validate the access control and other RiBAC modules (M14-M17).
- Phase 2: Partial integration (if possible) – integration test environment with existing infrastructure (M18+).

Figure 46: TS offices in Cigaletova street

5 Conclusions

This deliverable presents the initial development of the Risk-Based Access Control (RiBAC) tool within SUNRISE based on the architecture initially presented in the private deliverable D4.1. The RiBAC tool consists of a collection of modules focusing on pandemic-specific access control features (protective tool detection, temperature measurement, vaccination credential check) as well as the required supporting modules (e.g., the cryptography module) and their integration into existing Access Control Systems.

The modules were tested in lab environments based on different metrics relevant to the respective modules and use cases. Moreover, the document describes the test of a first integrated setup.

Next, the deliverable focuses on the piloting activities, where the tool will be tested in a real-world environment of various CI operators. In more detail, the tool will be tested in seven CI pilots from the Czech Republic as well as the Italian and Slovenian Clusters.

This document also provides the first version of RiBAC tool and training guide. The content of this deliverable will be continuously updated and reported in the next versions in D4.3 (M20) and D4.5 (M31). The pilot reports will be presented in D4.4 (M23), and finally in D4.6 (M34).

Annex I - Informed consent of pilot participants

The template below is designed for IMA s.r.o. as operator and will be appropriately modified for other operators:

INFORMED CONSENT
OF A PARTICIPANT OF THE SUNRISE PROJECT VERIFICATION PHASE

I, ... *(name and surname)*, confirm that I was properly instructed about the purpose of the data processing and about the scope of the processed personal data in the verification phase of the SUNRISE project provided by IMA s.r.o., with its registered office at Na Valentince 1003/1, 150 00 Prague 5, Czech Republic.

A) I agree ☐ *(tick the check box if you agree. If you do not agree, do not tick the box or any other data)*

That my identification data and personal data to the extent of

- Name and surname
- Internal identifier (identification during an Entry / Exit)
- Identification number – identifier stored on the card
- Address
- Employer (name of the entity)
- Address of the employer
- Personal ID document number (state-issued ID, passport, or another photo document)
- Visited person / organizational unit
- Time of entry and exit to / from the building or from another monitored area

were further processed by the IMA s.r.o. development center for the research purpose of the SUNRISE project.

I am aware that I may withdraw my consent to the processing of my personal data mentioned above at any time by a written request.

I declare that I have been informed about the circumstances and actions of processing personal data in the SUNRISE project. I declare that I fully understood the information, and that my consent to the collection and further processing of my personal data by IMA s.r.o. was granted upon my free will.

.....	.....	.....
Participant's name and surname	Participant's signature	Date

Thank you for your cooperation on the SUNRISE project Demonstrator.

The SUNRISE project has received funding from the Horizon Europe research programme (2021-2027), the European Union's Research and Innovation programme under grant agreement no. 101073821. For more information, see: https://sunrise-europe.eu/.

Annex II – Privacy policy & User guide for CI operators

Privacy Policy for Product Testing

In the following we use:

- The term "**application operator**" (or just "**operator**") for the entity that operates the RiBAC project application and is responsible for the purpose of processing personal data and for complying with the conditions set out in the GDPR. The operator of the RiBAC project application is therefore in the position of a "**controller**" within the meaning of Article 4(7) GDPR.
- The term "**application user**" (or just "**user**") for an individual or entity that uses the functions of the RiBAC project application through the services of an "operator". A user has a reasonable expectation that his or her personal information is adequately protected when using the RiBAC Project Application and should not fear that his or her personal information will be misused in any way.
- The term "**data subject**" for an individual (natural person) whose personal information is used in the development, creation or operation of a RiBAC project application. A data subject may also be an "application user" if their personal information enters into any operation in the operation of the application.

Protection of personal data during application testing

If personal data of identifiable natural persons are used in the testing of the RiBAC project application, the project developer must take into account all relevant provisions and obligations of the GDPR. In particular, some exceptions arise in the application of certain data subjects' rights directly from the relevant provisions of the GDPR.

Data protection and Privacy by Design

When developing an application for the RiBAC project, it is necessary to take into account the requirements of personal data protection and privacy of the application user from the initial steps of development. Data protection as part of user privacy should be considered as an integral part of application development, not only in the testing phase. This requirement is based on the provisions of Article 25 of the GDPR, as the development department is the controller of personal data throughout the development and testing of the product.

Informed consent of participants in product testing

Legal basis for data processing

All processing of personal data about natural persons (data subjects) must comply with the processing principles set out in Articles 5 and 6 of the General Data Protection Regulation (GDPR). Article 9 of the GDPR then provides for specific derogations for the lawfulness of the processing of special categories of personal data (sensitive data).

Article 6 of the General Data Protection Regulation (GDPR) sets out 6 legal bases for processing personal data, and the order of these bases has no particular significance, i.e. no legal basis takes precedence over the others.

