



SUNRISE

Strategies and Technologies for **United** and **Resilient** Critical Infrastructures and Vital **S**ervices in Pandemic-Stricken **E**urope

D4.5 Access control tool and training guide V3

Document Identification			
Status	Final	Due Date	30/04/2025
Version	1.0	Submission Date	22/05/2025

Related WP	WP4	Document Reference	D4.5
Related Deliverable(s)	D4.1, D4.2, D4.3, D3.1, D3.2, D3.3	Dissemination Level (*)	PU
Lead Participant	IMA	Lead Author	Tomas Trpisovsky
Contributors	AIT, UKC, INS, UoW, SZ, CAF, TS	Reviewers	ICS
			UoW

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

Disclaimer for Deliverables with dissemination level PUBLIC

This document is issued within the frame and for the purpose of the SUNRISE project. This project has received funding from the European Union's Horizon Europe Programme under Grant Agreement No.101073821. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

The dissemination of this document reflects only the author's view, and the European Commission is not responsible for any use that may be made of the information it contains. **This deliverable is subject to final acceptance by the European Commission.**

This document and its content are the property of the SUNRISE Consortium. The content of all or parts of this document can be used and distributed provided that the SUNRISE project and the document are properly referenced.

Each SUNRISE Partner may use this document in conformity with the SUNRISE Consortium Grant Agreement provisions.

(*) Dissemination level: **(PU)** Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page). **(SEN)** Sensitive, limited under the conditions of the Grant Agreement. **(Classified EU-R)** EU RESTRICTED under the Commission Decision No2015/444. **(Classified EU-C)** EU CONFIDENTIAL under the Commission Decision No2015/444. **(Classified EU-S)** EU SECRET under the Commission Decision No2015/444.

Document Information

List of Contributors	
Name	Partner
Jan Orlicky	IMA
Tomas Trpisovsky	IMA
Stephan Krenn	AIT
Gilda De Marco	INS
Matjaž Tavčar	UKC

Document History			
Version	Date	Change editors	Changes
0.1	24/03/2025	J. Orlicky (IMA)	First draft with adaptations
0.2	31/03/2025	J. Orlicky (IMA)	Updates sections in Chapter 1
0.3	03/04/2025	J. Orlicky (IMA)	New sections in Chapter 3, Chapter 4
0.4	14/04/2025	T. Trpisovsky (IMA)	Initial overall review
0.5	28/04/2025	T. Trpisovsky (IMA)	Contribution of INS & UKC incorporated
0.6	07/05/2025	J. Orlicky (IMA)	Prefinal updates before internal review
0.7	13/05/2025	D.Slavik, T.Trpisovsky (IMA)	Final version for internal review
0.8	20/05/2025	J. Orlicky (IMA)	Final version with addressed comments from reviewers
0.9	21/05/2025	Juan Alonso (ATS)	Quality Assessment
1.0	22/05/2025	Aljosa Pasic (ATS)	Final version

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Tomas Trpisovsky (IMA)	20/05/2025
Quality Manager	Juan Alonso (ATS)	21/05/2025
Project Coordinator	Aljosa Pasic (ATS)	22/05/2025

Table of Contents

Document Information.....	2
Table of Contents	3
List of Tables.....	6
List of Figures.....	7
List of Acronyms	9
Executive Summary	10
1 Introduction.....	11
1.1 Purpose of the document	11
1.2 Relation to other project work.....	12
1.3 Differences Between D4.3 and D4.5	13
1.4 Structure of the document	14
1.5 Glossary adopted in this document	14
2 Risk-Based Access Control Tool	17
2.1 General Architecture.....	17
2.1.1 Terminal hardware solution	17
2.1.2 Computing module.....	19
2.1.3 Motherboard	19
2.1.4 Power supply block.....	19
2.1.5 Real Time Circuit.....	20
2.1.6 EEPROM memory	20
2.1.7 USB port control	20
2.1.8 RFID card reader	20
2.1.9 Touch screen display	20
2.1.10 Inputs, outputs and peripherals	21
2.2 Tool Modules Description	21
2.2.1 Main loop	21
2.2.2 Terminal user interface	22
2.2.3 Communication Interface - API	23
2.2.4 Access Control Module.....	23
2.2.5 Protective Tools Detection Module.....	24
2.2.6 Temperature Detection Module	25
2.2.7 Vaccine Credential Detection Module	27
2.2.8 Privacy-Preserving European Digital Covid Certificates	29
2.3 Deployment.....	34
2.3.1 Initializing and configuring the terminal	34

2.3.2	Graphical interface	35
2.3.3	Power failure protection	36
2.3.4	Communication interface	36
2.3.5	Access rights	36
2.3.6	Mechanical solution	36
3	RiBAC Tool Validation in Lab Conditions	39
3.1	Lab Setup.....	39
3.2	Tool Modules Validation	40
3.2.1	Protective Tools Detection Module.....	41
3.2.2	Temperature Detection Module	46
3.2.3	Vaccine Credential Detection Module	50
3.2.4	Privacy-Preserving European Digital Covid Certificates	52
3.2.5	Prototypical Implementation	54
3.3	Integrated RiBAC Validation.....	56
3.3.1	Extended testing.....	58
3.4	Pilot Deployment Results and Feedback.....	59
3.4.1	Pilot Deployment Overview	59
3.4.2	Key Findings from First Round Pilots.....	60
3.4.3	Pilot-Driven Improvements	60
4	Pilot trials execution (feasibility analysis).....	62
4.1	Description of piloting activities	62
4.1.1	Pilot sites overview.....	62
4.1.2	Czech pilots.....	62
4.1.3	Italian cluster	64
4.1.4	Slovenian cluster	66
4.2	Description of End-Users' Roles.....	68
4.3	Second Pilot Phase Status	69
4.3.1	Enhancements for Second Pilot Phase	69
4.3.2	Partner Selections for Pilot Implementations	69
4.3.3	Objectives of the Second Pilot Phase	70
4.3.4	Current Status and Preparation	70
5	Conclusions.....	71
	References.....	72
	Annex I - Informed consent of pilot participants	75
	Annex II – Privacy policy	76
	Privacy Policy for Product Testing	76
	Informed consent of participants in product testing	76

Annex III – RiBAC Tool User guide for CI operators.....	80
RiBAC Terminal	80
General Schema	80
Technical Composition	81
Technical components:	81
RGB camera.....	82
Thermal (IR) camera.....	82
Touch screen terminal	82
Function description	83
Basic function	83
Features for the pandemic period	83
Installation Guide.....	84
Terminal Design and Measures.....	84
Positioning of the Terminal.....	85
Connections	85
Commissioning	85
Terminal Configuration.....	85
Pilot installation	89
Tested functions.....	89
Testing procedures.....	89
Time schedule of tests	89
Tests protocols	89
Troubleshooting instructions a fault or problem in operation.....	90
Remote Support.....	90
Terminal Interface User Guide	91
Example scenario flow	95

List of Tables

<i>Table 1: Differences between D4.3 [42] and D4.5 summary.....</i>	<i>13</i>
<i>Table 2: Effect of the distance of the person from the detection unit on the detection sensitivity</i>	<i>42</i>
<i>Table 3: Results of respiratory protection detection testing.....</i>	<i>44</i>
<i>Table 4: Test results of automated temperature measurement of persons.....</i>	<i>47</i>
<i>Table 5: Results of automated temperature measurement of people with a focus on the presence of glasses.</i>	<i>49</i>
<i>Table 6: Effect of the number of detected attributes on communication</i>	<i>51</i>
<i>Table 7: Total clearance time of the detection frame</i>	<i>57</i>
<i>Table 8: Pilot site overview.....</i>	<i>62</i>
<i>Table 9: End user profiles of the RiBAC Tool.....</i>	<i>68</i>

List of Figures

Figure 1: X block diagram of the terminal.....	18
Figure 2: Internal layout of terminal hardware components	18
Figure 3: Internal layout of terminal hardware components	19
Figure 4: Wiring the terminal block on the back of the terminal	21
Figure 5: Wiring diagram of the level converter from 5V Wiegand to 3.3V for the calculation module	21
Figure 6: RiBAC tool modules	22
Figure 7: RFID reader main board	23
Figure 8: Antenna board.....	24
Figure 9: Camera module	24
Figure 10: Neural Compute Stick 2	25
Figure 11: Development sample of the AI profile temperature measurement module	26
Figure 12: External view of a working sample of the temperature measurement module.....	26
Figure 13: Internal layout of the functional sample of the temperature measurement module	27
Figure 14: Block diagram of the reference target	27
Figure 15: CovidPass verification system.....	28
Figure 16: Mobile phone CovidPass application.....	29
Figure 17: The LINDDUN Multistep approach	30
Figure 18 : Data flow diagram of the EUDCC [21].....	31
Figure 19 : Detailed DFD for credential verification [21].....	32
Figure 20: Screenshot from the application GUI builder	35
Figure 21: Screenshots from the terminal - Default screen with reasons, permissions, rejections.....	35
Figure 22: Contents of delivery of the terminal with mounting frame.....	37
Figure 23: View of the bottom of the terminal with the screws ready for mounting.....	37
Figure 24: Slot in terminal cover for display, plexiglass with black frame	38
Figure 25: Terminal from the back, mounting frame, mounted frame on the terminal	38
Figure 26: The test setup	40
Figure 27: The test setup with user	41
Figure 28: Example of surgical drapes used for airway protection detection testing	41
Figure 29: Measurement of the detector sensitivity as a function of the distance of the object from the frame.	44
Figure 30: Test results of the task of detecting the use of respiratory protection.	45
Figure 31: Sample of the respiratory protection detection testing process.	46
Figure 32: TrueLife Q7 non-contact thermometer for measuring human skin temperature.	46
Figure 33: Comparison of body temperature measured with a non-contact thermometer and tested thermocamera.....	48
Figure 34: Illustration of the effect of wearing glasses on the measurement of emitted thermal radiation, a) face without glasses, b) face with glasses.....	49
Figure 35: Comparison of body temperature measured with a non-contact thermometer and SUNRISE with correction of the resulting temperature.....	50
Figure 36: Effect of the number of detected attributes on communication.....	51
Figure 37: Information on the display.	51
Figure 38 : Running times of necessary extensions of the OLYMPUS attribute-based credential library compared to a basic reference policy (BRP)	52
Figure 39: High-level flow of privacy-preserving biometric matching.....	53
Figure 40: Credential issuance.....	54
Figure 41: Fetching a credential.....	54
Figure 42: Initializing a presentation.....	55

Figure 43: Validating a presentation.....	55
Figure 44: The test setup with turnstile.....	56
Figure 45: Cumulative histogram of the total clearance time of the co-located detection frame.....	57
Figure 46: Example of experimental testing.....	58
Figure 47: Vaccine credential verification	59
Figure 48: Piloting Schedule for Czech pilots.....	62
Figure 49: Military University Hospital in Prague.....	63
Figure 50: Rectorate of the CTU in Prague	63
Figure 51 : Piloting schedule of the Italian cluster	64
Figure 52: Insiel HQ entrance	65
Figure 53: Insiel HQ - turnstile	65
Figure 54 : Piloting schedule for Slovenian cluster.....	66
Figure 55: UKC Ljubljana Old City Children Hospital.....	67
Figure 56: Main railway station in Ljubljana.....	67
Figure 57: TS offices in Cigaletova street	68
Figure 58: The RiBAC terminal.....	84
Figure 59 : Measurements of the RiBAC terminal (front and side view)	84
Figure 60: Different positions of the RiBAC terminal.....	85
Figure 61 : Password entry (default values are described at the end of the paragraph).....	86
Figure 62 : Terminal configuration.....	87
Figure 63: Static IP address	88
Figure 64: Uploading cards.....	88
Figure 65: Application home screen	91
Figure 66: List of required protective equipment	92
Figure 67: Terminal screen after successful detection of protective equipment.....	93
Figure 68: Access granted	94
Figure 69: Access not granted	94

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
IAM	Identity and Access Management
IDM	Identity Management
IPS LCD	In-plane Switching Liquid Crystal Display
IR camera	Infrared camera
ML	Machine Learning
NFC	Near Field Communication
NN	Neural Network
PCB	Printed Circuit Board
PMOS	P-type Metal-Oxide Semiconductor
PPE	Personal Protective Equipment
RC circuit	Resistor-capacitor Circuit
RGB camera	Red-Green-Blue camera
RiBAC	Risk-Based Access Control
RiBEC	Risk-Based Exit 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 four technological tools developed within the SUNRISE project. It provides a comprehensive solution for augmenting access control systems in critical infrastructure sites with pandemic-specific risk factors to enhance security and resilience during health emergencies. This final version of the RiBAC tool has reached Technology Readiness Level 7 (TRL7), representing a system prototype demonstration in an operational environment, and offers a production-ready solution for CI operators.

The RiBAC tool employs a modular approach to integrate multiple risk factors into access control decisions, including the detection of protective equipment (such as face masks), body temperature measurement, and verification of vaccination credentials. Throughout its development, the tool has placed special emphasis on privacy protection, GDPR compliance, security, scalability, and economic efficiency, making it suitable for deployment across diverse critical infrastructure sectors.

The concept of RiBAC as a tool for strengthening critical infrastructure security was first presented in D4.1 [40] and subsequently developed through D4.2 [41] and D4.3 [42]. This final deliverable (D4.5) documents the culmination of this development journey, presenting the fully operational RiBAC tool that has been refined based on extensive testing and real-world deployment feedback.

The development of the RiBAC tool has been guided by requirements and specifications from WP3 deliverables (D3.1-D3.3), which provided the technical foundations for its architecture. The tool aligns with the SUNRISE strategy developed in WP2, focusing on non-pharmaceutical interventions during pandemics. In turn, insights from RiBAC implementation have provided feedback to WP2 regarding essential worker availability and legacy system integration challenges, contributing to the project's holistic approach to critical infrastructure resilience.

The field validation of the RiBAC tool has been conducted through a comprehensive pilot program spanning multiple countries (Czech Republic, Slovenia, and Italy) and critical infrastructure sectors (healthcare, transportation, digital services, and industry). The first round of pilot deployments, documented in D4.4 [43], provided valuable insights that directly informed the advancement to TRL7. These pilots demonstrated the tool's flexibility, reliability, and user acceptance across different operational environments, with 99% of users expressing trust in the solution.

Based on the feedback from the first pilot phase, several key improvements have been implemented, including enhanced environmental adaptability, user experience refinements, and improved deployment and maintenance tools. These enhancements address the challenges identified during real-world deployment and strengthen the tool's readiness for production use.

A second pilot phase is now being prepared to validate these improvements and further demonstrate the TRL7 readiness of the system. This phase will focus on testing enhanced features including offline operation with event generation capabilities and specialized exit control functionality (RiBEC), which have been selected by the CI partners based on their specific operational needs.

This deliverable provides a comprehensive documentation of the RiBAC tool, including its architecture, implementation details, validation results, and deployment guidelines. It serves as a definitive guide for CI operators on implementing, configuring, and maintaining the RiBAC system in their facilities, ensuring they can effectively enhance their resilience against future pandemics while maintaining operational continuity and regulatory compliance.

The RiBAC tool represents a significant advancement in critical infrastructure protection, offering a balanced approach to security, privacy, and operational efficiency. Its ability to seamlessly transition between normal and pandemic operational modes provides CI operators with a valuable tool for enhancing their preparedness and response capabilities in the face of evolving health threats.

1 Introduction

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.

During the Covid-19 pandemic, different approaches for risk minimization were implemented, including protective wear requirements (such as face masks) and mandatory temperature checks at entrance gates. However, many of these solutions were deployed hastily without thorough consideration of key requirements related to data protection, privacy, efficiency, scalability, and contactless operation. The need for integrated solutions that address these concerns comprehensively has become increasingly apparent.

The SUNRISE project's Risk-based Access Control (RiBAC) tool was developed to address these challenges. Now in its final iteration (TRL7), the RiBAC tool provides a comprehensive architecture and software component that incorporates scalability, privacy protection, and compatibility with GDPR requirements. The tool offers a modular approach to augment existing access control systems with pandemic-specific decision factors, such as the presence of protective equipment, body temperature readings, and vaccination status verification.

Building on the foundations established in previous deliverables (D4.1[40], D4.2[41], and D4.3 [42]), this final RiBAC solution represents the culmination of three years of development, testing, and refinement. It incorporates feedback from extensive pilot deployments documented in D4.4 "Access control pilot report V1" [43] and lessons learned from real-world implementation across multiple critical infrastructure sectors, including healthcare, transportation, digital services, and water utilities.

The RiBAC tool is production-ready, offering critical infrastructure operators a resilient, adaptable, and privacy-preserving access control solution that can function effectively during both normal operations and pandemic situations. This capability to seamlessly transition between operational modes without significant reconfiguration or additional investment represents a key innovation and commercial advantage of the system.

The developed RiBAC solution is partially based on the results of the SACON [1], CyberSec4Europe [2] and OLYMPUS[3] European projects.

1.1 Purpose of the document

The SUNRISE project aims to enhance the resilience of essential services within Europe's Critical Infrastructure (CI) by equipping CI operators and authorities with the necessary tools to handle pandemic situations. The main objective is "to ensure greater availability, reliability, and continuity of critical infrastructures in Europe, including transport, energy, water, and healthcare." To achieve this, the project has developed a comprehensive strategy and a set of tools, including the risk-based access control tool developed within WP4.

The main purpose of D4.5, "Access control tool and training guide V3," is to provide comprehensive documentation of the final version of the RiBAC tool at Technology Readiness Level 7 (TRL7). This deliverable serves as the definitive guide for CI operators on implementing, configuring, and maintaining the RiBAC system in their facilities. It consolidates all the refinements, improvements, and lessons learned throughout the project lifecycle, particularly incorporating feedback from the pilot deployments documented in D4.4 [43].

Specifically, this document:

1. Presents the final architecture and implementation details of the RiBAC tool
2. Documents the transition from TRL6 to TRL7, highlighting the key improvements made
3. Summarizes pilot feedback and provides pilot status update

4. Includes the necessary training materials for system administrators and end-users

This deliverable represents the culmination of three years of development, testing, and refinement within the SUNRISE project. It offers a production-ready solution that CI operators can implement to enhance their resilience against future pandemics while ensuring operational continuity, regulatory compliance, and protection of personal data.

The target audience for this document includes end-users for tools developed in WP4. In the context of WP4, definition of end-users refers to the primary operators of the tool, consisting of personnel from diverse Critical Infrastructures (CI) across various sectors (including water, health, transportation and digital services). More details on user roles and profiles can be found in Section 4.2.

1.2 Relation to other project work

Deliverable D4.5, "Access control tool and training guide V3," represents the fifth deliverable 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
- ▶ T4.5 Demonstration, training, evaluation, and validation.

Like all other tools developed within WP5-WP7 of SUNRISE (whose final outcomes are documented in D5.5, D6.5, and D7.5, respectively), WP4 is interconnected with collaboration (WP1), strategy (WP2), and design (WP3), as well as dissemination and exploitation (WP8), ethical requirements (WP10) and management (WP9).

From a technical perspective, the primary connection is to WP3, which gathers requirements and serves as a hub for the development of all the tools in the respective work packages.

The development of the RiBAC tool has also been guided by the SUNRISE strategy developed within WP2, particularly focusing on non-pharmaceutical intervention (NPI) related risks during pandemic situations. On the other hand, WP4 and the practical implementation and piloting of the RiBAC tool has generated valuable insights that will feed back into the SUNRISE strategy (to be included in the next WP2 deliverable). These insights address critical resource management aspects including:

- ▶ Essential worker availability during pandemic situations
- ▶ Training requirements for new access control technologies
- ▶ Operational constraints related to integration with legacy systems

This document builds directly upon previous deliverables:

- ▶ **D4.1 "Access control conceptualization"** [40] provided the foundational architecture for the RiBAC tool, its requirements, and security and privacy guarantee along with an initial introduction to the pilots.
- ▶ **D4.2 "Access control tool and training guide V1"** [41] presented the initial implementation of the RiBAC components at TRL5, focusing on the core functionalities and proof-of-concept demonstrations.
- ▶ **D4.3 "Access control tool and training guide V2"** [42] documented the enhancements made to reach TRL6, including the integration of privacy-preserving technologies and preparations for pilot deployments.
- ▶ **D4.4 "Access control pilot report V1"** [43] described the outcomes of the extensive pilot deployments across multiple CI sectors and provided valuable feedback that helped shape the final version of the RiBAC tool documented in this deliverable.

Furthermore, this document is closely related to the outcomes of:

- **D3.3 "Final technical specifications and designs"** which provided the technical specifications that guided the development of the final version of the RiBAC tool.
- **D8.4 "Exploitation and Standardization Plan V2"** and **D8.7 "Business Models and Sustainability Strategy"** which outline the commercial exploitation plan for the RiBAC tool beyond the SUNRISE project.

