

SEKEYRITY

P I C I Access Management

Bruna Ferreira

Miguel Ameixa

Miguel Andrade

António Ribeiro

Afonso Coelho

João Barros



TÉCNICO LISBOA

P R O B L E M D E F I N I T I O N



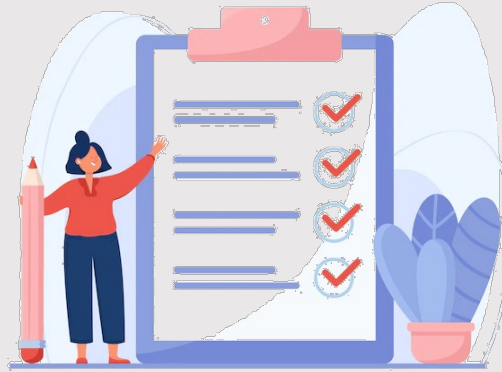
We realized that accessing NEEC (Núcleo de Estudantes de Engenharia Eletrotécnica e de Computadores) rooms in the North Tower was a **slow, outdated process** that severely depended on security guards' surveillance

P R O B L E M D E F I N I T I O N

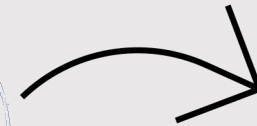
C U R R E N T P R O C E S S



Users request keys from the security guard at the tower's reception.



The guard manually checks a long list of accesses and records key transactions manually