The processing of personal data is lawful only if at least one of these conditions is met and only to the relevant extent:

a) the data subject has given **consent to the** processing of his/her data;

b) the processing is necessary for the **performance of a contract** to which the data subject is a party or for measures taken before the conclusion of the contract;

c) processing is necessary for compliance with **a legal obligation**;

d) processing is necessary to protect the **vital interests of the** data subject;

e) processing is necessary for the performance of **a task carried out in the public interest** or in the exercise of official authority vested in the controller;

f) processing is necessary for the **pursuit of the legitimate interests of the controller**, provided that those interests do not override the interests or fundamental rights and freedoms of data subjects requiring the protection of personal data, in particular where the data subject is a child.

It is clear that not all of the above legal titles will be acceptable for the processing of data in the test phase of the RiBAC product. Clearly, legal titles (c) /fulfilment of a legal obligation/, (d) /vital interest of an individual/, (e) /task carried out in the public interest/ will not be applicable. The most appropriate legal title for testing a RiBAC product is probably the **consent of the individual** whose personal data will be entered into the testing.

Should the RiBAC project developer choose the legal title of the **legitimate interest of the controller**, then a balancing test between the interest of the controller (the project developer) and the interest of the natural person concerned in the protection of his fundamental rights and freedoms must be carried out. If the interests of the individual concerned outweigh the interests of the controller, this legal title cannot be used for the processing of personal data for the testing of the RiBAC product. Within the meaning of the GDPR (Recital 47), the interests and fundamental rights of the data subject could override the interests of the data controller, in particular where the processing of personal data takes place in circumstances where the data subjects do not reasonably expect further processing. Therefore, the application of the legal title 'legitimate interest of the controller' requires three cumulative conditions to be met - (a) firstly, the pursuit of the legitimate interest of the controller, (b) secondly, the necessity of the processing of the personal data for the pursuit of the legitimate interest pursued and (c) thirdly, that the interests or fundamental rights and freedoms of the data subject requiring the protection of personal data do not take precedence over that interest. However, in order for this legal title to apply, it is also necessary that the processing in question is necessary for the fulfilment of this interest of the controller (app operator) and that the interests or fundamental rights and freedoms of the data subject do not override this right of the app operator. In balancing these conflicting rights and interests (the rights and interests of the controller on the one hand and the rights and interests of the data subject on the other), account must be taken, inter alia, of the reasonable expectations of the data subject and the scope of the processing in question and its impact on that natural person (data subject).

The legal basis for the processing of personal data in the "vital interest of the individual (data subject)" or in "tasks carried out in the public interest" can be used in cases of significant societal risks, such as natural disasters, epidemics, significant societal interest, etc. In these situations, the processing of personal data must be carried out in accordance with the document issued in 2020 by the European Data Protection Board (EDPB)[24] .

Consent of the data subject

The data subject's consent to the processing of personal data may provide a legal basis for the processing of the data, provided that it has been obtained in accordance with the provisions of Article 6(1)(a), and the conditions set out in Article 7 of the General Regulation (GDPR).

[24] https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-processing-personal-data-context-covid-19_en

A participant in product testing is a natural person - a data subject. If any personal data will be processed during the testing of the RiBAC project product, it is necessary to comply with the General Regulation (GDPR). However, it should be noted that the natural person who participates in the testing of the RiBAC product must provide 2 consents to the entity responsible for the testing: **(a)** consent to participate in the testing process, **(b)** consent to the processing of personal data.

> **Ad (a)** - Consent to participate in the testing process is not governed by the principles of the General Regulation (GDPR), but by the rules and principles established by general laws (e.g. Labour Code, Civil Code, laws on contract law, etc.) and ethical standards. It is therefore not possible to provide a comprehensive overview of the legal norms for this section, as it is derived from the general laws of the individual EU Member States.
>
> **Ad (b)** - consent to the processing of personal data in the testing process is subject to the principles set out in the General Data Protection Regulation (GDPR). The GDPR defines consent as "any **free, specific, informed and unambiguous** indication of the data subject's wishes, by which he or she gives his or her consent to the processing of his or her personal data, by means of a declaration or other manifest acknowledgement"[25] .

Consent is an essential aspect of the fundamental right to the protection of personal data as explicitly recognised by the Charter of Fundamental Rights of the European Union. [26]

Free consent has two complementary parts - (i) the **freedom to give consent** (consent is given without any form of coercion or compulsion) and (ii) **the freedom to maintain consent** (the data subject's ability to withdraw consent at any time). **It is** up to the data subject's free choice whether to consent and how long the consent will last. Any unacceptable coercion or influence on the data subject (which may take various forms of expression) preventing the data subject from exercising his or her free will renders the consent invalid. The controller must establish mechanisms and means to ensure that data subjects' consents are **clearly separate** and **distinct, that** they are documented and properly stored, and that the data subject can easily withdraw consent at any time. The General Regulation (GDPR) does not provide for the form of consent, so it can be given in writing (handwritten or electronic) or orally. However, the controller must be able to provide evidence of the consent given (e.g. to a supervisory authority). It must be a **dynamic process (activity)** on the part of the data subject. Silence, pre-ticked boxes or inaction cannot be considered as consent. It should be recalled that consent must apply to all processing activities carried out for the same purpose. If the processing has several purposes, consent must be given for each individual purpose.