1.3 Differences Between D4.3 and D4.5

Deliverable D4.5 is the final version of the RiBAC tool documentation, building upon the previous versions (D4.2[41] and D4.3[42]). The purpose of this document is to report on the upgrades performed since the delivery of D4.3[42] and to provide a comprehensive guide for the production-ready TRL7 version of the tool. To support the reader, the following table outlines the differences between D4.3[42] and this deliverable.

Table 1: Differences between D4.3 [42] and D4.5 summary

Section in D4.5	Section in D4.3 [42]	Differences
Executive Summary	Executive Summary	Updated
1 Introduction	1 Introduction	Updated
1.1 Purpose of the document	1.1 Purpose of the document	Updated
1.2 Relation to other project work	1.2 Relation to other project work	Updated
1.3 Relation between D4.3 [42] and D4.2 [41]	1.3 Relation between D4.3 [42] and D4.2 [41]	Updated
1.4 Glossary adopted in this document	1.4 Glossary adopted in this document	Updated
1.5 Structure of the document	1.3 Structure of the document	Updated
2 Risk-Based Access Control Tool	2 Risk-Based Access Control Tool	Unchanged
2.1 General Architecture	2.1 General Architecture	Unchanged
2.2 Tool Modules Description	2.2 Tool Modules Description	Minor updates
2.3 Deployment	2.3 Deployment	Unchanged
3 RiBAC Tool Validation in Lab Conditions	3 RiBAC Tool Validation in Lab Conditions	Unchanged
3.1 Risk assessment	3.1 Risk assessment	Unchanged
3.2 Tool Modules Validation	3.2 Tool Modules Validation	Updated
3.3 Integrated RiBAC Validation	3.3 Integrated RiBAC Validation	Unchanged
3.4 Pilot Deployment Results and Feedback		New section
4 Pilot trials execution (feasibility analysis)	4 Pilot trials execution (feasibility analysis)	<i>No text in subsection</i>
4.1 Description of piloting activities	4.1 Description of piloting activities	Minor updates
4.2 Description of End-Users' Roles	4.2 Description of piloting activities	Unchanged
4.3 Second Pilot Phase Status		New section
5 Conclusions	5 Conclusions	Updated

Section in D4.5	Section in D4.3 [42]	Differences
6 References		Unchanged
Annex I – Informed consent of pilot participants	Annex I – Informed consent of pilot participants	Unchanged
Annex II – Privacy policy	Annex II – Privacy policy	Unchanged
Privacy Policy for Product Testing	Privacy Policy for Product Testing	Unchanged
Informed consent of participants in product testing	Informed consent of participants in product testing	Unchanged
Annex III – RiBAC Tool User guide for CI operators	Annex III – RiBAC Tool User guide for CI operators	Unchanged

1.4 Structure of the document

This document is structured in 5 major chapters and 3 annexes.

- ▶ **Chapter 1** presents the purpose of this deliverable (D4.5), 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, highlighting the improvements to achieve TRL7.
- ▶ **Chapter 3** presents the comprehensive evaluation results of the RiBAC tool, including both laboratory testing real-world deployment data with feedback from the pilot trials documented in D4.4 [43].
- ▶ **Chapter 4** provides details about the implementation of the RiBAC tool in various CI environments, including the status of the second piloting phase.
- ▶ **Chapter 5** summarizes the main achievements of the RiBAC tool development within the SUNRISE project and outlines potential future developments.
- ▶ **Annex I** provides templates for informed consent and data processing agreements for organizations implementing the RiBAC tool.
- ▶ **Annex II** contains detailed privacy policies and compliance documentation for the RiBAC tool, ensuring alignment with GDPR and other relevant regulations.
- ▶ **Annex III** includes the comprehensive user guide for the RiBAC tool, with separate sections tailored to different user roles (system administrators, security personnel, and end users).

1.5 Glossary adopted in this document

Critical Infrastructure (CI): Power distribution networks, transportation networks, and information and communication systems are all examples of critical infrastructure. The defence of critical assets is indeed essential for ensuring the safety and well-being of the European Union (EU) and its citizens. The electrical grid, transportation systems, and information and communication networks are key examples of what is known as "Critical Infrastructures". These infrastructures are essential to maintain in order to ensure that vital societal functions continue to operate smoothly. Natural disasters, acts of terrorism, and criminal activities all have the potential to cause damage to or destroy essential infrastructure, which may have serious repercussions for both the safety of EU residents and the complete EU.

Critical Assets (CAs): Are the significant resources that support both the social and business parts of an economy. If some of these assets fail, it will bring significant issues for business continuity. This does not mean that the likelihood of failing is high. For planning purposes, each business or organization must identify its critical assets and know the corresponding information about them.

Use Case: A description of the interaction between an actor (e.g. a user or system component) and the system, outlining the sequence of actions or steps taken to achieve a specific goal. It represents a technical or functional task relevant to a particular operational need.

Scenario: Scenarios provide narrative or technical framing for a use case, with two types:

- ▶ **Contextual Scenario:** A broader, real-world context such as a pandemic or multi-hazard threat environment that may influence multiple systems.
- ▶ **Use Case Scenario:** A focused variant or narrative path within a specific use case, detailing alternative technical or procedural flows.

Pilot: Real-world validation phase of the project, built on defined use cases and scenarios. It involves the deployment and evaluation of solutions under realistic conditions.

WP-Specific Terminology

- ▶ **Authentication and authorization:** These are two vital information security processes that administrators use to protect systems and information. Authentication verifies the identity of a user or service, and authorization determines their access rights.
- ▶ **End-User:** The primary operator of a tool, consisting of personnel from diverse Critical Infrastructures (CI) across various sectors (e.g. energy, water, health, transportation, digital services).
- ▶ **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” [5].
- ▶ **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 an EU member state. As for countries other 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 [6].

- ▶ **Identity management (IDM):** also called **identity and access management (IAM)** is the organizational and technical processes for first registering and authorizing access rights in the configuration phase, and then in the operation phase for identifying, authenticating and controlling individuals or groups of people to have access to applications, systems or networks based on previously authorized access rights. Identity management (IDM) is the task of controlling information about users on computers. Such information includes information that authenticates the identity of a user, and information that describes data and actions they are authorized to access and/or perform. It also includes the management of descriptive information about the user and how and by whom that information can be accessed and modified. In addition to users, managed entities typically include hardware and network resources and even applications.
- ▶ **Risk-Based Access Control (RiBAC):** An approach to access control that dynamically adjusts access permissions based on risk factors associated with the access request, the requesting entity, and the environmental context. In the context of the SUNRISE project, this includes pandemic-specific risk factors such as body temperature, wearing of protective equipment, and vaccination status.
- ▶ **Technology Readiness Level (TRL):** A method for estimating the maturity of technologies during the acquisition phase of a program. The RiBAC tool has progressed from TRL5 (validation in relevant

environment) through TRL6 (demonstration in relevant environment) to TRL7 (system prototype demonstration in operational environment).

2 Risk-Based Access Control Tool

The following section presents a general architecture for the RiBAC tool as designed in D4.1 [40]. Furthermore, a detailed description of all tool modules is given.

On a high level, the presented result is a graphical touch-screen terminal equipped with an RFID card reader for interaction with supervised persons. The terminal is also equipped with several 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.

Since the first iteration of this deliverable, i.e., D4.2 [41], all modules have been carefully screened, e.g., to ensure that no superior components are available for a lower price or whether more efficient solutions regarding sensors, etc., are available. The stability and functionality of the current RiBAC tool will be demonstrated in May and June 2024, expecting a TRL of 6 at the end of the trial phase.

The RiBAC terminal was implemented with partial use of the results of the ADOPSIO [7] project co-financed with the contribution of the Ministry of the Interior of the Czech Republic.

Along with the development of RiBAC, IMA is also considering measures to strengthen its subsequent commercialization, which will be further detailed in D8.4 and D8.7. The idea is to ensure that the tool can be used also in normal mode without an ongoing pandemic but can easily be switched to pandemic mode with low personnel overhead and additional costs. Other examples of such added value in normal mode is for example the use of RiBAC as a Risk based EXIT Control terminal. Another challenging function might be the locker management enabling the use of smart lockers at the CI entrance receptions.

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.

2.1.1 Terminal hardware solution

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 [8][9].

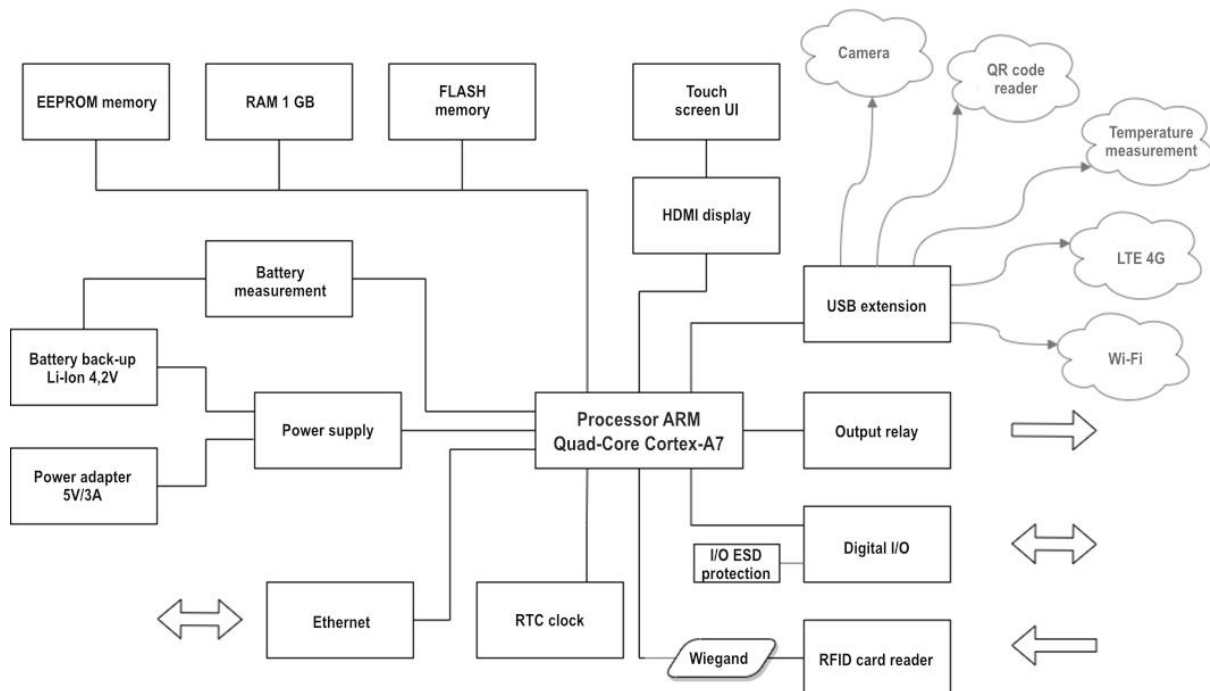


Figure 1: X block diagram of the terminal



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 labelled "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.

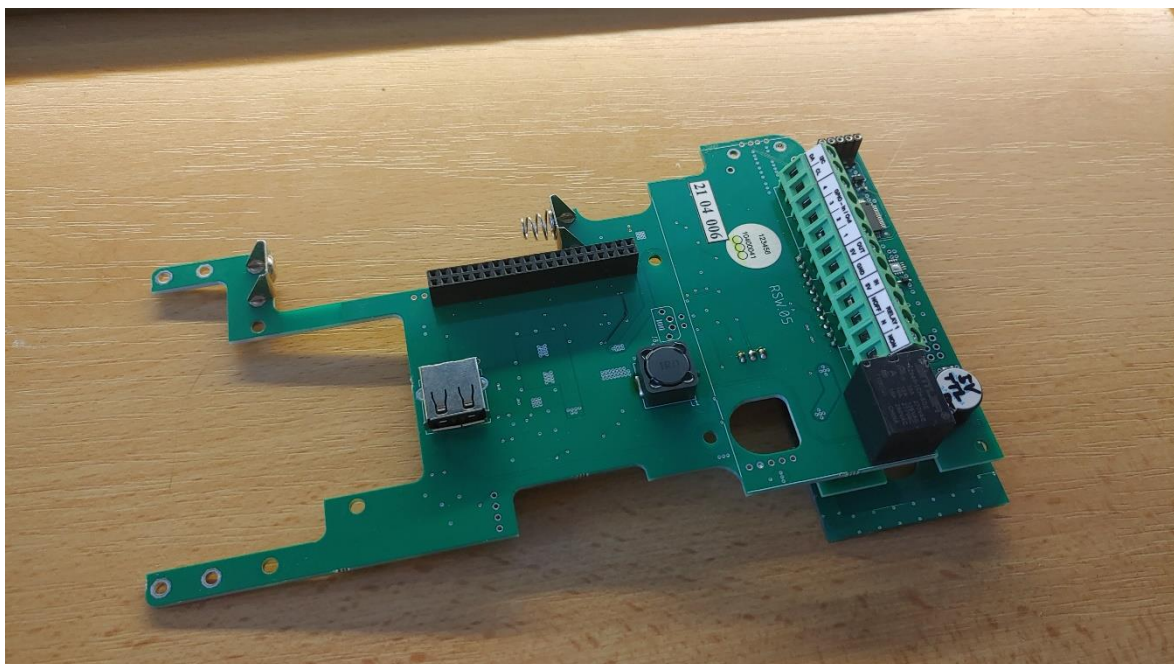


Figure 3: Internal layout of terminal hardware components

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.

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 from the adapter). The voltage converter can maintain a 5V/2.8A output as long as there is at least 2.5V 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 can deliver 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 labelled "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 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.

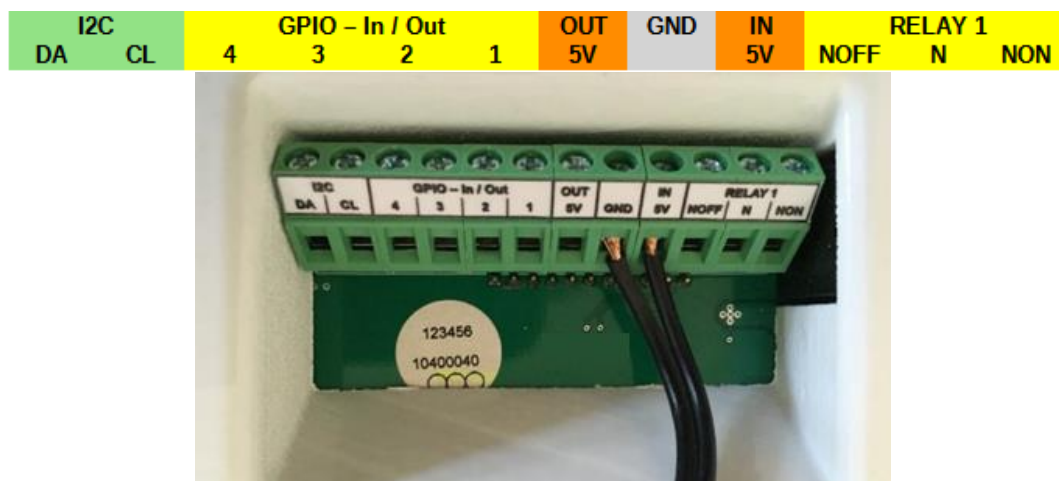


Figure 4: Wiring the terminal block on the back of the terminal

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

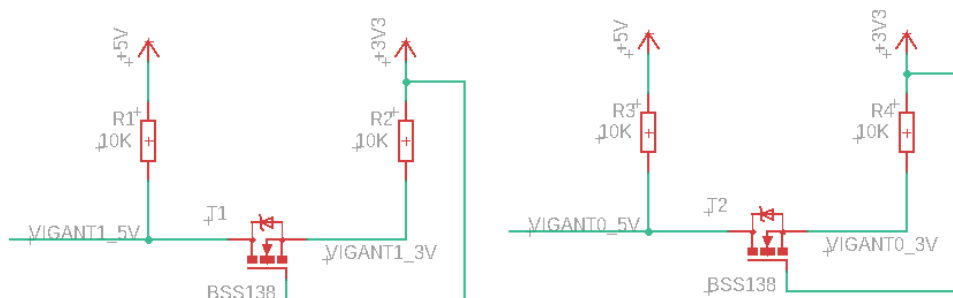


Figure 5: Wiring diagram of the level converter from 5V Wiegand to 3.3V for the calculation module

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.

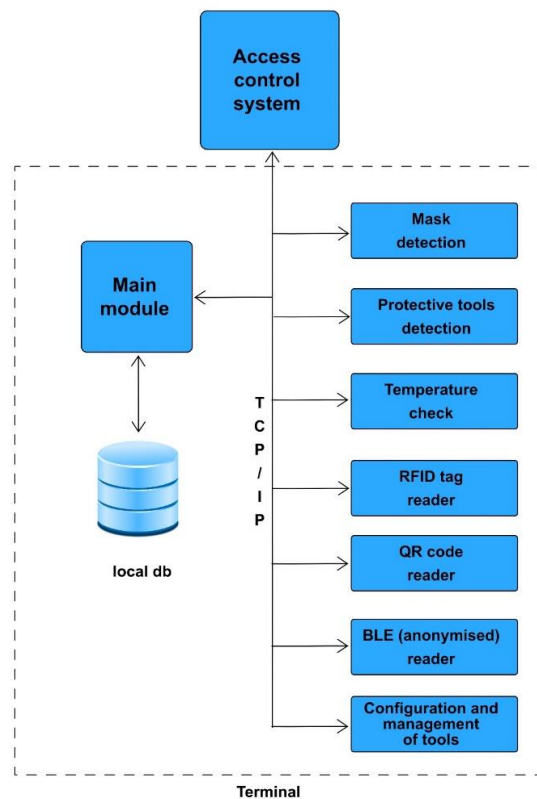


Figure 6: RiBAC tool modules

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 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 [10]. The RF interface is made by LEGIC chip SM6300[11] . This configuration can operate with cards according to standards ISO 14443 and ISO 15693as well as with mobile phones with Bluetooth 4.0 and above.

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

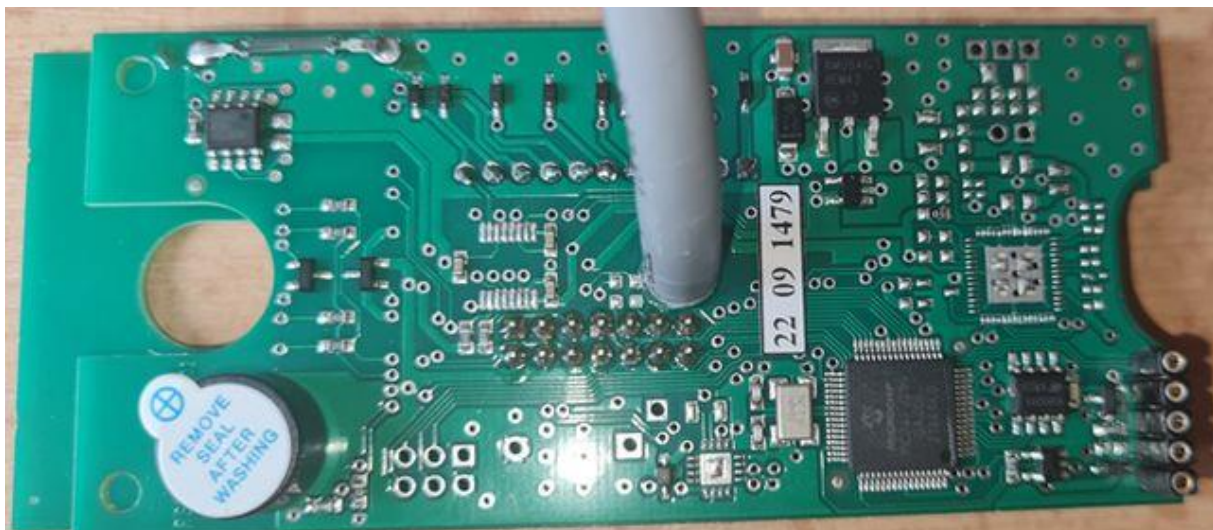


Figure 7: RFID reader main board

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 the area 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[12] 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 optimal protective tools detection within 1m distance. The camera module is on the Figure 9.