Consent must be **specific, it** must be clear to which personal data and for what processing purposes it is provided. The data subject's declaration should also not give rise to any concern as to whether or not consent has been given by the declaration. Even where the data subject expresses his or her will in writing, processing may not be considered legitimate if the text of the consent is too vague or general, if the text does not contain details and specifications.

The General Data Protection Regulation (GDPR) reinforces the requirement that consent must be **informed, which means** that consent is invalid if the data subject has not been adequately informed of the relevant circumstances and context relating to the processing of personal data. Information about the circumstances of the processing must be unambiguous, understandable to the data subject, and given in readable (understandable) language. All the necessary information must be provided in

---

[25] Article 4(11) GDPR

[26] Article 8(2) of the EU Charter of Fundamental Rights states that personal data may be processed "on the basis of the consent of the person concerned or on any other legitimate ground provided for by law". https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A12016P%2FTXT

advance or at the time consent is sought and should cover the essential aspects of the processing which the consent is intended to legitimise. Therefore, the controller is obliged to inform the data subject at least about the following facts of the processing before requesting consent:

(i) the identity of the administrator,

(ii) the purpose of each of the processing operations for which consent is requested,

(iii) what data (types of data) will be collected and used,

(iv) the existence of a right to withdraw consent,

(v) the use of data for decisions based purely on automated processing, including profiling,

(vi) the potential risks of transferring data to third countries (where consent to transfer is involved), in the absence of a decision on an adequate level of data protection and appropriate safeguards.

Consent expresses the will of the data subject, identifies the person to whom it is addressed and can therefore be objectively **considered as an agreement**. The requirement to freely give consent is derived from a principle of civil law, and no circumstances must be created which would render consent invalid. Consent to the processing of data not necessary for the conclusion or performance of a contract cannot be taken as a mandatory factor in exchange for the performance of a contract or the provision of a service.

The template of recommended INFORMED CONSENT is attached in ANNEX I of this document.

Instructions for the RiBAC operator/application operator

Guidelines for users and operator on the Product RiBAC application

In the practical use of the final product of the RiBAC project, the end-user of the application is in the position of a "data controller" within the meaning of Article 4 of the GDPR. This means that this operator of the RiBAC product is fully responsible for the protection of the personal data of all individuals whose personal data will be processed. This responsibility is imposed on it by Article 5(2) of the GDPR and means that the operator (i.e. the controller) shall, taking into account the nature, scope, context and purposes of the processing and the different likely and different risks to the rights and freedoms of natural persons, put in place appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is carried out in accordance with the GDPR. The controller is obliged to take such measures to ensure that prevent:

- unauthorised or accidental access to personal data,
- unauthorised alteration of data,
- the destruction or loss of personal data,
- unauthorised transfers of personal data to third parties,
- other unauthorised processing of personal data, or
- any other misuse of personal data.

The application operator (administrator) is obliged to protect personal data not only from the consequences of human error (intentional or negligent), but also from natural events and the failure of the technology used to process personal data. The GDPR requires that data protection be included in the early stages of the design of information systems for the processing of personal data when using a Data Protection and Privacy by Design product.

Background

GDPR sets out the basic principles for the processing of personal data. Personal data must be processed in a lawful and transparent manner and a specific and legitimate purpose for processing the data must

be established. An important principle is so-called data minimisation, which requires that the scope of the data processed is proportionate, relevant and necessary in relation to the stated purpose of the processing. The fundamental principles also include the requirement that the personal data processed must be accurate and up-to-date in relation to the purpose of the processing. The operator of the application must also ensure that the retention period of personal data is limited to the time necessary to fulfil the stated purpose, and throughout this period the data must be protected by technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage. The operator of the RiBAC product application must also deal with the rights of data subjects granted to them by the GDPR.

During user applications of the RiBAC product in various application areas, personal information relating to natural persons may be processed. The RiBAC project draws the attention of the RiBAC product application operator to important obligations directly related to the use of the product in different application areas, which must be fulfilled in order to comply with the GDPR.

Principles and conditions for the processing of personal data (Article 5)

The principles and lawfulness of the processing of personal data are set out in Articles 5 and 6 of the GDPR. Personal data relating to natural persons (data subjects) may be subject to processing if the responsible user/operator (controller) of the RiBAC product application complies with the principles that the personal data processed:

a) are used only in a way that does not contravene the law and is fair and transparent to the persons concerned (data subjects). Individuals whose personal data will be processed by RiBAC must be made aware of the personal data being processed and the purpose of the processing. Under the transparency principle, clear information about the use of the RiBAC product should be made available to each individual concerned (whose personal data is the subject of the processing). This information also includes the identity of the operator of the application, including contact details, so that the individual (data subject) knows who to contact if he/she exercises his/her rights or needs more detailed information about the operation of the application (**Principle of lawfulness, fairness and transparency**);

b) the "**controller**" (the operator of the RiBAC product application) shall ensure that the product is used and applied only for the predetermined, written and legitimate purpose(s) (**Purpose Limitation Principle**);

c) are processed only to the extent necessary to fulfil the stated purpose of the RiBAC product (**Data Minimisation Principle**);

d) are retained only for the necessary period of time that corresponds to the need for the operation of the specific application. This period should be specified in the internal operating rules of the RiBAC product application operator and should be justified. The operator of the application should periodically verify that the personal data collected is still necessary, otherwise remove it from the application in question. (**Data Retention Limitation Principle**);

e) the data controller (i.e. the RiBAC app operator) takes responsibility for how personal data is processed and for compliance with all relevant principles set out in the GDPR (**the Responsibility Principle**).

The principle of accountability is one of the key principles of the new data protection legislation and requires the controller to put in place appropriate technical and organisational measures that both enable the assessment of the risks arising from the application of the RiBAC product to the possible violation of the rights and freedoms of natural persons, and also enable these risks to be eliminated or reduced. When implementing these measures, the controller (user/operator of the application) shall keep appropriate records and documentation to demonstrate compliance with the GDPR at any time.

(f) are lawful in accordance with the conditions set out in Article 6 of the General Data Protection Regulation (GDPR), which sets out 6 lawful principles for the processing of personal data (see 5.2).

(g) be proportionate and necessary for the legitimate purpose pursued. The user/operator must not use the RiBAC product in an application that allows covert tracking of individuals or for a purpose other than that for which the data processing was intended. The RiBAC product may not be used to collect and process personal data that is not necessary and required for the functionality of the application (purpose).

Lawfulness of the processing of personal data (Article 6)

If personal data of a natural person (data subject) will be processed in the application of the RiBAC product, then the controller (application operator) must ensure that the processing of the data in question is lawful, i.e. has an appropriate legal basis for such processing (the so-called legal title).

The lawfulness of the processing of personal data is regulated by Article 6 of the GDPR. It lists six legal grounds, but for RiBAC applications, the main grounds are the "consent" of the data subject, the "conclusion and performance of a contract" with the application operator, or the "legitimate interest" of the application operator providing the necessary services for the operation of the RiBAC product.

In practical applications of the RiBAC product, the lawfulness of the processing of personal data will be based mainly on the "consent" of the natural persons concerned or on the "legitimate interest" of the operator of the specific application. If the legitimate basis for the processing of personal data in a RiBAC product application is the 'legitimate interest' of the operator (within the meaning of Article 6(1)(f) of the GDPR), then the operator is required to perform a balancing test balancing its interest against the interest and fundamental rights and freedoms of the natural persons concerned (data subjects). If the interest and fundamental rights and freedoms of the natural persons outweigh the interests of the operator, then the 'legitimate interest' cannot be used as a legitimate basis for the processing of data in a RiBAC product application;

a) the elements of "**consent**" to the processing of personal data are set out in Article 7 of the GDPR. It is worth recalling here that consent must be given by the natural person concerned before processing begins and the operator of the application ('data controller') must be able to demonstrate consent throughout the processing of personal data. Consent must be freely given (without coercion or pressure on the person concerned), on the basis of prior information provided by the data controller (operator) (for the content of the information, see Articles 13 and 14 GDPR, see chapter 4.3.). If the processing of personal data in the RiBAC product application is based on the consent of the natural person, then it should be noted that such consent may be withdrawn at any time by that person. However, withdrawing consent could be problematic or risky for some applications (e.g. the application could no longer be used). In the event that such a risk would arise, the operator must choose another legal ground for processing the data.

(b) A suitable alternative could therefore be, for example, a "**contractual relationship**" with the natural person, declaring the necessity of processing the data for the duration of the contract. However, it should be noted here that only personal data which are necessary for the conclusion and performance of the contractual relationship may be requested under a 'contractual relationship'. Therefore, the contractual relationship cannot legitimise the processing of any other personal data.

c) However, another suitable alternative is the "**legitimate interest**" of the administrator (the operator of the application). In this case, however, the controller must assess whether the legitimate interest of the controller is outweighed by the interest of the individual in the protection of privacy and personal data. Performing this 'balancing test' is a necessary part of the application of this alternative (see Chapter 3.1).