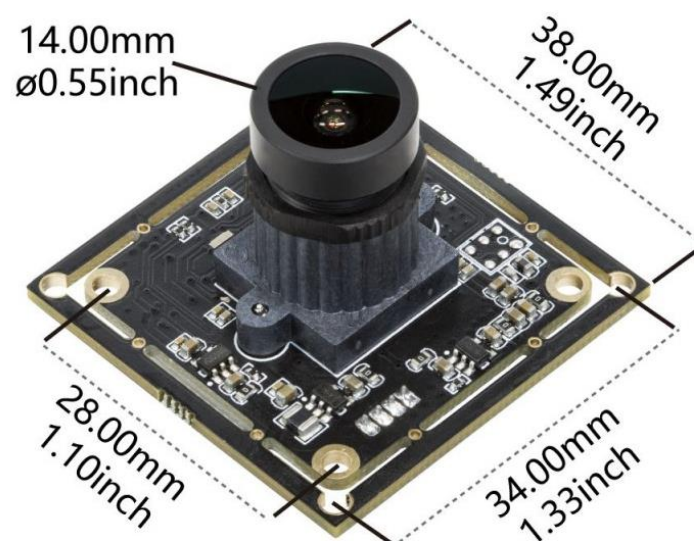


Figure 9: Camera module

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 larger amount 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) [13] module, which can be connected directly to the Raspberry via USB. This module is based on an Intel® Movidius™ Myriad™ X VPU [14] with 16 programmable shave cores and a dedicated computational engine for hardware acceleration of neural network computations. The advantages of this module are 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 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 [15], the IR camera is a Seek Thermal S304SP [16], and the TEC controller is an Analog Devices LTC1923[17] (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 bevelled, 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.

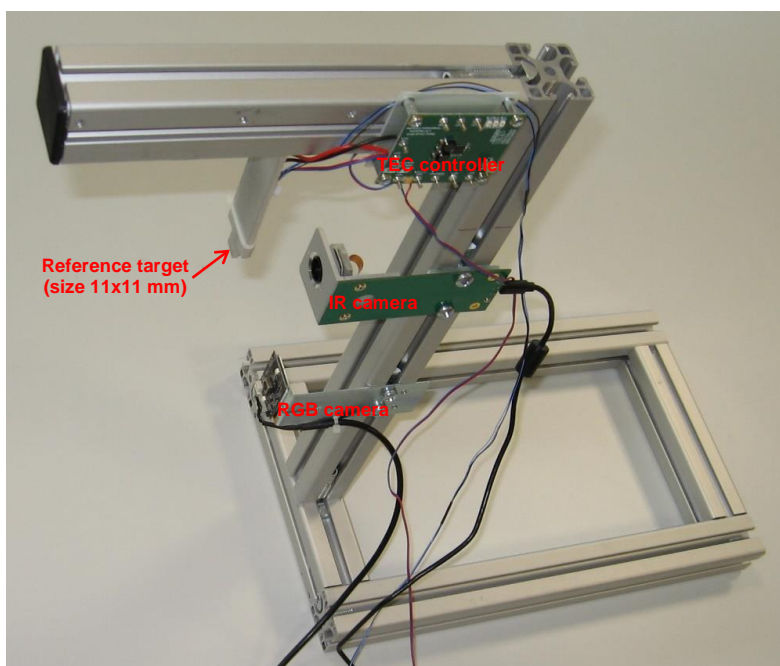


Figure 11: Development sample of the AI profile temperature measurement module

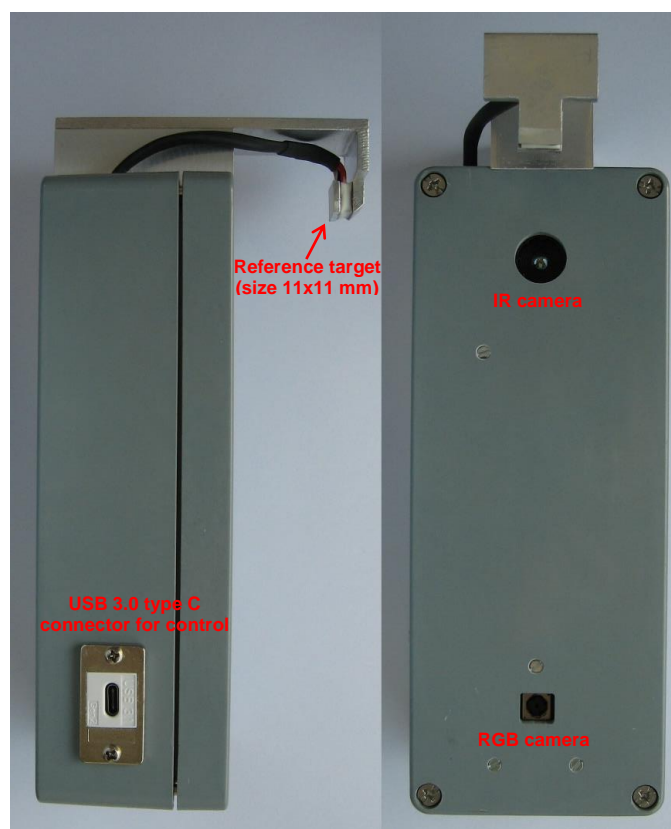


Figure 12: External view of a working sample of the temperature measurement module

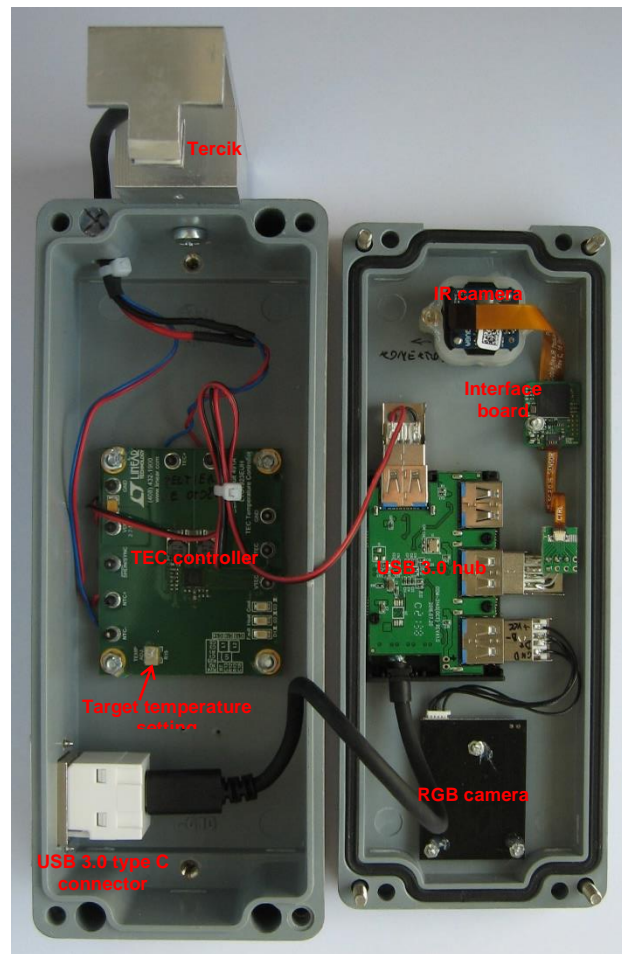


Figure 13: Internal layout of the functional sample of the temperature measurement module

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

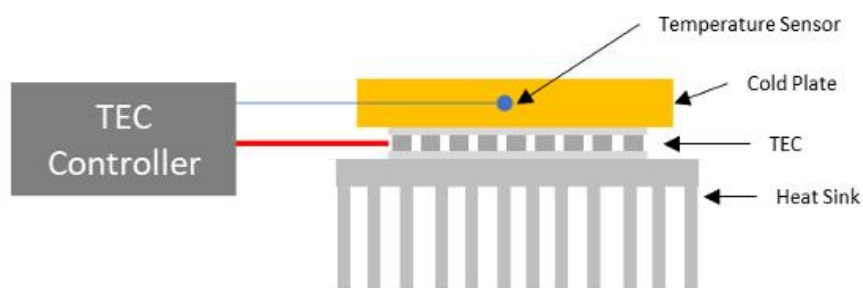


Figure 14: Block diagram of the reference target

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 and time-period) that will be evaluated and only general information about their fulfilment 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 to fully comply with EU standards. The latter will be based on the open-source EUDCC framework [18] 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.

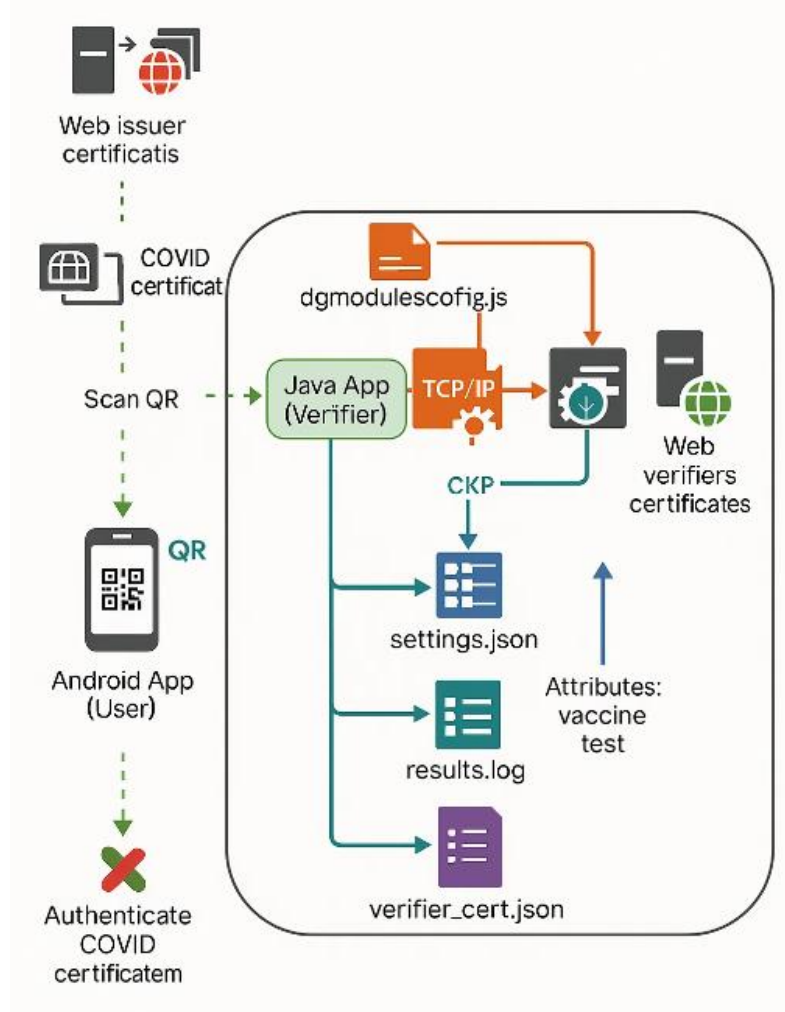


Figure 15: CovidPass verification system

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 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.

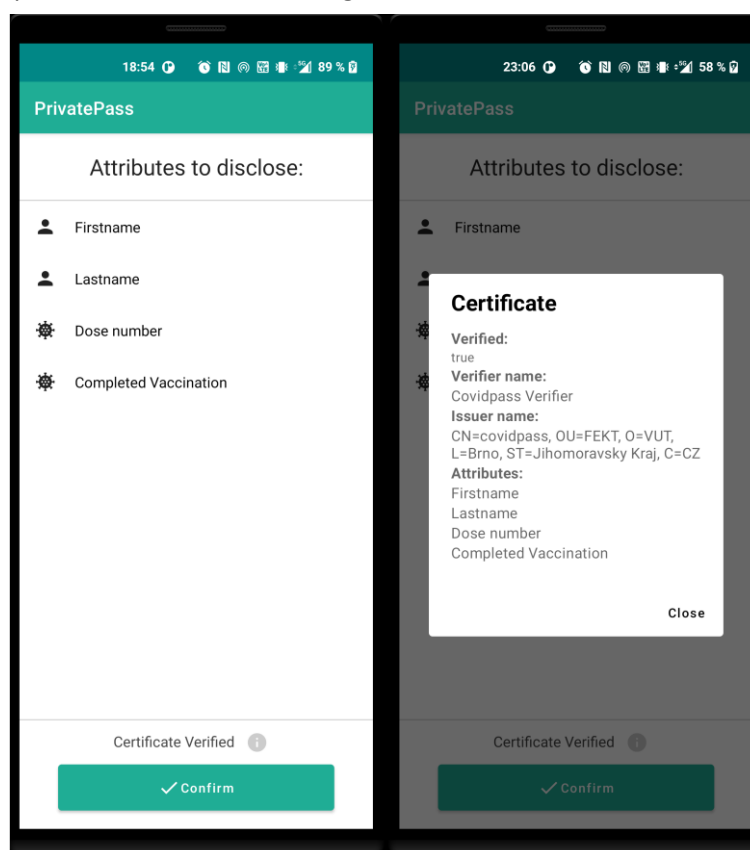


Figure 16: Mobile phone CovidPass application

2.2.8 Privacy-Preserving European Digital Covid Certificates

As described in more detail in D3.2 [39] and D4.1 [40], this module is envisioned to provide privacy-preserving cryptographic mechanisms to realize RiBAC in a way that still achieves a high level of compatibility with 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 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.

The purpose of this section is to first provide an in-depth understanding and analysis of the data flows in the current EUDCC architecture, and to analyse the potential privacy risks emerging from the current EUDCC architecture. Subsequently, we will describe mechanisms for mitigating those risks by the deployment of appropriate privacy-enhancing technologies.

In contrast to the remaining modules, this module has only achieved a lower TRL, due to the relative novelty of the approach and related open research and development challenges to be solved, so that the following description is also on a more technical level. However, on a metalevel, the design allows for a smooth integration into the overall RiBAC architecture.

2.2.8.1 Privacy-Analysis of the Current EUDCC Architecture

As a first step, we provide a brief overview of the LINDDUN analysis performed for the current architecture of the EUDCC. LINDDUN is an acronym standing for

- ▶ Linkability,
- ▶ Identifiability,
- ▶ Non-repudiation,
- ▶ Detectability,
- ▶ Data disclosure,
- ▶ Unawareness and unintervenability, and
- ▶ Non-compliance.

In a certain way, LINDDUN can be seen as a privacy-focused equivalent of the more prominent STRIDE/DREAD approach which is focused on identifying potential security threats and prioritizing them based on their severity and potential impact. In contrast, LINDDUN rather focuses on privacy and confidentiality risks of applications.

A brief overview of the phases of LINDDUN is depicted in Figure 17 (inspired by Linddun [19]).

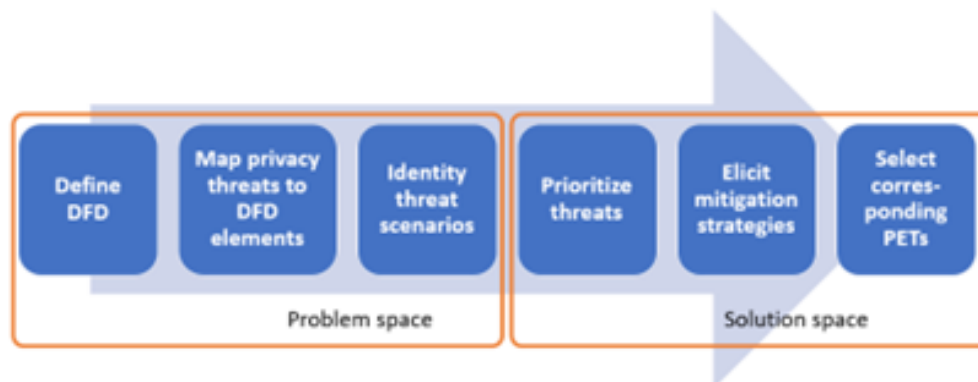


Figure 17: The LINDDUN Multistep approach

On a high level, the approach consists of six steps:

- ▶ Firstly, a detailed data flow diagram (DFD) specifying all involved entities, parties, data and information flows, and trust boundaries, is created.
- ▶ Secondly, a mapping of threat categories is performed for each DFD elements.
- ▶ Thirdly, the identified potential threats are further assessed and documented.
- ▶ In a fourth step, the identified threats are prioritized, depending on their likelihood and potential impact.
- ▶ In a fifth step, mitigation strategies are developed to minimize the risks identified before.

- ▶ Lastly, appropriate privacy-enhancing technologies are selected to instantiate the mitigation strategies developed before.
- ▶ Consequently, as a first step, we performed an in-depth assessment of the reference architecture of the European Digital Covid Certificate[18][19][20]. The analysis resulted in the DFD presented in the following Figure 18. [21]

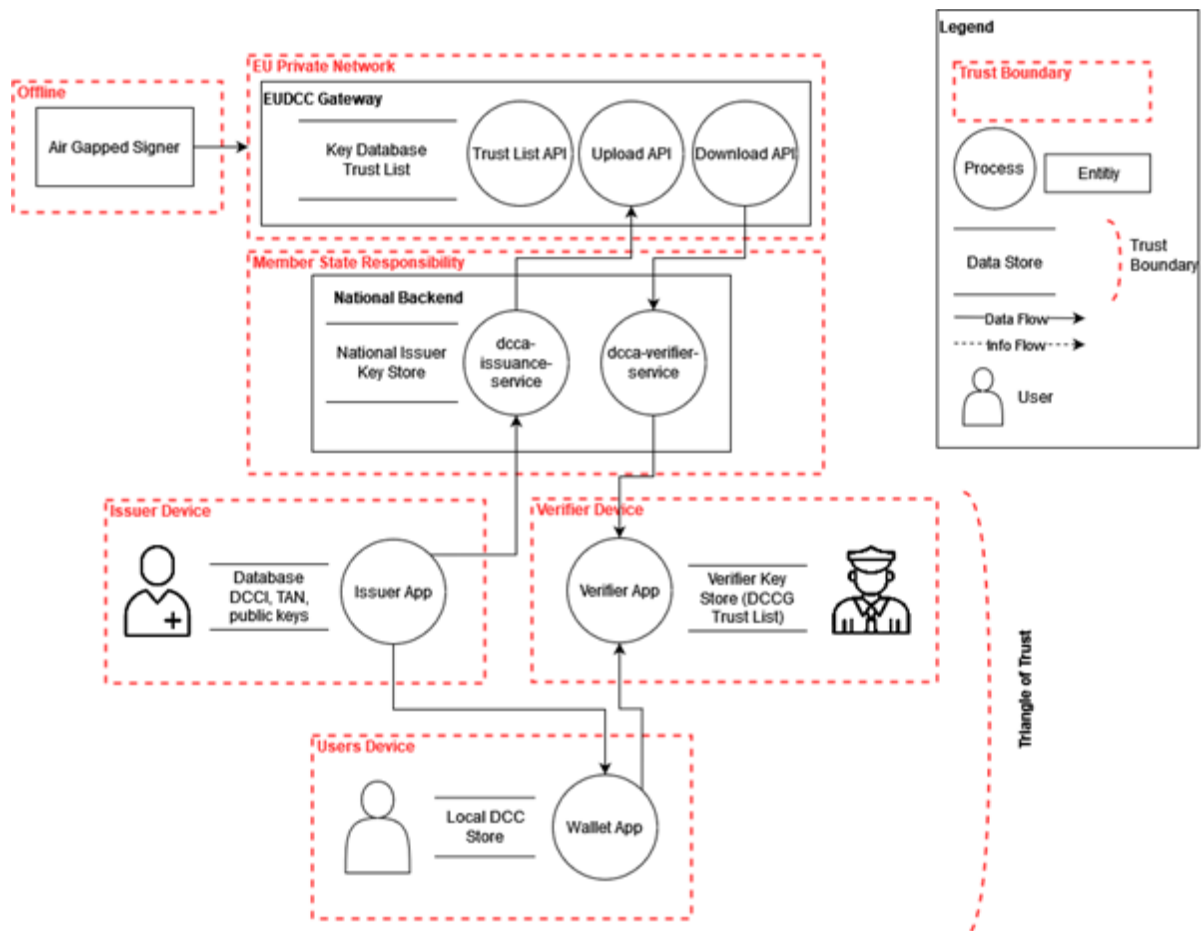


Figure 18 : Data flow diagram of the EUDCC [21]

For an in-depth discussion of this DFD, we refer to Stummer [21]. For the rest of our analysis, the most interesting user story is that of a citizen presenting their health status to a verifier, cf. Figure 19.