Provision of information to natural persons (Articles 12, 13, 14)

When using (processing) personal data in practical applications of the RiBAC product, the relevant natural persons (data subjects) must be informed of such processing in an appropriate manner. The information should be provided to these individuals prior to the processing of the data and should include basic information about the RiBAC product and its use in real-life applications. The minimum scope of this information is set out in Articles 13 and 14 of the GDPR respectively. This information obligation of the operator of the RiBAC product application towards the natural person is part of the transparency of the entire data processing in the product application. Each individual must be told how and what data about him/her is processed in the RiBAC product application.

Rights of the natural person (data subject) (Articles 15 - 21)

The General Regulation (GDPR) gives individuals (data subjects) a number of rights that can be exercised against the data controller - the operator of the RiBAC product application. The communication of these rights should be part of the information provided to the natural person whose personal data is used (processed) in the application in question.

The operator of the RiBAC product application must take measures to ensure that the rights of natural persons exercised are dealt with. It should be noted that these rights under the GDPR are not absolute rights, which means that there may be a number of circumstances where the application operator will only partially comply with the applicant's asserted right or not at all. Requests to exercise the rights of natural persons (data subjects) must be dealt with individually, taking into account the specific circumstances of each individual RiBAC product application. For each right that the GDPR provides to an individual, certain limitations or exceptions to its exercise are indicated.

The General Regulation (GDPR) gives individuals (whose personal data is the subject of processing in a given application) a number of rights, but the following rights are particularly important for RiBAC applications:

Right of access to personal data[27]

The natural person (data subject) whose personal data is the subject of processing in the use (application) of the RiBAC product has the right to access the processed personal data and detailed information about the application of the RiBAC product. The scope of this information is enumerated in Article 15 of the GDPR and is similar to the information given to the data subject before the data collection by the RiBAC product application (see section 4.2.). According to this right, the data subject may obtain from the controller a copy of the processed data concerning only him/her (data on other persons cannot be disclosed). The right of access comprises three different components: a) Confirmation of whether or not personal data are processed; b) Access to those personal data; and c) Access to information about the processing (e.g. the purpose of the processing, the categories of data and recipients, the retention period of the data, the rights of the data subjects, as well as information about the algorithms used in the processing). If a request for access to personal data is made by a person whose data is not used in the RiBAC product application, the operator (controller) will only inform such applicant that his/her personal data is not used in the application. Such applicant shall not have the right to request detailed information about the RiBAC product application.

Right to rectification and erasure

[27] See also EDPB Guidelines no.01/2022 - https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf

If a natural person (data subject) whose personal data is processed in the RiBAC product application discovers that his or her personal data is incorrect, inaccurate or erroneous, he or she has the right to request the application operator to correct such data. The operator of the application should comply with this request without delay, in particular where the inaccurate data could have an adverse effect on the individual.

If the individual concerned (applicant) no longer uses the services of the RiBAC product application, he/she has the right to request the application operator to delete his/her personal data. The application operator shall comply with the request for deletion of data, in particular in cases where the personal data of the applicant for deletion is no longer required for the purposes of operating the application, or the applicant withdraws his/her consent or objects to his/her participation in the RiBAC product application and the operator has no other legitimate reason to continue to work with the personal data of the applicant (data subject), or it has been proven that the processing of the applicant's personal data is in breach of the law.

However, the operator of the RiBAC product application will not comply with a request to delete data from the application if the data is necessary for the establishment, exercise or defence of its legal claims (e.g. the data is necessary for the resolution of a security incident in the application).

Right to object

A natural person (data subject) may object to the processing of his or her personal data in the RiBAC product application in cases where the processing of the data is carried out on the basis of the performance of a task in the public interest or on the basis of a legitimate interest of the operator of the RiBAC product application. However, the natural person may not exercise this right against the operator if the processing of personal data in the application is carried out on the basis of the natural person's prior consent.

If the applicant exercises this right against the operator, the applicant's personal data must not be further processed, except where the operator of the application demonstrates its legitimate grounds for continuing to process the data and these grounds override the interests or rights and freedoms of the applicant (data subject).

Automated individual decision-making, including profiling (Article 22)

The RiBAC product application must not be designed to allow its use for the purpose of profiling individuals. Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or estimate, analyse or predict aspects of the individual's job performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Deliberate and standard protection of personal data (Articles 24 and 25)

As part of the responsibility principle, the operator of the RibAC product application is obliged to establish and implement appropriate technical and organisational measures to ensure that the use of the application complies with the General Regulation (GDPR). These measures should take into account the severity and likelihood of risks to the rights and freedoms of natural persons involved in the implementation phase of the application. The effectiveness and compliance of the measures taken should be regularly evaluated and, where appropriate, updated by the operator of the application.

At the time of deciding whether to use the RiBAC application, the operator of the application should assess all the likely and varying risks in relation to the nature, scope, context and purpose of the processing of personal data in the application, and, in light of these risks, take organisational, technical and personnel measures to implement and comply with all the principles of data protection as set out in Article 5 of the GDPR (principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, limitation of storage time, integrity and confidentiality, and accountability). In

making this assessment, the operator of the application shall also take into account the current state of technical means, the cost of implementing the application or other significant risks to the rights and freedoms of natural persons. The application operator shall ensure that, for each specific application of the RiBAC product, personal data is used by default only to the extent necessary.

Use of the services of a processor (Article 28)

A processor is an entity that carries out certain personal data processing activities instead of or on behalf of the controller (Articles 4 and 28 GDPR) with the personal data of natural persons using the services of other cooperating entities (processors), must ensure that these other entities are bound by obligations that ensure adequate protection of the personal data of natural persons throughout the RiBAC product application. The scope of the obligations is detailed in Article 28 of the GDPR and also in the EDPB document. These obligations include, in particular, the conclusion of a contractual relationship with the cooperating entity and the requirements related to ensuring the protection and security of the personal data processed.

The contractual relationship with the collaborating entity must address the position of each party (administrator vs. processor) and the resulting level of responsibility in operating the RiBAC product application. The contractual relationship should address the circumstances of the cooperation and the obligations of the parties, e.g. how individuals will be informed about the AI-related processing of their personal data and, if necessary, how their consent will be obtained or how they will be given the opportunity to object before their personal data is used to train AI algorithms (machine learning model).

Security and protection of personal data (Articles 32 to 35)

The operator of the RiBAC product application shall establish appropriate and effective technical and organisational measures prior to the commencement of routine operation of the application to ensure that the personal data of natural persons processed are reasonably and appropriately protected and secured against unauthorised access and use.

Prior to the start of routine operation of the application, the operator of the application shall assess the impact of the application on the privacy and data protection of the persons to be included in the application. In assessing this impact, the operator of the application shall also take into account the requirements set out by the European Data Protection Board (EDPB)[28] and the national supervisory authority for data protection[29] .

The recommendations provided in this Operator's Guide are not a complete list of the obligations that the RiBAC application operator must implement to ensure full compliance with applicable data protection legislation (GDPR). The RiBAC application operator must ensure compliance with other GDPR obligations that are not directly related to the application being implemented, but arise from their own status and activities as a controller or processor of personal data. We are referring here, for example, to the notification and reporting of personal data breaches (Articles 33 and 34 GDPR), the obligation to consult with a supervisory authority on the processing of data with a high risk to the rights and freedoms of natural persons (Article 36 GDPR), or the appointment of a data protection officer (Articles 37-39 GDPR), where the operator of the RiBAC product application must assess its own activities and the circumstances of the overall handling of personal data of natural persons (i.e. including activities not directly related to the RiBAC product application).

[28] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679; Artcle 29 Working Group, doc. WP 248, April 2017.

[29] Overview of supervisory authorities - see https://edpb.europa.eu/about-edpb/about-edpb/members_en

In the idle state, a welcome screen is displayed, which shows Figure 47.

The user is guided by informational messages on the display. The program awaits the user's arrival in front of the terminal's camera.

Once this happens, the presence of the person is detected and the system modules are activated to check the required items.

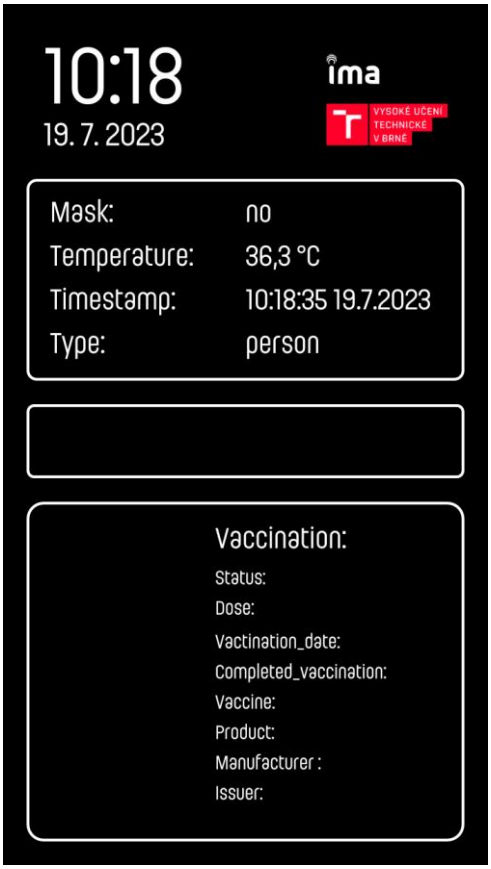


Figure 47: Application home screen

The terminal then displays a list of the required protective equipment that are required to be worn by the user (Figure 48).

Already detected protective equipment is marked with a green "pipe", those that have not yet been detected are marked with a red cross.