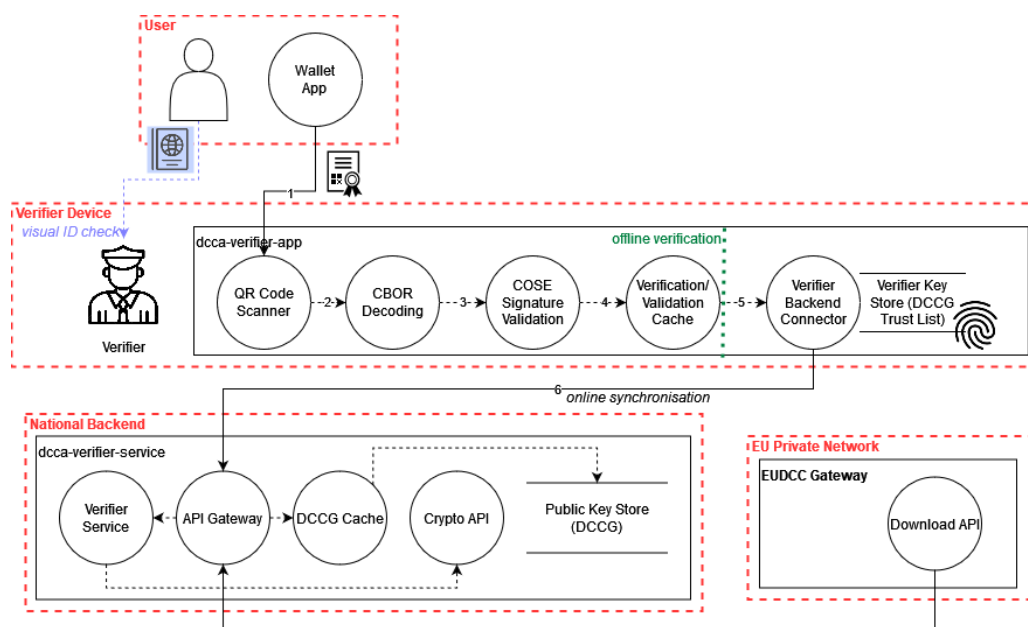


Figure 19 : Detailed DFD for credential verification [21]

Data flow diagram. On a high level, the flow starts with the verifier's initial request for the certificate holder to furnish evidence of vaccination, recovery, or a negative Covid-19 test. Subsequently, it falls upon the user to present either the paper or digital certificate through the wallet app. The verification process commences with the verifier app conducting a QR Code check, ensuring compliance with national regulations. Following this, the verifier inspects the certificate holder for the name and date of birth, and proceeds to request an official form of identification, such as a passport or identity card, to confirm identity. Upon receiving the passport from the DCC holder, the verifier manually verifies the name and date of birth before returning the document. This comprehensive procedure ensures thorough verification while adhering to established protocols.

Mapping threats to the DFD. While we will not provide a comprehensive LINDDUN analysis here and refer to Stummer [21]. However, the main finding is related to **identifiability**, **data disclosure**, and **link ability** during the presentation. More precisely, during presentation, a large amount of information is revealed to the verifier, together with a signature to certify the authenticity. This information comprises:

- ▶ the user's full name,
- ▶ data of birth,
- ▶ type of certificate (e.g., vaccinated, tested, recovered),
- ▶ date of test / vaccination / recovery, depending on the type, and
- ▶ the type of test / type and number of vaccinations, depending on the type.

Furthermore, as the verifier needs to physically check an additional document of the user to verify that the user is indeed the legitimate owner of the certificate, also any information contained in this identity document is revealed (e.g., nationality in case of a passport).

In addition to the information being revealed, the user is also fully linkable when re-using the same credential twice, due to a (static) identifier of the certificate.

Threat identification. There are at least two main threat scenarios immediately related to the above finding:

- ▶ Firstly, while legal regulations during the pandemic only required, e.g., that a user had been vaccinated (e.g., within the last 365 days) or that they had been tested (e.g., using a PCR test within the last 48 hours), revealing all information may lead to discrimination due to a certain level of division of society experienced during the pandemic.
- ▶ Secondly, full identification of a user allows to track users and identify recurring users. Furthermore, by pooling information across multiple verifiers could allow profiling of users (despite the legal limitations put out in Article 19 of the GDPR), both related to user preferences (which types of services a user attends), as well as geolocation.

Threat prioritization. To prioritize the risk, we need to estimate the likelihood of the threat being exploited, as well as the impact. While the former is hard to estimate, the impact for an individual may be significant, particularly in the case of discrimination due to, e.g., not having been vaccinated. While current solutions often rely on not showing this information to security personnel checking the status, this can easily be circumvented (in particular, as the reference architecture is available as open source), and users have no option to verify whether the information has been properly deleted after verification. Even in an optimistic scenario, we thus consider the threat sufficiently relevant to deserve further attention and mitigation.

Mitigation strategies. Overcoming the threat can be addressed by some changes to the current architecture:

- ▶ On the one hand, means to minimize the information revealed to the verifier need to be found. That is, the verifier needs to receive formal guarantees that a user satisfies a given policy (e.g., regarding timelines for tests or vaccinations), but without revealing any information beyond that. While this might not be possible for on-paper solutions, QR-codes could be generated on-demand by a mobile phone application per verifications session.
- ▶ On the other hand, to avoid over-identification via identity documents such as passports, certificates could be bound to users, e.g., using their biometrics. Upon verification, users could then additionally show that they are the physical owners of the certificate without having to reveal their identity data. This of course needs to be performed in a way that fully preserves the confidentiality of the biometric templates being processed, given that these are special category data according to Article 9, GDPR.

2.2.8.2 Selection of Privacy-Enhancing Technologies

A natural choice to realize the aforementioned mitigation strategies are so-called attribute-based credentials [22] which offer a dynamic and flexible approach to digital identity management by providing verifiable, granular access to specific attributes or characteristics rather than presenting a static, all-encompassing credential. Unlike traditional credentials, which require the disclosure of all certified – and, for specific verifications, often unnecessary personal information – attribute-based credentials (ABCs) allow users to selectively share only the pertinent attributes required for authentication or authorization, thereby enhancing privacy and minimizing the risk of identity theft. These credentials are particularly valuable in scenarios where individuals need to access diverse services or resources, as they enable tailored access control based on specific attributes such as age, role, or affiliation, without compromising sensitive personal data. Through attribute-based credentials, users maintain greater control over their digital identities, fostering trust and security in digital interactions.

Furthermore, various extensions exist in the literature. What is most important for our scenario are four extensions:

- ▶ On the one hand, range proofs (starting with work of Boudot [23] and Lipmaa [24]) allow one to prove that a certified number lies within an interval. Specifically in the context of EUDCC, this would allow to prove that a digital Covid certificate has not yet expired, without having to reveal the actual – e.g., vaccination – date.

- ▶ On the other hand, to prove that one was either vaccinated or tested, it is necessary to prove that different branches of a complex policy are satisfied. This can be done using techniques to prove partial knowledge as proposed by Cramer et al.[25]
- ▶ When only proving, e.g., that one was either vaccinated or tested, one needs to be aware that this information may still leak implicitly: for instance, if the certificate has been issued by a testing laboratory, the public key under which the certificate can be validated already reveals this information. What is thus needed are techniques to prove that a credential had been issued by a legitimate issuer, without revealing by which one. This concept of issuer-hiding anonymous credentials was first introduced by Bobolz et al. [26] and has been further advanced within the SUNRISE project by Mir et al. [27]
- ▶ Finally, as mentioned already in D4.2 [41], techniques to bind certificates to human beings need to be developed. This extension has been researched within the SUNRISE project and has resulted in a top-tier publication. [28]
- ▶ Put together, these PETs can address the threat identified before. However, integrating it into the current EUDCC architecture is non-trivial, as this also requires to update certain information flows: for instance, while in the current setting, the verifier defines the policy and does not need to transfer it to a user's device, after the upgrade of the architecture the user device needs to be aware of the precise policy, as the QR-code would be generated ad-hoc for a specific policy. A detailed discussion of the upgraded information flows is given by Stummer [21].

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 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 [29], 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 inside 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.

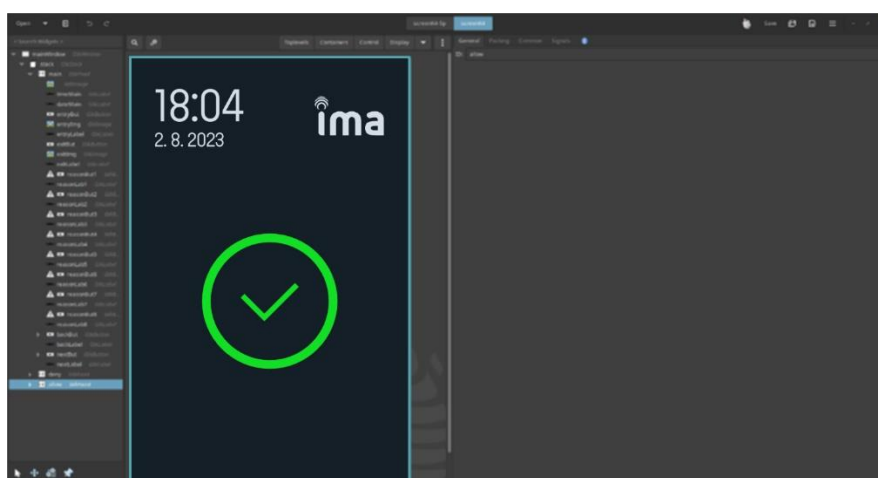


Figure 20: Screenshot from the application GUI builder

So far, the terminal program has a simple user interface with three screens. The reasons for 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 21.



Figure 21: 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 keep the terminal running 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 = 0, the pulse on the signal is D0. For bit = 1, the pulse is on signal D1. The pulse length is in the order of 10µs, 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 must 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

considered 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 22: 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 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 23: 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. Thus, the holder in the housing is only an additional mechanical fixing, the main one is the printed circuit board (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 24: 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 25.

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 25: Terminal from the back, mounting frame, mounted frame on the terminal

3 RiBAC Tool Validation in Lab Conditions

The general components of a RiBAC system consist of the following components:

- ▶ detection frame,
- ▶ control terminal,
- ▶ camera sensor,
- ▶ proximity temperature sensor,
- ▶ authentication object reader,
- ▶ display panel, and
- ▶ data interfaces.

While most of the modules described in the previous chapter are also present in traditional access control systems, the following will describe those aspects in detail that are specific to the RiBAC extensions developed within the SUNRISE project.

Specifically, we will explain the following aspects:

- ▶ Detection of protective equipment,
- ▶ non-contact body temperature measurement,
- ▶ two variants for vaccination status validation.

3.1 Lab Setup

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 26.

The tested modules were:

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

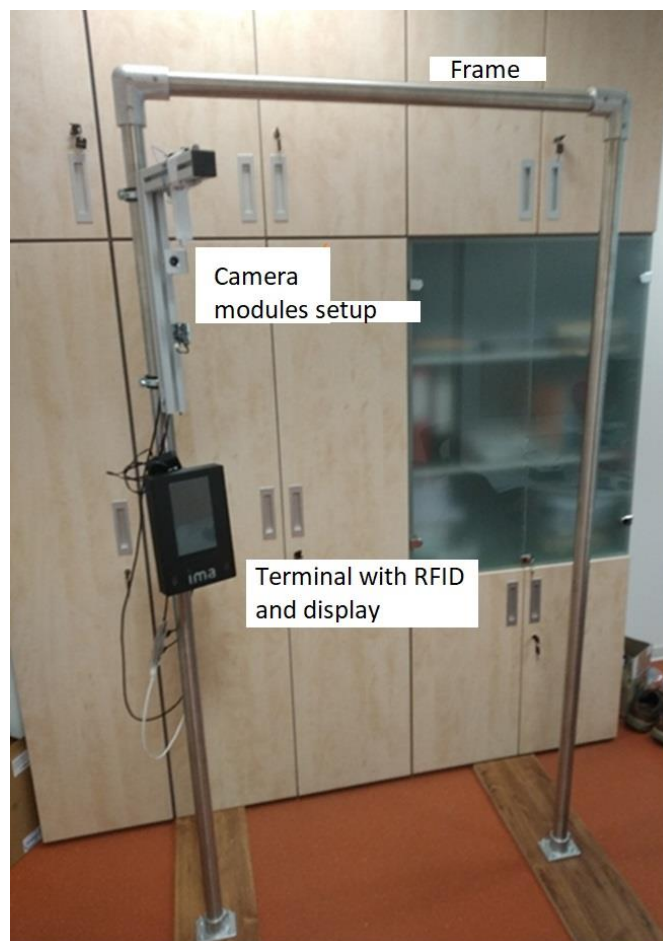


Figure 26: The test setup

3.2.1 Protective Tools Detection Module

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 27.

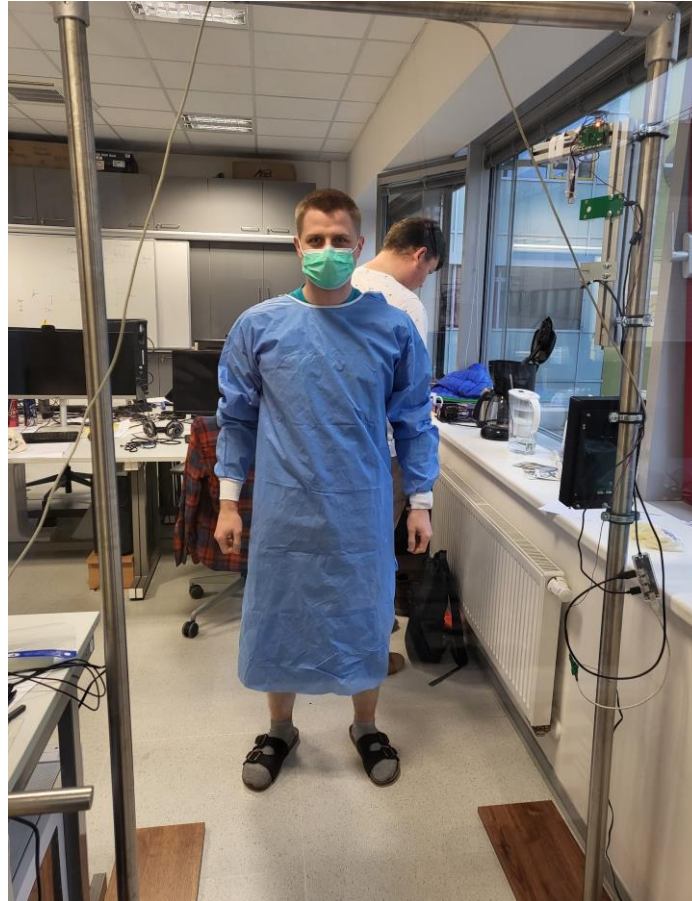


Figure 27: The test setup with user

Respirators and surgical drapes in different colours were used to control the respiratory protective equipment (respirators and respirators) deployed (see Figure 28).



Figure 28: 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 2, Table 3, Table 4, Table 5, and Table 6) 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

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

A distance lesser 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 2 and plotted graphically in **¡Error! No se encuentra el origen de la referencia..**

Table 2: 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

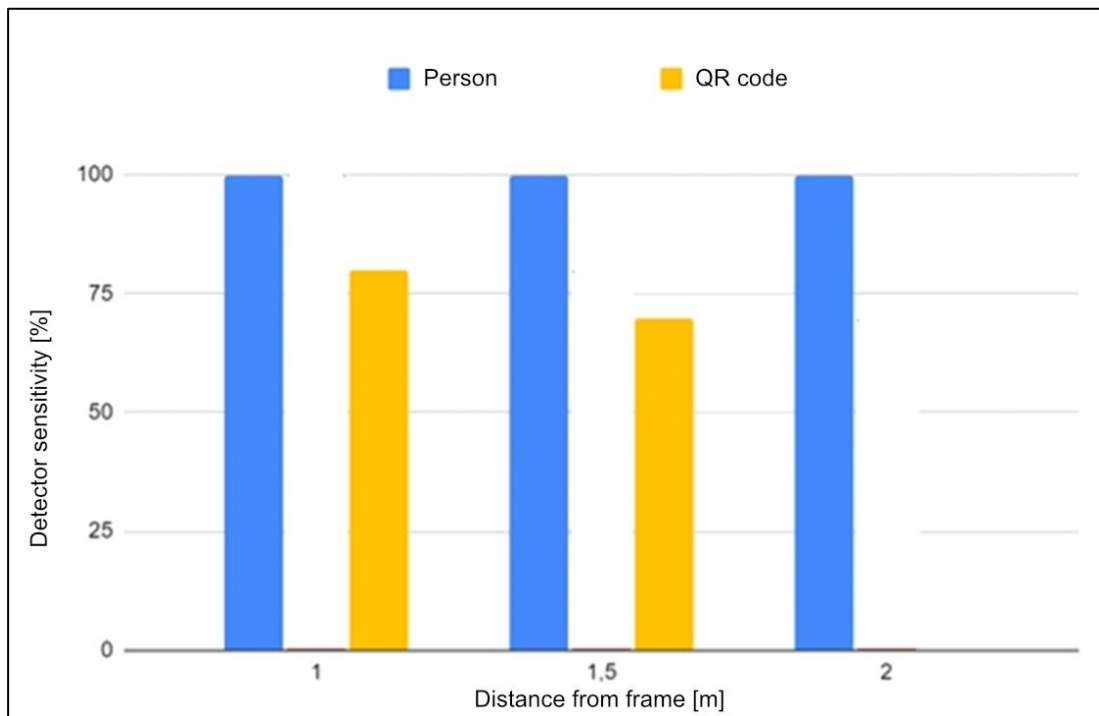


Figure 29: Measurement of the detector sensitivity as a function of the distance of the object from the frame.

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 subjects were successively approached in front of the detection frame within 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 subjects do not linger in front of the frame but walk away smoothly. To verify the robustness of the system against subjects with beards in the case of unfitted respiratory protection, special attention was paid to this category during testing. The ratio of subjects with respiratory protection to subjects without protection was set at 4:3. The results are presented in Table 3 and graphically illustrated in Figure 30.

Table 3: 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

Person	Beard	Respirator/ Drape (colour)	TP	TN	FP	FN
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%**. Significantly, 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. Whether the subject 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 any negative effect on the detection success rate.

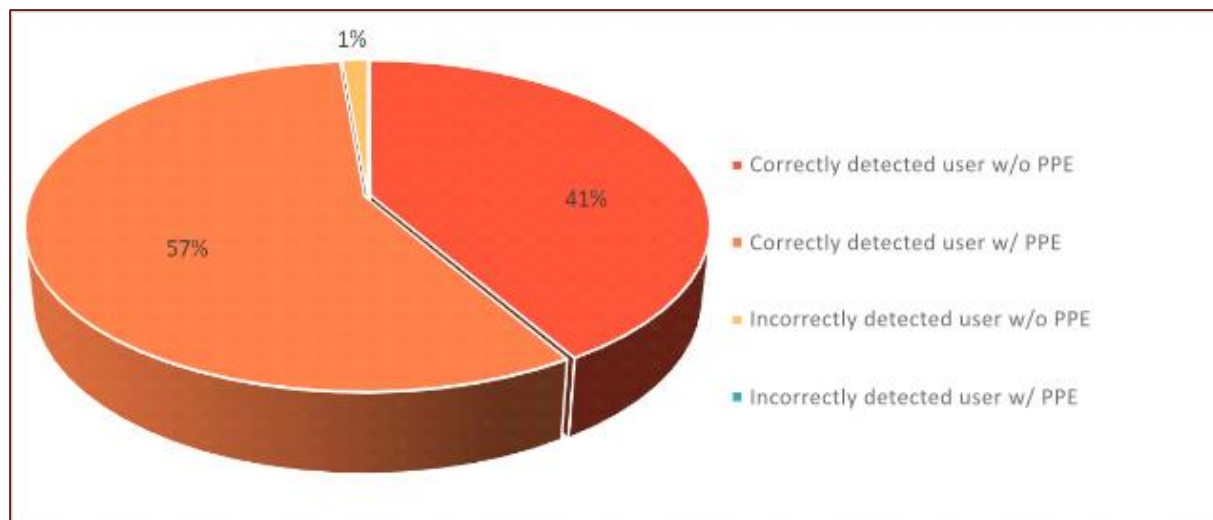


Figure 30: Test results of the task of detecting the use of respiratory protection.



Figure 31: Sample of the respiratory protection detection testing process.

3.2.2 Temperature Detection Module

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 [30] 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 very 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 32: 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 1 m, and the temperature was read from the unit's display on the SUNRISE system's display panel. It was problematic to secure subjects with elevated body temperature during this testing (testing was conducted in full operation on university premises), fortunately one subject with signs of acute illness was presented during the testing. This subject 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 4 and plotted graphically in Figure 33.

Table 4: 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

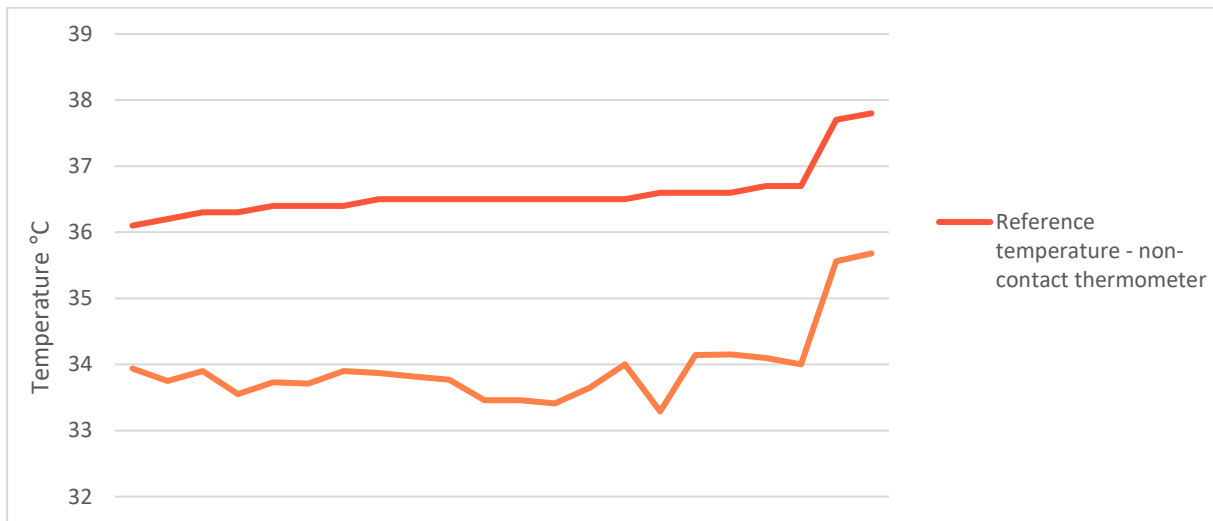


Figure 33: Comparison of body temperature measured with a non-contact thermometer and tested thermocamera.

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):

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

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

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, while glasses reflect thermal radiation, can have a negative effect on the measurement (see Figure 34). For this reason, attention has been paid in this section to subjects wearing glasses. The results of this experiment are presented in Table 5.

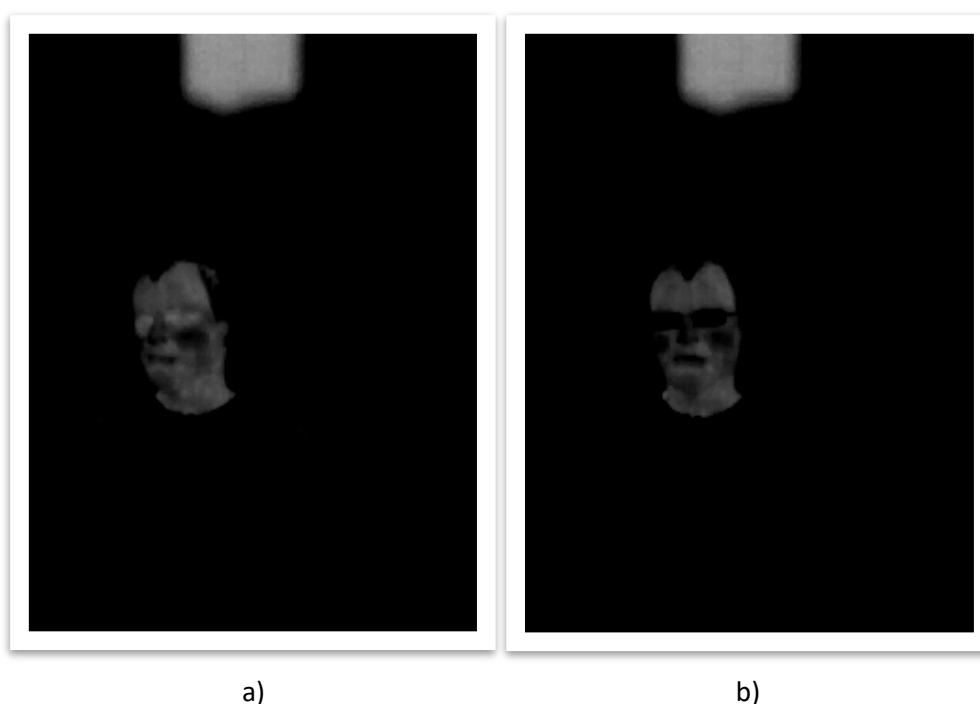


Figure 34: Illustration of the effect of wearing glasses on the measurement of emitted thermal radiation, a) face without glasses, b) face with glasses.

Table 5: 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 subjects with and without glasses: 1.96 ± 0.21 °C (without glasses) and 2.47 ± 0.14 (with glasses). Shown in Figure 35 are the temperatures measured by the reference thermometer and the temperatures measured by SUNRISE after correcting the values by the calculated average value for subjects 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 for a removal of glasses for the duration of the measurement.



Figure 35: 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) $\Delta T_{AVG} = 0,14^{\circ}C$.

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

3.2.3 Vaccine Credential Detection Module

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, other times, 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 6 and the graph in Figure 36 describe the dependency of the message exchange time on the number of detected attributes.

Table 6: 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

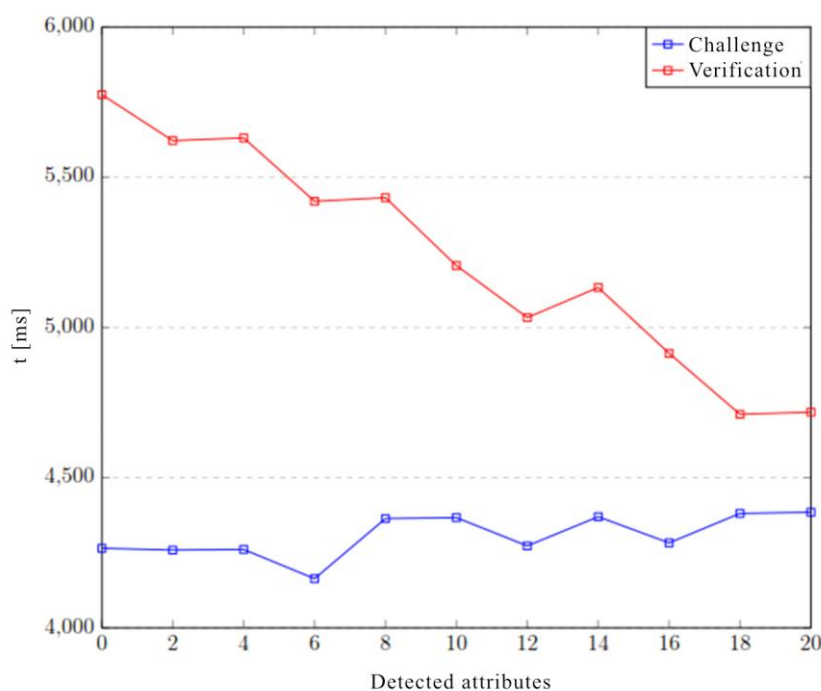


Figure 36: Effect of the number of detected attributes on communication.

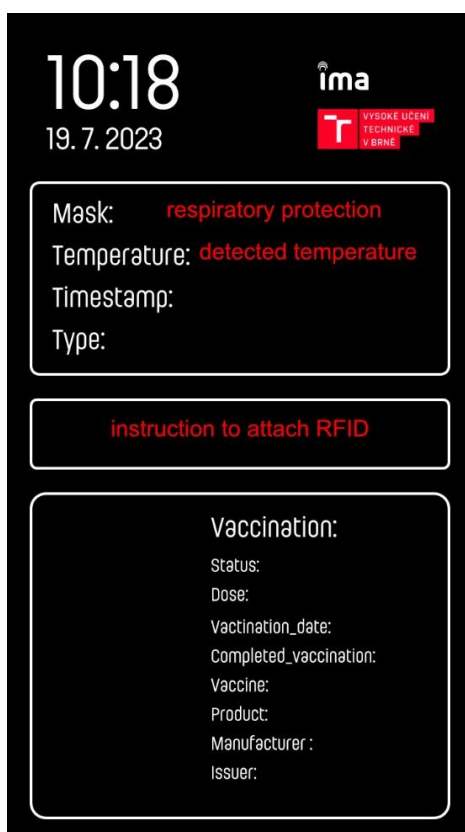


Figure 37: Information on the display.

3.2.4 Privacy-Preserving European Digital Covid Certificates

In line with the challenges and mitigation strategies developed in Section 2.2.8, the following advancements have been made within the context of SUNRISE.

Cryptographic libraries. Regarding cryptographic libraries, we contributed to the OLYMPUS open-source project for privacy-preserving attribute-based credentials, in close collaboration with the partners of the eponymous OLYMPUS [3] project.

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. For instance, if there is justified reason that a misuse or sharing of certificate happened, an external entity (e.g., a court) could re-identify the owner. However, this would happen in a way that ensures that the user is actually aware of this option already at the time of presentation, so that informed consent is guaranteed at all times;
- ▶ **Pseudonyms:** for scoped and user-controlled linkability. This could, e.g., be used to avoid duplication of certificates: in a larger context, re-use of the same credential within a predefined time zone (forming the scope) could be detected. In case of suspicious behaviour (e.g., because the corresponding locations are too far apart), this could then trigger the inspection functionality;
- ▶ **Revocation:** in case of fraudulent certificates or in case, e.g., of a positive Covid test despite a vaccination, it might become necessary to (temporarily) deactivate a credential.

Depending on the concrete deployment scenario and regulatory decisions, different combinations of the above features may be activated.

The extensions have been extensively tested under lab conditions to demonstrate the practical efficiency and usability of the extensions [31]. The results of these benchmarks are shown in the following figure.

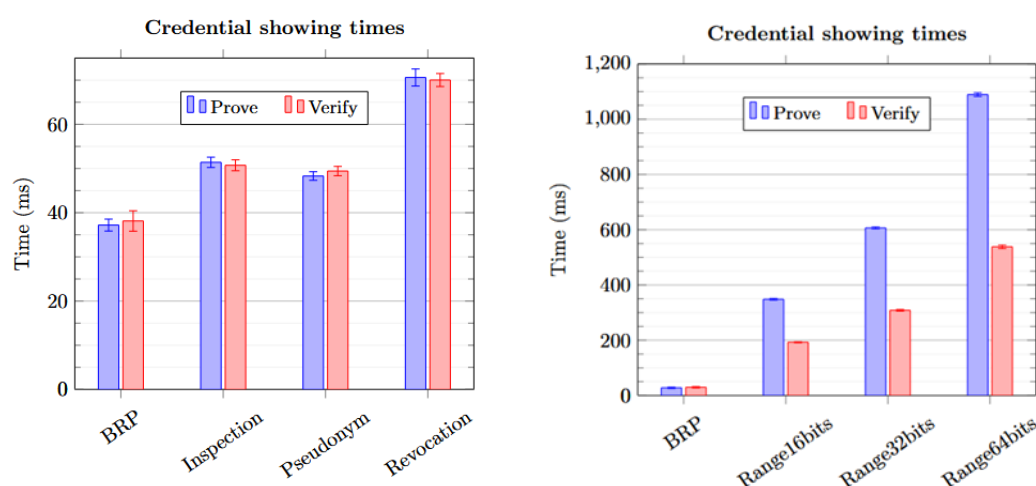


Figure 38 : Running times of necessary extensions of the OLYMPUS attribute-based credential library compared to a basic reference policy (BRP)

Assuming a granularity of one hour (to cover the validity period of tests with a sufficiently high preciseness) shows that 16-bit attributes for the expiration date would suffice for about 7 years of deployment. Furthermore, considering that a typical presentation policy could, e.g., be in the form of:

$\text{last-vaccination} < 365 \text{ ago OR last-test} < 48 \text{ ago,}$

and the ambition to hide which one is true, runtimes in the range of about 800ms could be achieved, not taking into account precomputations or hardware-specific optimizations.

The approach can thus be considered practically promising and will be further investigated in the next project phase.

Binding of credentials to users. Regarding the binding of physical identities to human beings, the team has developed all necessary protocols and cryptographic primitives [28]. On a high level, the protocols are attribute-based credential systems that allow one 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.

A high-level flow of the concept is also illustrated in Figure 39:

- In Step 1, the issuer issues a certificate to the user, thereby certifying the user's attributes and biometrics. The user stores this certificate, e.g., in an EU Identity Wallet compatible storage.

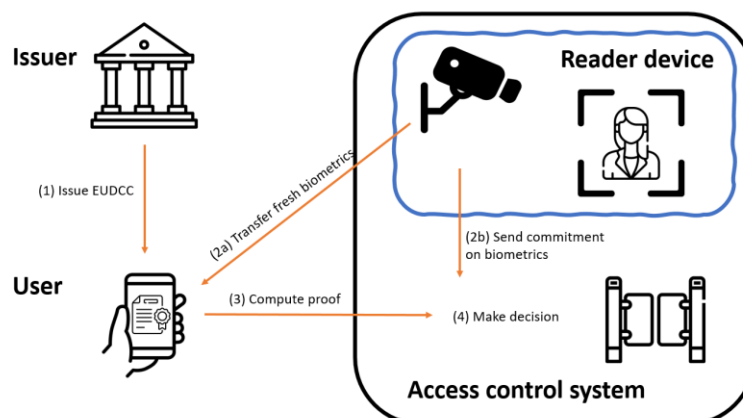


Figure 39: High-level flow of privacy-preserving biometric matching

- To authenticate, the access control system's camera now captures a fresh biometric reading of the user and sends it to the user (Step 2a). Concurrently, it also sends a commitment on this data to the access control system (Step 2b). This cryptographic commitment guarantees that the user is bound to a valid reading of the camera system but does not leak any information about the biometric template to the access control system.
 - The core assumption here is that this reader device can be a relatively small and well-audited piece of hardware and software, that both (users and verifiers) can agree to trust: while users need to trust that this system properly protects their biometric data, the verifier needs to trust that it received well-formed commitments on proper and fresh biometric measurements.
- In Step 3, the user's app now computes a presentation of their certificate received from the issuer, proving in addition that the biometric readings certified by the issuer and measured by the reader match each other (according to the metrics of the scheme).
- Finally, in Step 4, the access control system can now make an informed decision whether to grant the user access.

Similar to the above, the feasibility of this approach has been demonstrated using micro-benchmarks, i.e., by benchmarking the individual phases of the protocol separately. This resulted 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), again without any optimizations or pre-computations. Considering the time, it takes security personnel to physically inspect identity documents together with Covid certificates, and the fact that ICT solutions are easier to scale, this approach was considered sufficiently promising a further investigation.

As a result, the implementation of a lab demonstrator running inside a virtual machine was initiated. As a facial matcher, the OpenFace model nn4.small2.v1.t7 [32] was selected. The resulting runtimes were less than 100ms for generating the zero-knowledge proofs of facial matching, and less than 130ms for verifying the validity of a proof. All other parts (e.g., related to template extraction) were negligible.

Compared to the microbenchmarking, all computations were carried out on a powerful machine, which may not adequately reflect reality in terms of computational power of mobile phones or cameras. Future work will therefore take into consideration different computing platforms for different entities.

3.2.5 Prototypical Implementation

In addition to the above microbenchmarking, the above system has also been implemented as a standalone prototype, in order to demonstrate the practical usability of the application.

SUNRISE DEMO Issuer Screen	Date	2025-05-19
	Version	...

▼Camera


Take picture

Issue

Figure 40: Credential issuance

Figure 40 shows the issuance of a credential, relying on a picture of the user for later use as a biometric reference template. All key material of the issuer is set up in the background, and the issuer only has to confirm the identity of the user. Note in the context of a vaccination passport, this process would only need to be performed once, and the reference picture could then also be used for subsequent certificates.

SUNRISE DEMO User Screen	Date	2025-05-19
	Version	...

Issuer URL
 http://127.0.0.1:8001

Fetch credential

Enter Code Generated When Credential Was Issued
 code

Save

Figure 41: Fetching a credential

As can be seen in Figure 41, users can then simply fetch their credentials from the issuer, based on the code generated when the credential was issued. The credential is then stored locally on the user's device.

SUNRISE DEMO User Screen	Date	2025-05-19
	Version	...

Reader/Verifier URL


Figure 42: Initializing a presentation

Looking at Figure 42, when a user wants to present her credential, she has to actively initialize the presentation, e.g., by clicking the respective button. The device then connects to the specified verifier device, e.g., by IP address or alternatively by listing, e.g., compatible devices nearby. The user then receives data from a fresh reading from the sensor, which she confirms and computes the computation of the actual presentation, which she then sends to the user. The last two steps could be merged into a single one, yet were split for educational purposes to better explain the processes happening in each individual step.

SUNRISE DEMO Reader Screen	Date	2025-05-19
	Version	...

Issuer URL

▼Camera



Threshold: 0.6

Figure 43: Validating a presentation

Finally, Figure 43 shows the verifier's perspective. After accepting a presentation request, a fresh picture is taken, and finally the received proof is verified by the turnstile. Notably, the fresh reading (i.e., the picture) is only present within in the trusted reader device, and is again only shown for educational purposes and would not exist in real-world applications. The shown value "threshold" is an adjustable parameter to balance between false (positive or negative) acceptance rates.

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 44.



Figure 44: 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 7 and plotted graphically in Figure 45.

Table 7: 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

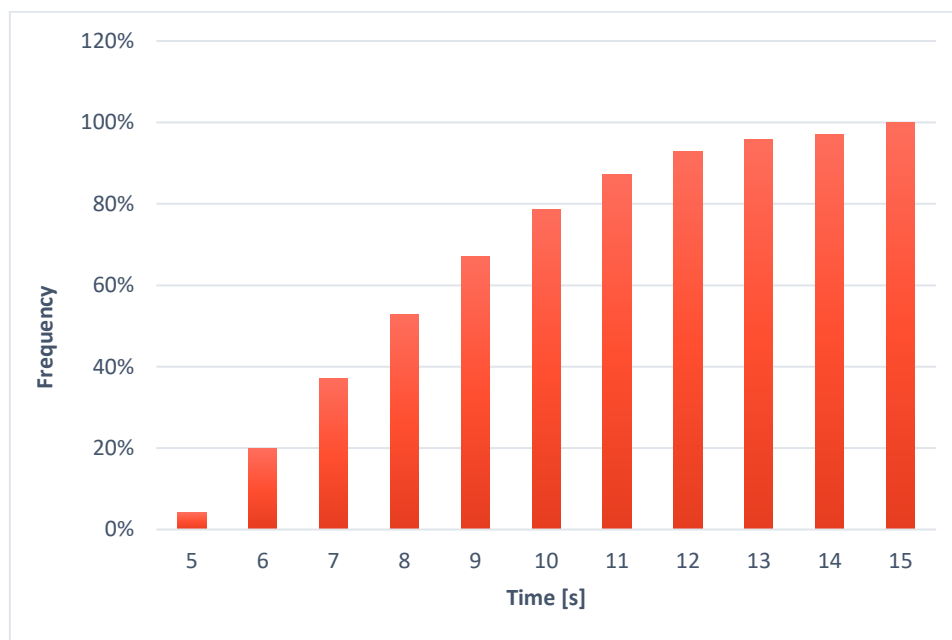


Figure 45: Cumulative histogram of the total clearance time of the co-located detection frame.

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

When checking then $T_{AVG} = 10,09 \pm 4,14$ s

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

96% of subjects 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.