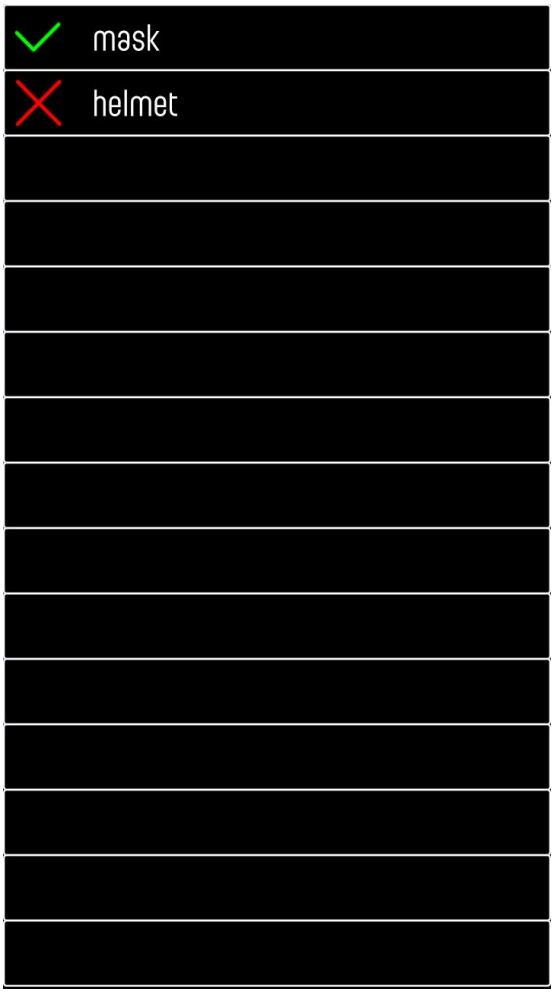


Figure 48: List of required protective equipment

Once all the required equipment has been detected, the terminal then returns back to the original screen.

The original screen then provides an overview of the available camera data (temperature measurement) and vaccine credential status.

In the middle of the screen, there is a message urging the user to attach their RFID card (or other identifier) for the access control module.

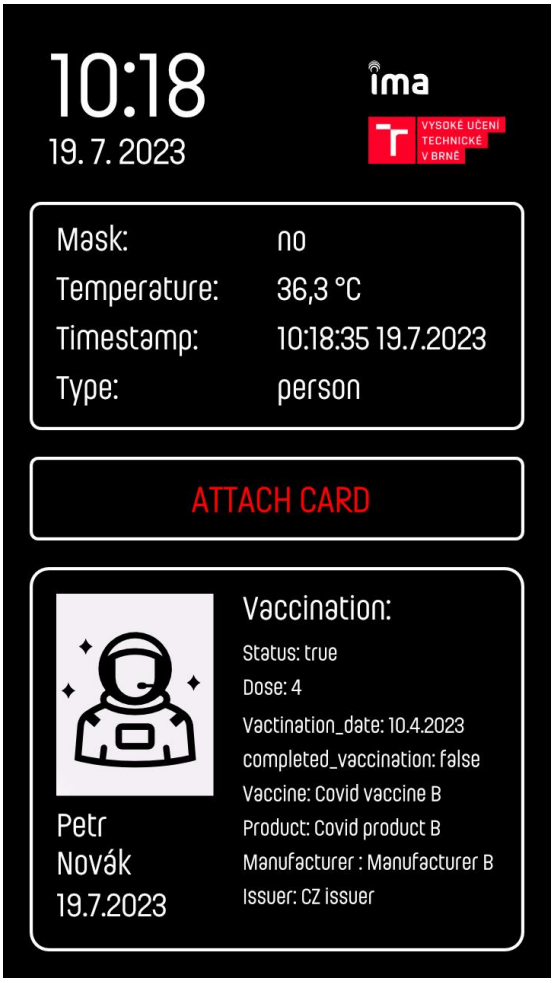


Figure 49: Terminal screen after successful detection of protective equipment

A 15-second timer is running in the background to monitor the activity of access control and other system modules. With each message, this timer is reset. If no information is received within this interval, the processing is terminated, and the user is shown an “access not granted” message (Figure 51).

If an RFID card has been attached, the access control module then checks if the user’s card contains corresponding access rights. If the user meets all the conditions, the user is then granted access. This event is then shown on the display (Figure 50).

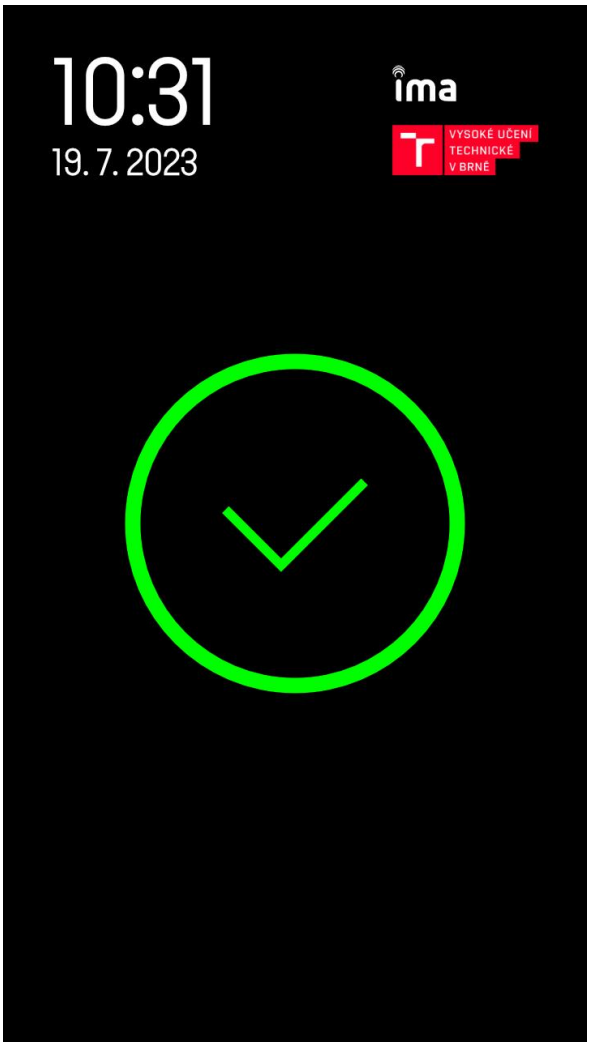


Figure 50: Access granted

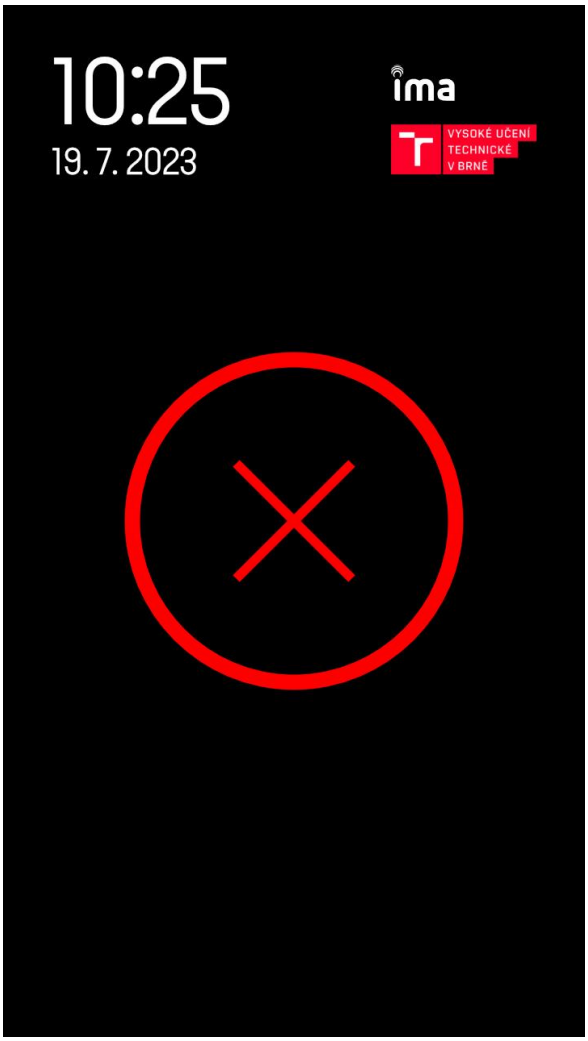


Figure 51: Access not granted

Example scenario flow

Following steps provide an overview of an example scenario flow:

Scenario – Basic functionality of RiBAC tool

Steps

- **Step 1:** User approaches the terminal.
- **Step 2:** User is guided in front of the terminal.
- **Step 3:** Camera module checks user's temperature, detects which protective tools are worn by the user and checks user's vaccination credential.
- **Step 4:** Successfully detected protective tools are shown on the terminal display.
- **Step 5:** After all required protective tools are detected, terminal returns to the original display screen.
- **Step 6:** Terminal screen shows an overview of user's temperature and vaccination status.
- **Step 7:** User is guided to attach their RFID card (identifier) to the reader (access control module).
- **Step 8:** Access control module checks if the user has corresponding access rights.
- **Step 9a:** If user has corresponding access rights and meets all required conditions, they are granted access.
- **Step 9b:** If the user does not have corresponding access rights and/or does not meet all required conditions, they are not granted access.
- **Step 10:** Display screen corresponding to the 9a/9b outcome is shown to the user.
- **Step 11:** In case of a positive outcome, the corresponding access point (door/turnstile/etc.) is opened.