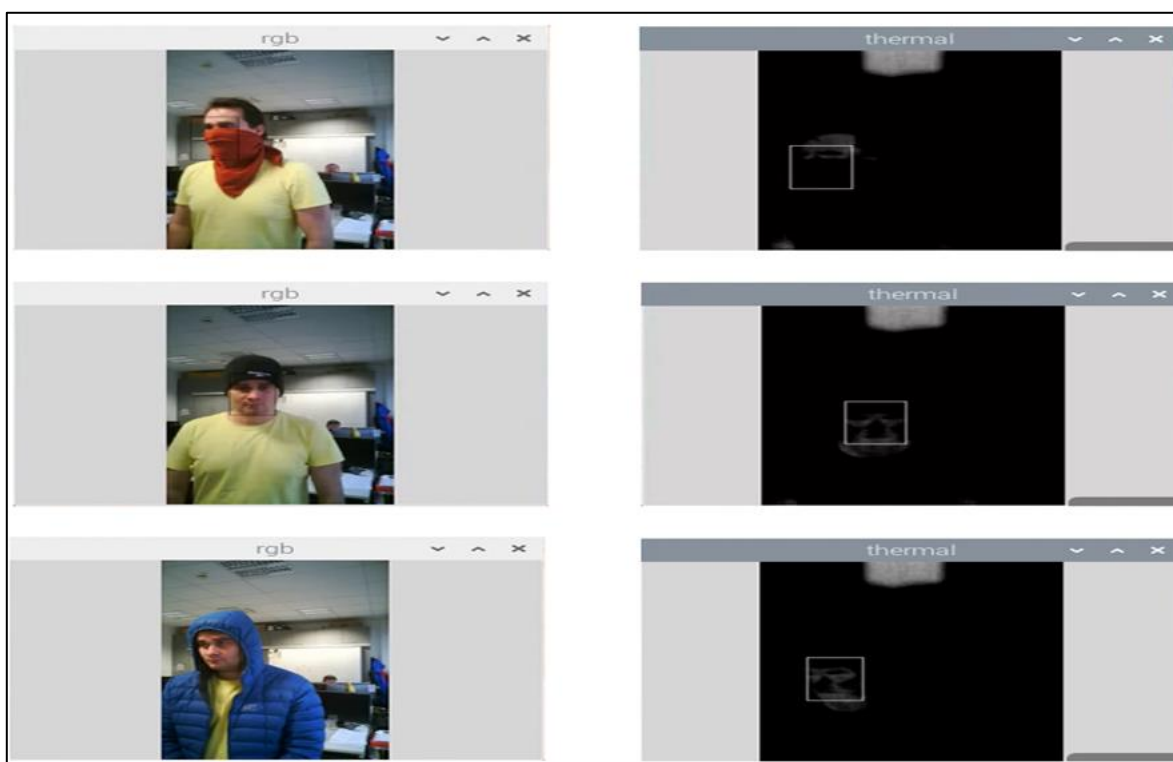


Figure 46: Example of experimental testing.

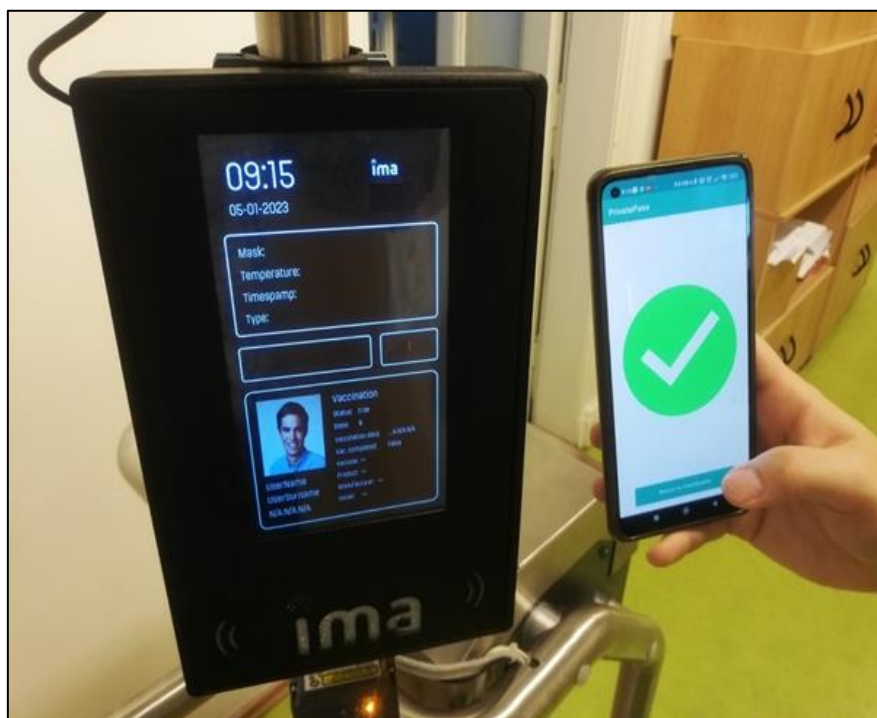


Figure 47: Vaccine credential verification

3.4 Pilot Deployment Results and Feedback

The first round of pilot deployments, documented in detail in D4.4 [43], provided invaluable insights for the advancement of the RiBAC tool to TRL7. This section summarizes the key findings from these deployments and how they informed the final refinements of the system.

3.4.1 Pilot Deployment Overview

As described in D4.4 [43], the RiBAC tool was deployed across nine pilot sites spanning three countries (Czech Republic, Slovenia, and Italy) and multiple CI sectors:

1. **Healthcare sector** (3 sites)
 - UKC Ljubljana Children's Hospital – two devices (Slovenia)
 - UKC Exit Control (Slovenia)
 - Military University Hospital in Prague (Czech Republic)
2. **Transportation sector** (1 site)
 - SZ/PIL Prometni Institute Ljubljana offices (Slovenia)
3. **Digital services sector** (3 sites)
 - Telekom Slovenije (Slovenia)
 - Insiel HQ (Italy)
 - CAFC (Italy)
4. **Industry sector** (2 sites)
 - IMA/WITTE (Czech Republic)

Each pilot site implemented different configurations of the RiBAC tool, depending on their specific requirements and operational context. This diversity of deployments provided a comprehensive evaluation of the system's flexibility and adaptability.

3.4.2 Key Findings from First Round Pilots

The pilot deployments highlighted several important aspects of the RiBAC tool's performance in real-world environments:

Technical Performance

1. **Module Reliability:** Overall, the core modules performed well, with most sites reporting successful validation of the following requirements:
 - FR.WP4.01 (Protective equipment detection): 8/9 sites reported successful validation
 - FR.WP4.02 (Temperature check): 7/9 sites reported successful validation
 - FR.WP4.03 (Cryptogram creation): 5/9 sites reported partial validation
2. **Integration Challenges:** The integration with legacy access control systems (NFR.WP4.02) presented the most significant challenges, with 3/9 sites achieving full integration during the first pilot phase.
3. **Real-time Performance:** The near real-time operation requirement (NFR.WP4.01) was successfully validated at all sites, confirming the system's responsiveness.

User Experience

1. **User Acceptance:** Overall user acceptance was high, with 99% of users expressing trust in the solution.
2. **Throughput Concerns:** Several sites raised concerns about the throughput capacity during peak periods, particularly in healthcare and transportation environments.
3. **Training Requirements:** The need for clear user guidance and training was emphasized, with 47 employees successfully trained across the pilot sites.

Environmental Factors

1. **Lighting Conditions:** Variable lighting was identified as a challenge for the protective equipment detection module at 3 sites.
2. **Temperature Variations:** Environmental temperature fluctuations affected the accuracy of temperature measurements at 4 sites.
3. **Physical Space Constraints:** Installation requirements varied significantly across sites, highlighting the need for flexible mounting options.

3.4.3 Pilot-Driven Improvements

Based on the feedback and findings from the first round of pilots, the following key improvements have been implemented in the advancement to TRL7:

1. **Environmental Adaptability:**
 - Improved operation under variable lighting conditions
 - Enhanced temperature calibration for different environmental settings
 - Development of flexible mounting solutions for various installation scenarios
2. **User Experience Refinements:**
 - Customizable user scenario to improve throughput
 - Clearer visual guidance on the terminal
3. **Deployment and Maintenance Tools:**
 - Enhanced remote configuration and monitoring capabilities
 - Improved diagnostic and troubleshooting features

These improvements are directly addressing the challenges identified during the first pilot phase and have been validated through laboratory testing prior to the second round of pilot deployments.

4 Pilot trials execution (feasibility analysis)

4.1 Description of piloting activities

4.1.1 Pilot sites overview

Table 8 provides an overview of the different modules that are deployed at the different pilot sites. Specifically, depending on whether there is an ongoing pandemic or the system is operated in standard mode, different modules of the access management can be deployed. This also illustrates the dynamic and modular design of the system, which can also be considered a key selling point of the architecture.

Table 8: Pilot site overview

Pilot sites	Pandemic Scenario					Standard operation				
	temp	mask	vaccin	ident	extra	temp	mask	vaccin	ident	extra
A/ SL-UKC-main entr. to children's clinic	Y	Y	Y/SL	off	off	off	off	off	off	off
B/ SL-UKC-entr.from the parking	Y	Y	Y/SL	Y	off	off	off	off	Y	off
C/ SL-UKC-exit from the operating theatre	off	off	off	off	RGB	off	off	off	off	RGB
D/ SL-TS-Testing lab	Y	Y	Y/SL	Y	off	off	off	off	Y	off
E/ SL-SZ-Testing lab	Y	Y	Y/SL	Y	off	off	off	off	Y	off
F/ IT-FVG-Testing lab	Y	Y	Y/IT	Y	off	off	off	off	Y	off
G/ IT-FVG-Testing lab	Y	Y	Y/IT	Y	off	off	off	off	Y	off
H/ CZ-WITTE&IMA	Y	Y	Y/CZ	Y	off	off	off	off	Y	off
I/ CZ-MUH Prague	Y	Y	Y/CZ	Y	off	off	off	off	Y	off

4.1.2 Czech pilots

IMA has been a long-term supplier of a robust access control system (AC system) called IMAPorter Pro [33] 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 first piloting schedule for Czech pilots contained several phases, see Figure 48:

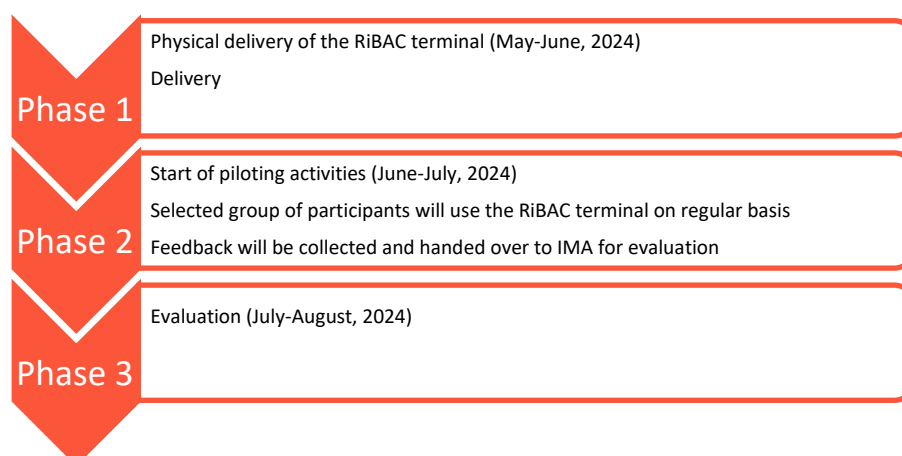


Figure 48: Piloting Schedule for Czech pilots

4.1.2.1 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. The system is being run by security department employees of the military university hospital in Prague (MUH).

RiBAC tool will therefore serve as an extension to the existing legacy ACS supplied by IMA and provide additional layers of access control based on current pandemic conditions. In case of normal operation, the MUH may continue to use just the access control module of RiBAC without risk-based pandemic measures.

The pilot itself will mimic the pandemic scenario, therefore (see Table 8) in the case of MUH, following tool modules will be switched on:

- ▶ Temperature check
- ▶ Mask detection
- ▶ Vaccination passport check
- ▶ Access (user identification)



Figure 49: Military University Hospital in Prague

4.1.2.2 Czech Technical University in Prague (education)

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

RiBAC tool will be tested at the entrance to the Department of Microelectronics.

RiBAC will be installed in parallel to legacy ACS, but users will be able to use their existing access cards for legacy ACS as well as for RiBAC.



Figure 50: Rectorate of the CTU in Prague

Following tool modules will be switched on to test the pandemic scenario:

- ▶ Temperature check
- ▶ Mask detection
- ▶ Vaccination passport check
- ▶ Access (user identification)

4.1.3 Italian cluster

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

The first piloting schedule for both Italian cluster pilots (INS, CAF) took place as follows:

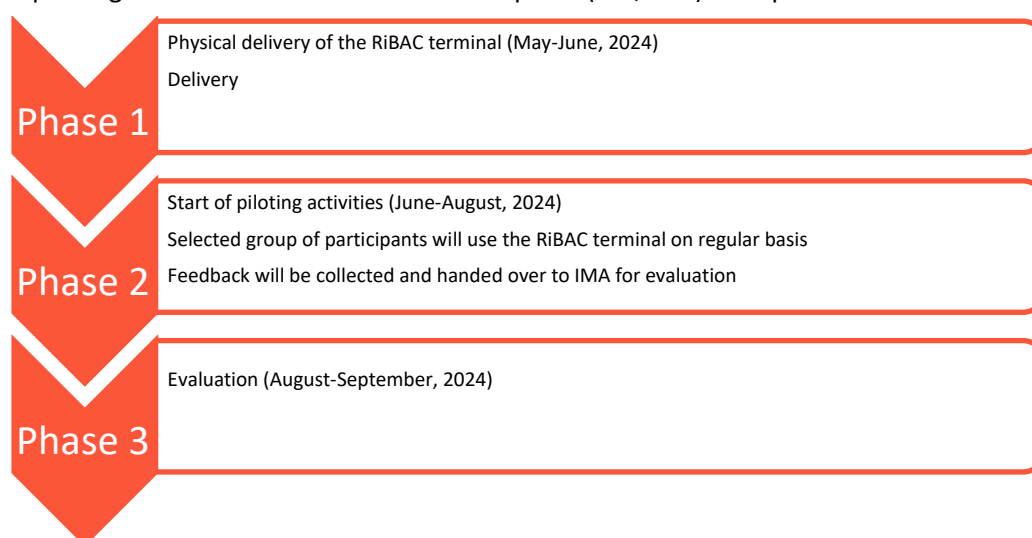


Figure 51 : Piloting schedule of the Italian cluster

Following tool modules will be switched on to test the pandemic scenario:

- ▶ Temperature check
- ▶ Mask detection
- ▶ Vaccination passport check
- ▶ Access (user identification)

4.1.3.1 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 at the main entrance.

The physical access control is structured in two parts, the main door (Figure 52) is open from 7:00 to 19:00 and opens on request for the rest of the day.



Figure 52: Insiel HQ entrance

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

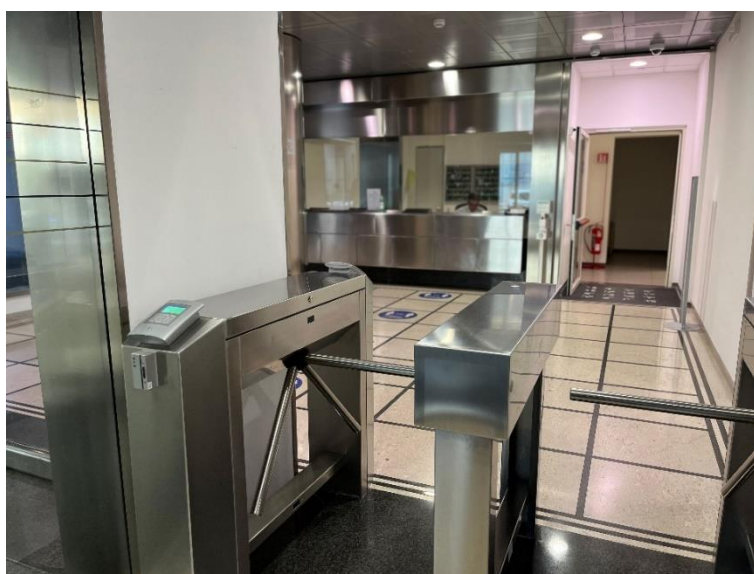


Figure 53: Insiel HQ - turnstile

Recently Insiel implemented a new access system 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 [34].

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, 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. For security policy, RiBAC tool will be deeply tested in the second phase in a secondary premises of Insiel, located in province of Udine.

4.1.3.2 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.

4.1.4 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 there will be as much as three separate RiBAC devices tested within UKC; one additional by SZ and one final by TS.

The first piloting schedule for the Slovenian cluster pilots (UKC, SZ, TS) took place as follows:

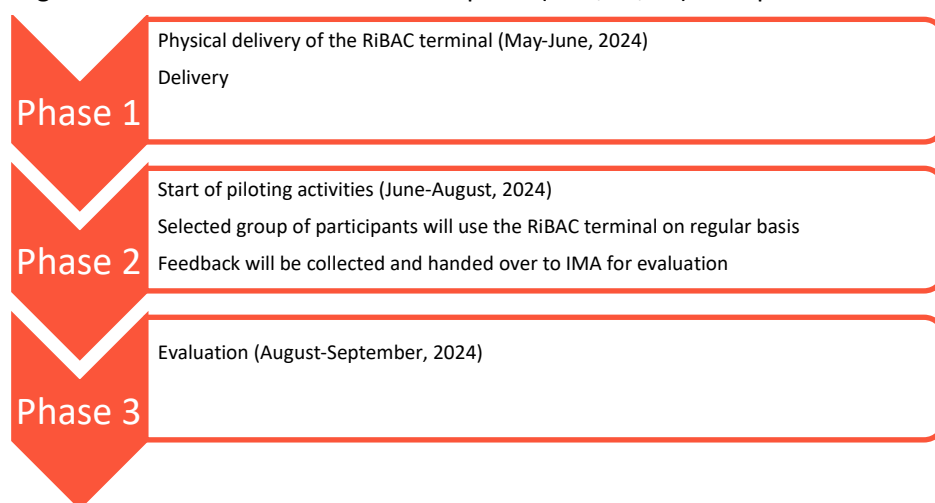


Figure 54 : Piloting schedule for Slovenian cluster

4.1.4.1 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.

Three separate pilots are envisioned within UKC.

- 1) Main entrance to the children's clinic, where the following modules will be tested: temperature check, mask detection, vaccination passport check
- 2) Entrance from parking lot: temperature check, mask detection, vaccination passport check, employee identification
- 3) Exit from an operating theatre, where the RiBAC terminal will serve as a precaution to prevent surgeons from exiting the theatre with contaminated clothing

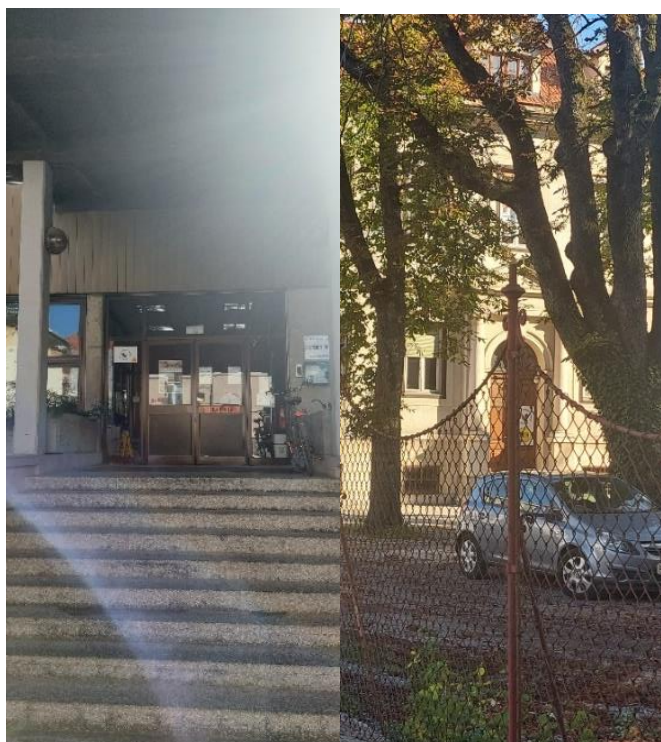


Figure 55: UKC Ljubljana Old City Children Hospital

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

One RiBAC tool terminal will be tested at an office of Prometni Institut Ljubljana, which is located opposite to the Ljubljana Main railway station by selected group of participants.



Figure 56: Main railway station in Ljubljana

4.1.4.3 TS - Office building of Telekom Slovenije (digital)

One RIBAC tool terminal will be tested in lab conditions of Cigatelova street office building of Telekom Slovenije, by a selected group of pilot participants.



Figure 57: TS offices in Cigatelova street

4.2 Description of End-Users' Roles

The term “end-user” regarding to WP4 RiBAC (Risk-Based Access Control) Tool refers to the **employees and personnel** of the different **Critical Infrastructures** (CIs), where the Tool will be piloted. In the case of piloting the RiBAC Tool in hospitals (SLO + CZ), the tool end users might also be the patients of the hospital (i.e. general public). Following table summarizes the end user profiles of the RiBAC Tool.

Table 9: End user profiles of the RiBAC Tool

User organization	End user profile	Role	Skills
CI operators	Tactical	IT personnel	Managerial (overseeing the pilot)
CI operators	General	Any employee	Generic (any pilot participant)
General public	General	Any CI visitor (e.g. hospital patients)	Generic

Within WP4, there are eight envisioned pilots to be taking place in three countries: Slovenia, Italy and the Czech Republic. Current piloting schedule of WP4 envisions the start of the piloting activities to M20. During the first phase of piloting, a group of participants will be selected from the personnel of each individual CI. User guide for the pilot participants will be released prior to the start of piloting activities in accordance with T4.5 led by INS.

Overview of the pilot partners listed by use case / sector and pilot location is below:

- ▶ **Health (Slovenia)** – University Medical Centre Ljubljana (UKC)
- ▶ **Transport (Slovenia)** – National Railways Operator (SZ, SZI)
- ▶ **Digital (Slovenia)** – Telecommunications Operator Slovenia (TS)
- ▶ **Digital (Italy)** - Health digital services (INS, FVG)
- ▶ **Water (Italy)** - Water provider (CAF)
- ▶ **Industry (Czech Republic)** – Automotive supplier WITTE Automotive
- ▶ **Health (Czech Republic)** – Military University Hospital Prague

4.3 Second Pilot Phase Status

Following the successful completion of the first pilot phase and the implementation of improvements based on the feedback received, planning and preparations for the second and final pilot phase have been finalized. This phase represents a critical step in validating the TRL7 version of the RiBAC tool across diverse operational environments.

4.3.1 Enhancements for Second Pilot Phase

Based on the insights gained from the first pilot phase and discussions with CI partners, a set of enhancement options was developed for the second pilot phase. These options were designed to address specific needs identified by the partners and to further advance the capabilities of the RiBAC tool:

- ▶ **Offline RiBAC System with Event Generation and Actuator Capabilities**
 - Enhanced screen notifications for users and operators
 - Sound signals for alerts and confirmations
 - Simulated door lock actuator control (via LED indicator)
 - Improved local processing capabilities without requiring continuous network connectivity
- ▶ **Specialized Functionality (RiBEC - Risk-based Exit Control)**
 - Adaptation of the RiBAC system for monitoring and controlling exits
 - Specialized detection parameters for exit scenarios
 - Additional reporting and monitoring capabilities
- ▶ **Software Upgrades for Reporting**
 - Implementation of simplified reporting capabilities
 - Collection and visualization of usage statistics (e.g., number of passages per day)
 - Enhanced data management for operational analytics

4.3.2 Partner Selections for Pilot Implementations

Following extensive discussions at the General Assembly meeting in Dublin and subsequent consultations, CI partners have selected the following enhancement options for their RiBAC installations:

- ▶ **INS/CAF, SZ, TS** have selected Option 2 - Offline RiBAC system with event generation capabilities
 - This configuration will enable these sites to operate more autonomously while providing clear feedback through visual and auditory signals
 - The simulated door lock control will demonstrate integration capabilities without requiring modifications to existing infrastructure
- ▶ **UKC** has selected Option 5 - Specialized functionality (RiBEC - Risk-based Exit Control)
 - This unique adaptation will showcase the flexibility of the RiBAC architecture for specialized use cases
 - In addition, software upgrades enabling simplified reporting will be implemented to enhance operational insights

These selections reflect the diverse operational requirements across different CI sectors while maintaining the core functionality of the RiBAC system.

4.3.3 Objectives of the Second Pilot Phase

Based on the selected enhancements, the second pilot phase will focus on the following objectives:

1. **Validating Enhanced Functionality:** Testing event generation and actuator capabilities in upgraded RiBAC Tool implementations, specialized RiBEC functionality at UKC
2. **Operational Autonomy:** Evaluating the reliability of offline systems, local processing effectiveness, and resilience during network disruptions.
3. **User Experience:** Assessing user response to enhanced notification systems and visual/auditory indicators.
4. **Integration Assessment:** Evaluating simulated integration capabilities and identifying pathways for full integration with existing access control systems.
5. **Data Collection:** Testing reporting capabilities and assessing the operational value of collected statistics.

4.3.4 Current Status and Preparation

As of the time of writing, preparations for the second pilot phase are well underway:

- ▶ Tool upgrade specifications have been finalized based on partner selections
- ▶ Development teams are implementing the selected upgrades for each installation
- ▶ Deployment planning is in progress with each partner site
- ▶ Testing protocols have been established to evaluate enhanced functionality

The development team is focused on ensuring timely implementation of all enhancements, with ongoing coordination with partner sites to address any specific requirements or considerations for their installations.

Full results of the second pilot phase will be documented in D4.6 "Access Control Pilot Report V2", which will provide a comprehensive evaluation of the TRL7 version's performance in operational environments and validate the system's production readiness.

5 Conclusions

This deliverable presents the final version of the Risk-Based Access Control (RiBAC) tool, documenting its advancement to Technology Readiness Level 7 (TRL7). The RiBAC tool has evolved from its initial conceptualization through progressive iterations, culminating in a production-ready system validated through extensive laboratory testing and real-world deployments.

The first round of pilot deployments across nine sites in three countries confirmed the system's effectiveness, with high validation rates for core functional requirements and a 99% user trust rating. Based on feedback from these pilots, significant enhancements have been implemented, including better environmental adaptability, streamlined user interfaces, and enhanced remote management capabilities.

Preparations for the second pilot phase are now complete, with CI partners having selected specific enhancements tailored to their operational needs: offline operation with event generation capabilities for INS/CAF, SZ, and TS, and specialized exit control functionality (RiBEC) for UKC. This phase will further validate the TRL7 readiness of the RiBAC tool and provide additional insights for potential commercialization.

The RiBAC tool demonstrates several key innovations: a modular design allowing selective activation of pandemic-specific components, a privacy-preserving approach ensuring GDPR compliance, seamless integration with existing infrastructure, multi-factor risk assessment combining protective equipment detection, temperature measurement, and vaccination status verification, and enhanced remote management capabilities.

This document completes the documentation requirements of Task 4.3 (UI for privacy-friendly risk-based access control) by providing final user interface specifications and Task 4.4 (Continuous integration and testing) by documenting the TRL7 validation. It also provides essential input for the ongoing Task 4.5 (Demonstration, training, evaluation, and validation), which will continue through the second pilot phase. The training materials and implementation guidelines presented here will directly support the remaining deployment activities and final evaluation of the RiBAC tool.

Looking beyond the SUNRISE project, the RiBAC tool offers CI operators an asset for enhancing their resilience against future pandemics. It represents a successful translation of research into practice, providing a concrete solution to the challenges faced by CI operators during the COVID-19 pandemic and establishing a foundation for enhanced preparedness against future health emergencies. The full results of the second pilot phase will be documented in deliverable D4.6, further validating the tool's readiness for wider adoption and implementation.

References

- [1] **SACON Project.** Online: <https://starfos.tacr.cz/en/projekty/7D19001>
- [2] **CyberSec4Europe Project.** Online: <https://cybersec4europe.eu/>
- [3] **OLYMPUS Project.** Online: <https://olympus-project.eu/>
- [4] **SUNRISE Project.** Online: <https://sunrise-europe.eu/>
- [5] **European Commission: EU Digital COVID Certificate** Online: https://commission.europa.eu/strategy-and-policy/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en
- [6] **Slovak Ministry of Health.** Online: <https://covid.gov.cz/en/situations/vaccination/validation-applications-ctecka-and-tecka>
- [7] **ADOPSIO Project.** Online: <https://starfos.tacr.cz/en/projekty/VI04000069>
- [8] **NXP. Mifare and Mifare DESFire.** Online: https://www.nxp.com/products/rfid-nfc/mifare-hf:MC_53422
- [9] **LEGIC.** Online: <https://www.legic.com/products/smartcards/legic-smartcard-ics>
- [10] **Microchip. PIC24FJ256DA106 MCU with Graphics Controller & USB.** Online: <https://www.microchip.com/en-us/product/pic24fj256da106>
- [11] **LEGIC. RFID, Bluetooth and Secure Element in one Module.** Online: https://www.legic.com/fileadmin/user_upload/Flyer_Broschueren/SM-6300_flyer_en.pdf
- [12] **ArduCam.** Arducam Mini 2MP Plus – OV2640 SPI Camera Module for Arduino UNO Mega2560 Board & Raspberry Pi Pico. Online: <https://www.arducam.com/product/arducam-2mp-spi-camera-b0067-arduino/>
- [13] **Intel.** Intel Neural Compute Stick 2 (Intel NCS2). Online: <https://www.intel.com/content/www/us/en/developer/articles/tool/neural-compute-stick.html>
- [14] **Intel.** Intel Movidius Myriad X Vision Processing Unit. Online: <https://www.intel.com/content/www/us/en/products/details/processors/movidius-vpu/movidius-myriad-x/products.html>
- [15] **Leopard Imaging.** LI-OV5640-USB-AF. Online: <https://www.leopardimaging.com/product/usb20-cameras/5m-usb-af-camera/li-ov5640-usb-af/>
- [16] **Seek thermal.** Mosaic Core 320x240 with 4.0mm Lens. Online: <https://www.thermal.com/mosaic-core-320x240-4mm.html>
- [17] **Analog devices.** LTC1923. Online: <https://www.analog.com/en/products/ltc1923.html>
- [18] **Official GitHub Organization of the EU Digital COVID Certificates (EUDCC) project.** Online: <https://github.com/eu-digital-green-certificates>

- [19] LINDDUN privacy engineering (2020). Online: <https://www.linddun.org/>
- [20] **European Commission.** EU Digital COVID Certificate. Online: https://health.ec.europa.eu/ehealth-digital-health-and-care/ehealth-and-covid-19_en#eu-digital-covid-certificate
- [21] **Sabrina Stummer.** Privacy-Friendly European Digital Health Credentials (Working title). MSc thesis, FH Burgenland University of Applied Sciences, 2024 (ongoing)
- [22] **Jan Camenisch, Stephan Krenn, Anja Lehmann, Gert Læssøe Mikkelsen, Gregory Neven, Michael Østergaard Pedersen:** Formal Treatment of Privacy-Enhancing Credential Systems. SAC 2015: 3-24
- [23] **Fabrice Boudot:** Efficient Proofs that a Committed Number Lies in an Interval. EUROCRYPT 2000: 431-444
- [24] **Helger Lipmaa:** On Diophantine Complexity and Statistical Zero-Knowledge Arguments. ASIACRYPT 2003: 398-415
- [25] **Ronald Cramer, Ivan Damgård, Berry Schoenmakers:** Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. CRYPTO 1994: 174-187
- [26] **Jan Bobolz, Fabian Eidens, Stephan Krenn, Sebastian Ramacher, Kai Samelin:** Issuer-Hiding Attribute-Based Credentials. CANS 2021: 158-178
- [27] **Omid Mir, Balthazar Bauer, Scott Griffy, Anna Lysyanskaya, Daniel Slamanig:** Aggregate Signatures with Versatile Randomization and Issuer-Hiding Multi-Authority Anonymous Credentials. CCS 2023: 30-44
- [28] **Jesús García Rodríguez, Stephan Krenn, Daniel Slamanig:** To pass or not to pass: Privacy-preserving physical access control. Comput. Secur. 136: 103566 (2024)
- [29] **Avahi.** Online: <https://www.avahi.org/>
- [30] **TrueLife.** TrueLife CARE Q7 Blue. Online: <https://eshop.truelife.eu/en/health-care/875-truelife-care-q7-blue-8594175354911.html>
- [31] **Jesus Garcia-Rodriguez, Stephan Krenn, Jorge Bernal Bernabe, Antonio Skarmeta:** Extension of multi-signature based privacy-ABC system with commit-and-prove techniques. Computer Networks, Elsevier. 2024.
- [32] **OpenFace.** Models and Accuracies. Online: <https://cmusatyalab.github.io/openface/models-and-accuracies/>
- [33] **IMA.** Access Control Systems IMAporter Pro. Online: <https://www.ima.cz/products/access-control-systems/imaporter-pro/?lang=en>
- [34] **Solari.** Access control solutions. Online: <https://www.solari.it/solutions/other-solutions/access-control/>
- [35] **European Data Protection Board.** Statement on the processing of personal data in the context of the COVID-19 outbreak. 2019. Online: https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/statement-processing-personal-data-context-covid-19_en

- [36] **Charter of the Fundamental Rights of the European Union.** Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12016P/TXT>
- [37] **Stephan Krenn, Jan Orlicky, Daniel Slamanig, Tomáš Trpišovský:** RiBAC: Strengthening Access Control Systems for Pandemic Risk Reduction while Preserving Privacy. In Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES 2023).
- [38] **SUNRISE. D3.1** Requirements and designs V1, George Tsakirakis, 2023.
- [39] **SUNRISE. D3.2** Requirements and designs V2, Ilias Seitanidis, 2023.
- [40] **SUNRISE. D4.1** Access control conceptualization, Jan Orlicky 2023.
- [41] **SUNRISE. D4.2** Access control tool and training guide V1, Daniel Slamanig, 2023.
- [42] **SUNRISE. D4.3** Access control tool and training guide V2, Stephan Krenn, 2024.
- [43] **SUNRISE. D4.4** Access control pilot report V1, Tomas Trpisovsky, 2024.

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

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 be concerned 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 account of 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 account of 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, particularly where the data subject is a child.

Clearly, 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, 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, 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) [35].

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 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).

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 two 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). In Article 4(11), the GDPR defines consent as "any **freely given, 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".

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.¹

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 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 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,

¹ 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" [36].

- (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.

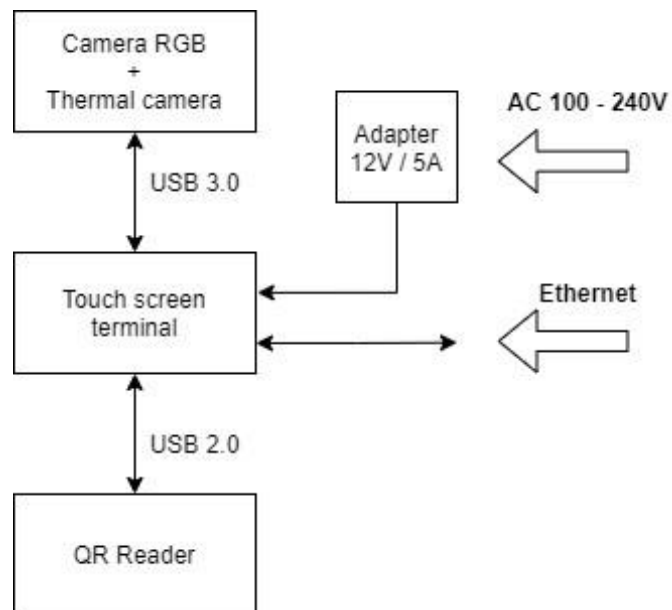
Consent expresses the will of the data subject, identifies the person to whom it is addressed and can therefore be objectively **considered an agreement**. The requirement to freely give consent is derived from a principle of civil law, and no circumstances must be created which would render consent 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 to ANNEX I of this document.

Annex III – RiBAC Tool User guide for CI operators

RiBAC Terminal

General Schema

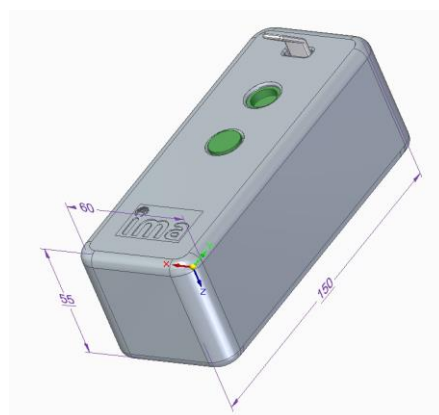


Technical Composition



Technical components:

Camera module



RGB camera

Optical sensor format 1/2,8"
 Sensor resolution 2 Mpx
 Sony IMX291 sensor
 Viewing angle 100°, Manual, fixed focus

Thermal (IR) camera

Resolution - Active Pixel Array 320H x 240V
 Pixel Size 12µm x 12µm
 9 Frames per Second

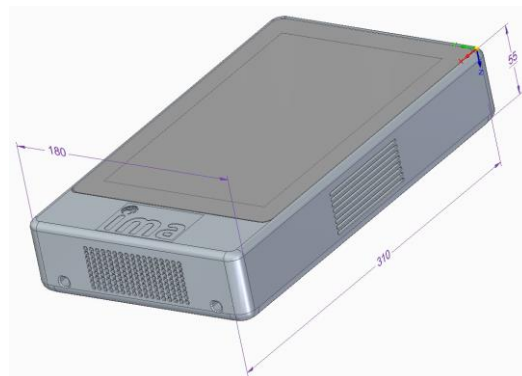
Temperature reference

Reference point 10x10 millimetres
 Thermal emissivity ϵ 0,95
 Calibrated reference temperature 37,3 °C
 Module is powered by USB – 5 V, 0,5 A max.
 Dimensions (w/o temperature reference) – H x W x D 150 x 60 x 55 millimetres, (D 75 millimetres with temperature reference)

Recommended operating conditions:

Face distance approx. 0.5 – 1 metre
 Whole face must be in the measured area (the area scanned by the thermal camera)
 No part of the face must be covered by the temperature reference
 It is necessary to avoid direct sunlight

Touch screen terminal



Function description

Basic function

- ▶ The camera constantly monitors the defined area and identifies faces.
- ▶ The user approaches the terminal.
- ▶ User checks the display to see if the camera has recognised it.
 - Whether he is visible on camera and his face is framed by a rectangle
 - If not, you need to move closer or further away from the camera
 - The ideal face-to-camera distance is 50 to 100 cm
- ▶ The display shows the requirements that must be met within the time interval
 - RFID card attachment
 - body temperature measured on the forehead
 - respiratory protective mask fitted
- ▶ The status of each request can be monitored on the display
- ▶ If all conditions are met, the **green light** is displayed, and the relay is switched on.
- ▶ In case the time runs out, a **red light** appears, and the **user is required to start over**.

Features for the pandemic period

The basic function can be supplemented by specific requirements for the pandemic period

- ▶ Temperature check - measured on the forehead
- ▶ respiratory protective mask check
- ▶ Vaccination passport check
- ▶ Automatic sending of control results (detected parameters) to the centre
- ▶ Direct link of control results to permission/disallowance of entry to the object

Installation Guide

The following provides brief guidelines regarding the installation of the RiBAC terminal.

Terminal Design and Measures



Figure 58: The RiBAC terminal

The RiBAC terminal is supplied with a camera module and a QR code reader on the stand.

- o The stand consists of 30 x 30 mm bars with 4 grooves of the AC 30-6 shape
- o A 4mm Allen key is needed to adjust the tilt in the joint

The precise measurements of the RiBAC terminal are depicted in the following figure.

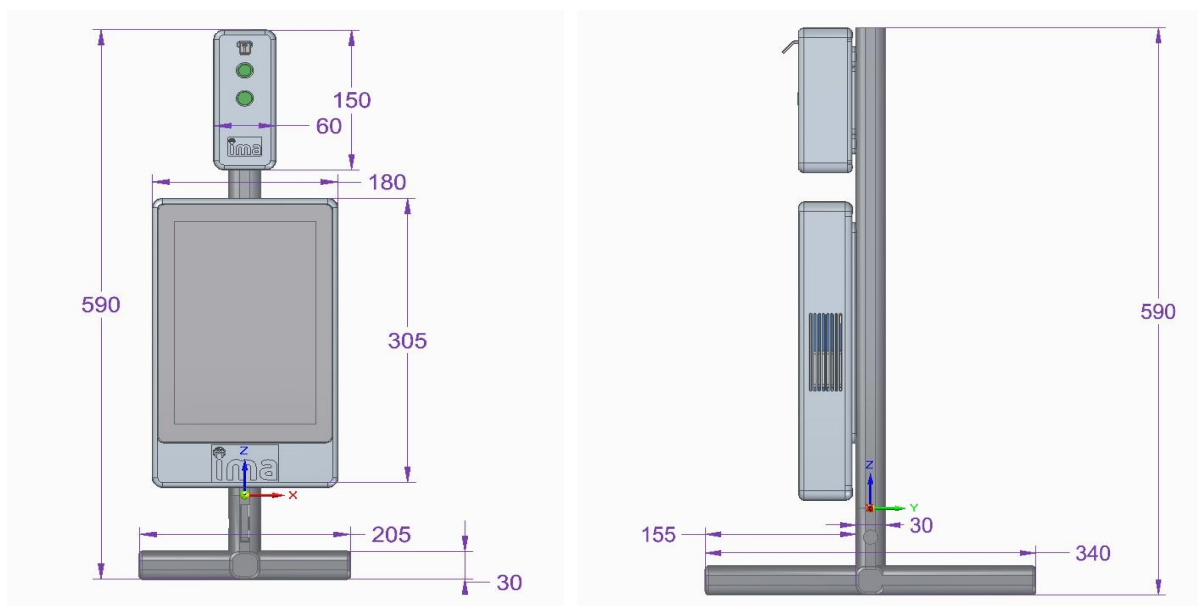


Figure 59 : Measurements of the RiBAC terminal (front and side view)

The stand has a joint at the bottom, so the angle of the terminal can be changed.

A 4mm Allen key is needed to adjust the tilt in the joint

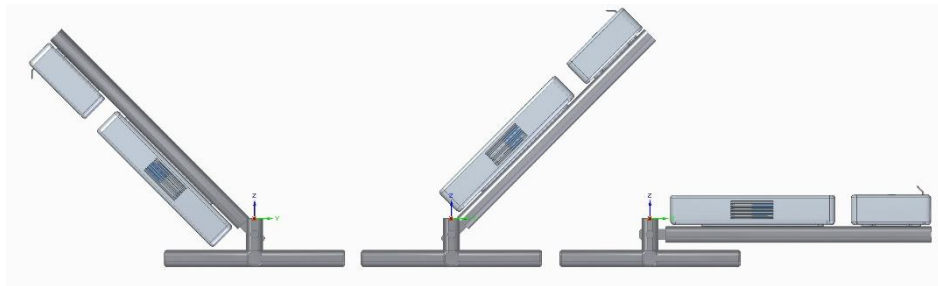


Figure 60: Different positions of the RiBAC terminal

Positioning of the Terminal

Location of the terminal stand.

The position of the terminal needs to fulfil certain requirements. Specifically:

- ▶ The terminal must be located indoors.
- ▶ Avoid placing in direct sunlight.
- ▶ It is assumed that the stand is placed on a table or similarly high base.
- ▶ Space in front of the terminal at least 2 m so that a person can stand in front of it.

No space is needed behind the terminal.

Alternative terminal location

If you require a wall mounted terminal, please contact IMA. Currently, we anticipate delivery on racks.

Connections

The terminal requires the following external connectors:

- ▶ AC socket 100 to 240 V
 - Included DC 12 V / 5 A adapter
 - Power input 60 W
- ▶ UTP cable with RJ45 connector with internet access
 - Connecting the cable to the Ethernet connector in the terminal

Commissioning

To activate the terminal, the following steps are required:

- ▶ the terminal is placed on the table,
- ▶ the adapter is connected to the 230 V socket
- ▶ the Ethernet data cable is plugged into the terminal
- ▶ the terminal starts up and can be used.

Terminal Configuration

Configuration of the RiBAC terminal is made easier with a web-based configurator available to users. This approach allows the configuration of the terminal not only via a computer using a web browser, but also from a mobile device. In this way, the user does not need to be physically present at the device to perform the configuration.

RiBAC's web-based terminal configurator provides users with a convenient interface for setting up their devices. After entering the IP address into the web browser, a dialog box appears that requires a

username and password (see Figure 61). This step ensures configuration security by restricting access to authorized users only and preventing unauthorized access to device settings.

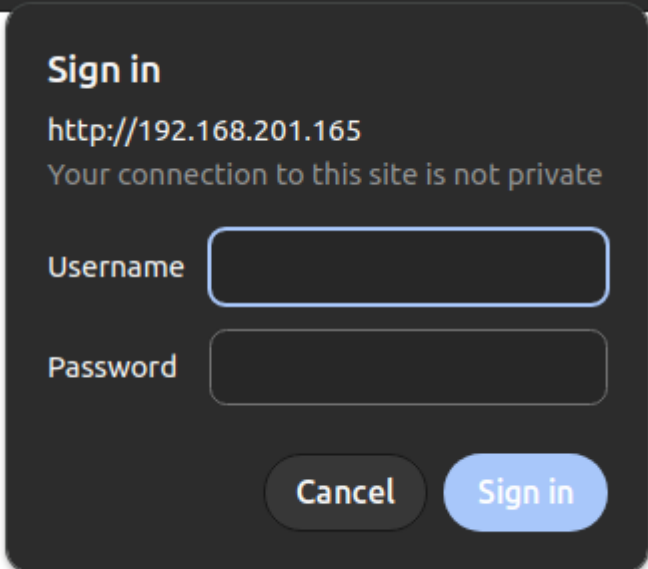


Figure 61 : Password entry (default values are described at the end of the paragraph)

After successfully entering the correct username and password, a screen containing configuration parameters that can be changed on the terminal is displayed (see Figure 62). This screen gives the user clear access to various settings and configuration options. Users can easily modify the parameters according to their needs and preferences. In this way, the RiBAC terminal configuration process is intuitive and flexible, contributing to a comfortable user environment and efficient use of the device.

After successfully entering the correct username and password, a screen containing configuration parameters that can be changed on the terminal is displayed (see Figure 62). This screen gives the user clear access to the various settings and configuration options. Users can easily modify the parameters according to their needs and preferences. In this way, the RiBAC terminal configuration process is intuitive and flexible, contributing to a comfortable user environment and efficient use of the device.

CONFIGURATION

CARDS

Parameters

Max. temperature (°C)

37.5

Check timeout (ms)

5000

☐ Attendance mode

☐ Check RFID

☐ Check covid pass

☐ Check BT authentication

Network

☒ DHCP ☒ Wi-Fi hotspot


 **SAVE**

Figure 62 : Terminal configuration

Configuration parameters:

Max Temperature: specifies the maximum temperature the terminal can measure and allow the user to enter.

Check Timeout: Specifies the maximum amount of time the user has to meet all conditions for admission. It also specifies the amount of time that the relay is active after all conditions have been met.

Attendance Mode: This parameter determines whether the terminal behaves only as an attendance terminal. In this mode, it is sufficient to insert a valid card contained in the list of allowed cards. In pandemic mode, when this parameter is not active, checking the temperature and wearing a mask is mandatory. In addition, other modules can be enabled in this mode, which must be fulfilled.

Check RFID: In addition to the temperature and wearing a face shield, the user must also attach a valid identification card.

Check Covid pass: in addition to temperature and wearing a veil, the user must show a valid vaccination certificate.

Check BT authentication: in addition to the temperature and wearing a visor, the user must authenticate with the app on the phone.

Network options:

It is also possible to change the network parameters of the terminal using the web interface. If DHCP is disabled, the terminal can be set to a static IP address (see Figure 63). It is also possible to enable a Wi-Fi client that connects to a predefined Wi-Fi network. After a successful Wi-Fi connection, the IP address of the terminal that was assigned by the Wi-Fi router or mobile hotspot is displayed in the lower left corner of the display. This allows easy configuration of the terminal using a web browser on the mobile device.

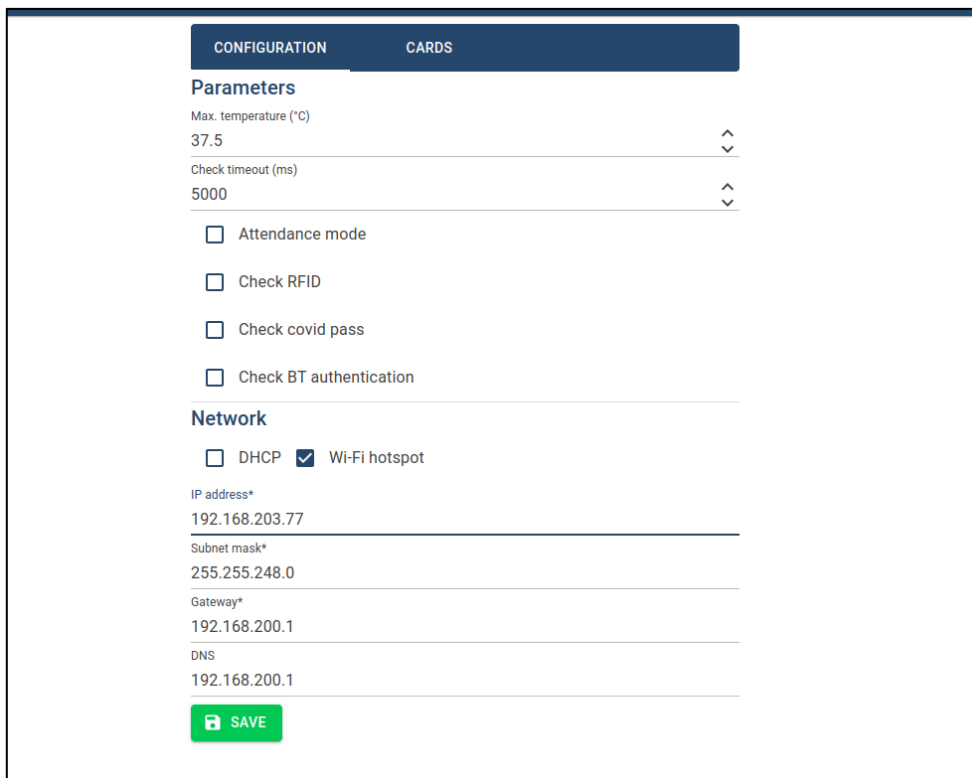


Figure 63: Static IP address

List of cards:

Users can upload a list of valid cards via the web interface of the terminal. In the "Cards" tab, the current valid card list is displayed, and a new card list can be uploaded. This process is done via a .csv file where each line corresponds to one valid card (see Figure 64). In this way, users are provided with an easy and efficient way to manage the list of authorised cards, which contributes to the secure operation of the RiBAC terminal.

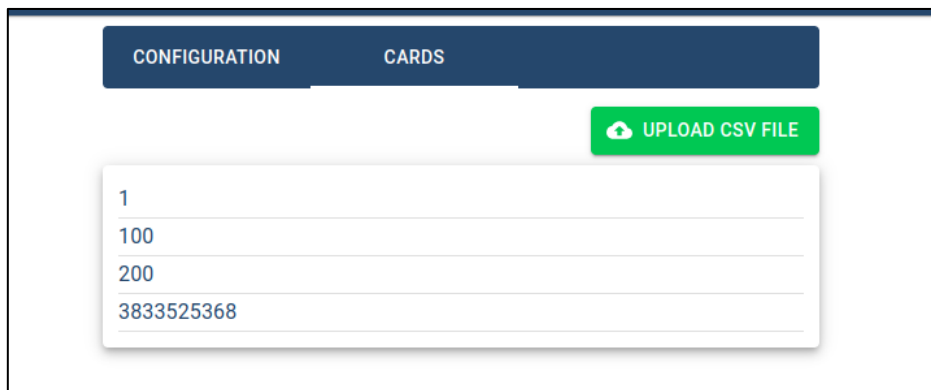


Figure 64: Uploading cards

Saving the configuration:

Parameter configuration and card upload to the terminal is done in real time, which means there is no need to restart the terminal. This dynamic and instantaneous change allows users to quickly and efficiently modify the terminal settings without interrupting its operation. This ensures smooth and uninterrupted operation of the RiBAC terminal even when configuration adjustments are being made.

Predefined parameters

The terminal will be supplied by the setup:

- ▶ Attendance mode
- ▶ DHCP
- ▶ Username: RiBAC
- ▶ User password: RiBAC5478921
- ▶ SSID: RiBAC
- ▶ Wifi password: RiBAC5478921

Pilot installation

Tested functions

- ▶ RiBAC off-line
- ▶ RiBAC on-line

Testing procedures

- ▶ Individual functionality test of RiBAC technical elements
 - IR camera
 - RGB camera
 - terminal
 - QR reader
- ▶ Functionality test of the entire RiBAC technical assembly in a pilot installation environment prior to on-site assembly of the local application
- ▶ Verification of IMA remote management functionality
- ▶ Test all functions of the installed RiBAC terminal in the local environment

Time schedule of tests

- ▶ Test all functions of the RiBAC terminal before expedition
- ▶ Checking all functions of the RiBAC terminal after delivery to the site before starting the local installation
- ▶ Checking all functions of the RiBAC terminal after installation on site
- ▶ Checking the correct and complete assembly and commissioning of the terminal by remote IMA connection

Tests protocols

All tests mentioned in the previous paragraphs will be documented in protocols and archived for the overall evaluation of the project.

Troubleshooting instructions a fault or problem in operation

Some of the most frequent possible problems when installing or deploying a RiBAC terminal are described below, together with possible mitigation strategies. In case any other issues emerge, or the proposed solutions do not work, users are encouraged to directly contact IMA.

The display goes off, but the fans are still audible.

- ▶ The display can put itself into power saving mode. This is controlled in the terminal software, but it can still happen on rare occasions.
- ▶ Touch the display, if it does not light up within a few seconds, the whole terminal is switched off.
- ▶ Restart the terminal by disconnecting it from the power supply.

The terminal shuts down suddenly

- ▶ Check the power supply
- ▶ Check that the device is not overheated. If so, let it cool down.
- ▶ Check if the fans are audible when the terminal is switched on.
- ▶ If the fans are not audible, contact IMA.

The screen does not show the video from the camera, but a static image.

- ▶ Restart the terminal by disconnecting it from the power supply.
- ▶ Check that all cables are connected correctly.

Only a black screen with text is visible.

- ▶ Restart the terminal by disconnecting it from the power supply.

The terminal does not start when connecting to power.

- ▶ Wait, startup may take a while.
- ▶ Check that the 230V socket is functional (circuit breaker off, etc...).
- ▶ In case of any other problem, please contact IMA.

Remote Support

All terminals are equipped with remote access for IMA to the local installation for remote management and diagnostics purposes.

To this end, the terminals are integrated into the IMA VPN, which is activated when connected to the Internet. Thanks to this network, the administrator can remotely manage the terminals. The terminal can be connected to the Internet either via an Ethernet connection or via a Wi-Fi hotspot. In this way, the administrator can monitor the status of the terminals, perform diagnostics and make remote adjustments or repairs if necessary.

Terminal Interface User Guide

In idle state, a welcome screen is displayed, shown on Figure 65.

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.

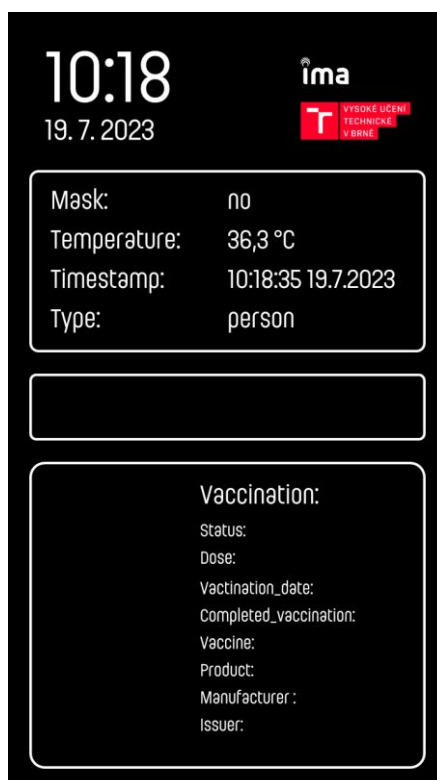


Figure 65: Application home screen

The terminal then displays a list of the required protective equipment that are required to be worn by the user (Figure 66).

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

[illegible]

Figure 66: List of required protective equipment

Once all the required equipment has been detected, the terminal returns 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, a message instructs the user to attach their RFID card (or other identifier) to the access control module.

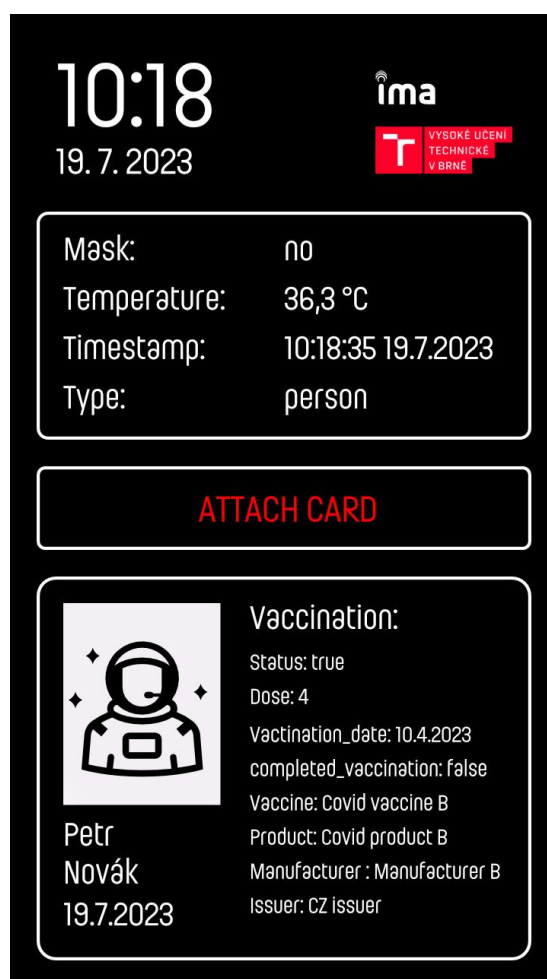


Figure 67: Terminal screen after successful detection of protective equipment

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 receives “access not granted” message (Figure 69).

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 is then shown on the display (Figure 68). Otherwise, the user is rejected (Figure 69).

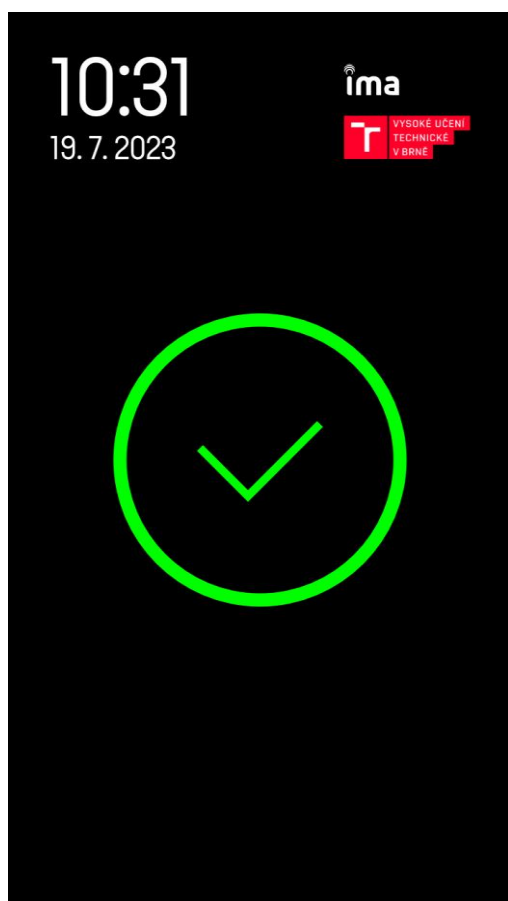


Figure 68: Access granted

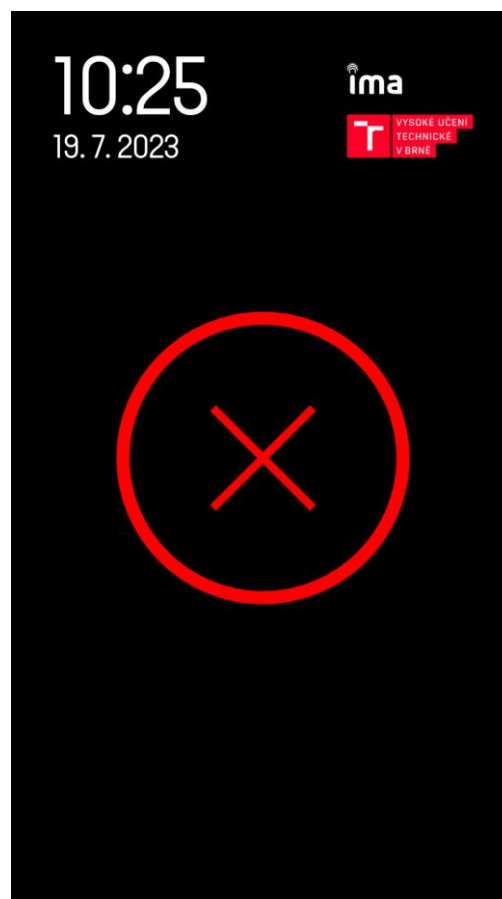


Figure 69: Access not granted

Example scenario flow

The following steps provide an overview of an example scenario flow. On a high level, though operating sequentially, the flow follows the “parallel” architecture blueprint developed in D4.1 [40] and by Krenn et al. [37]:

Scenario – Basic functionality of RiBAC tool

Steps

- ▶ **Step 1:** A user wishing to enter a facility approaches the terminal.
- ▶ **Step 2:** The user is guided in front of the terminal.
- ▶ **Step 3:** The risk-based extensions of the terminal are activated. Specifically, the user’s temperature, protective tools, and vaccination credential are checked by the appropriate extensions (e.g., camera).
- ▶ **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:** The 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 9:** An access decision is being made:
 - If user has corresponding access rights and meets all required conditions, they are granted access.
 - If the user does not have corresponding access rights and/or does not meet all required conditions, they are denied access.
- ▶ **Step 10:** Display screen corresponding to the outcome of the previous step is shown to the user.
- ▶ **Step 11:** In case of a positive outcome, the corresponding access point (door/turnstile/etc.) is opened.