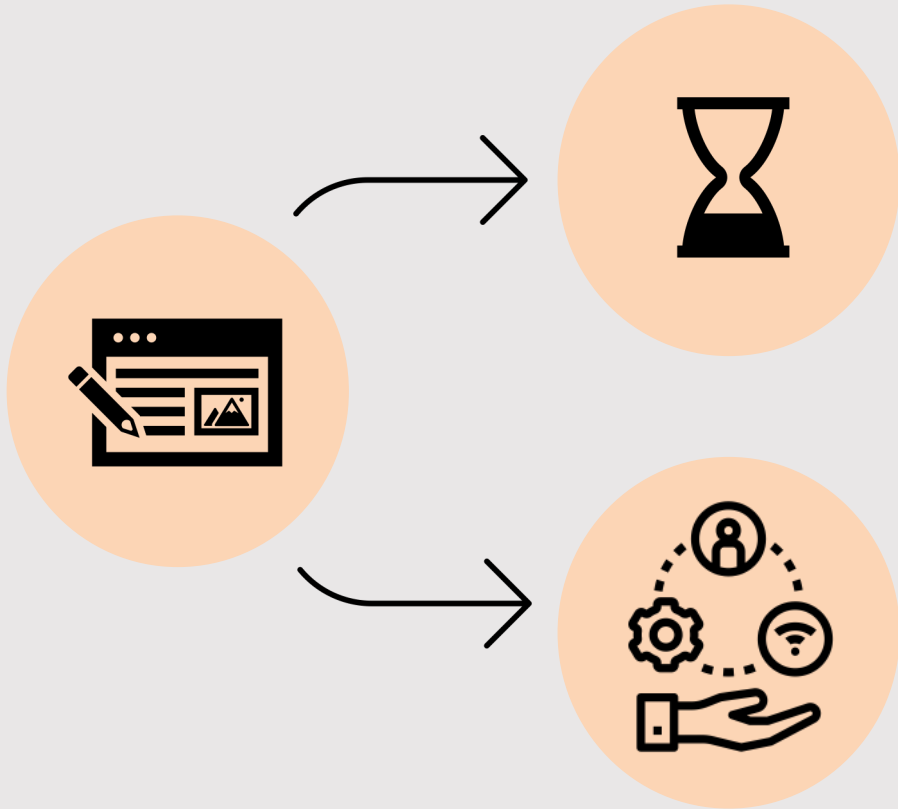


The key must then be returned by the user after leaving the respective room

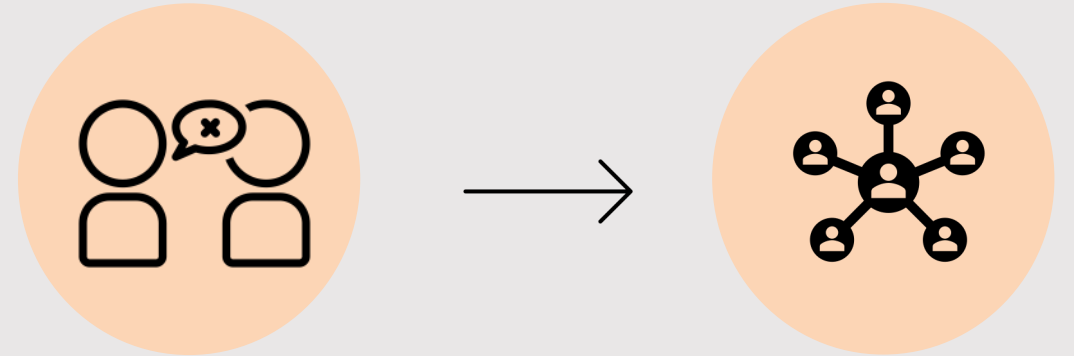


PROBLEM DEFINITION

IDENTIFIED PROBLEMS

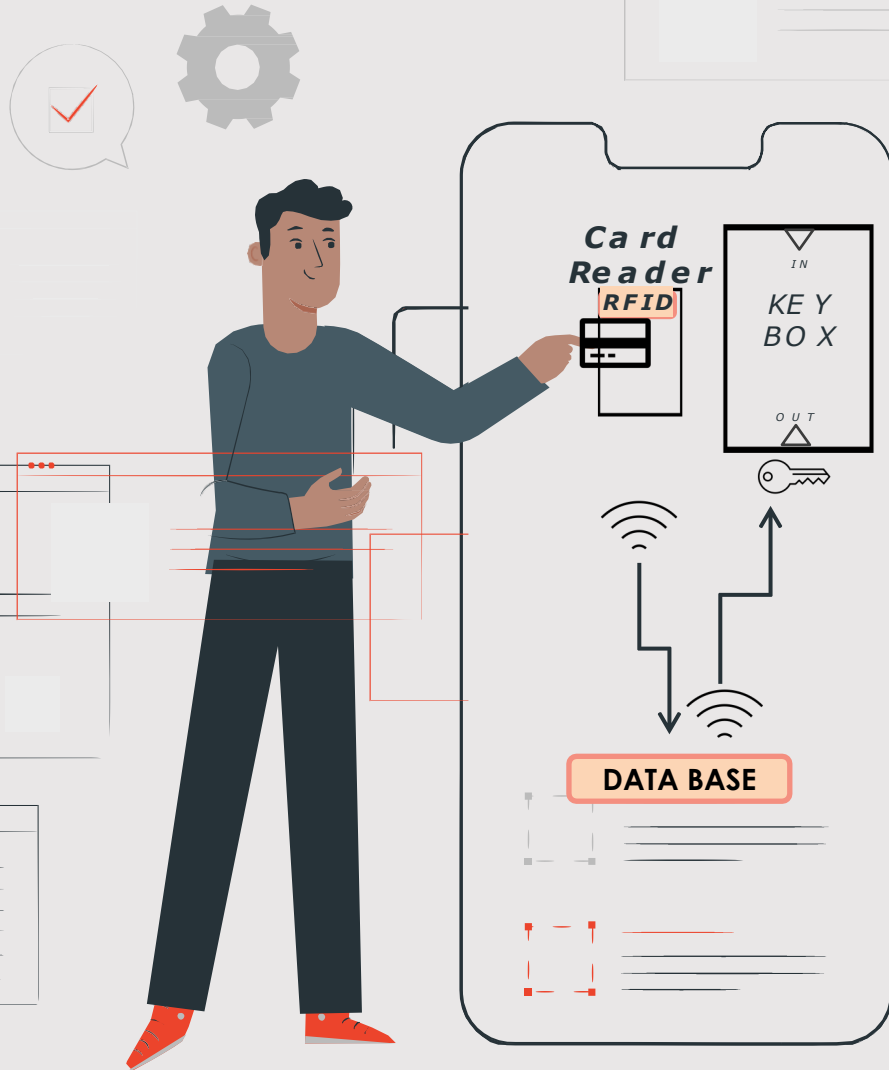


The manual process leads to inefficiencies and unnecessary time and resource allocation



Variability exists among guards regarding key return policies, causing confusion and inconvenience for users. Forgotten key returns also result in issues for both users and security staff.

TECHNOLOGICAL SOLUTION



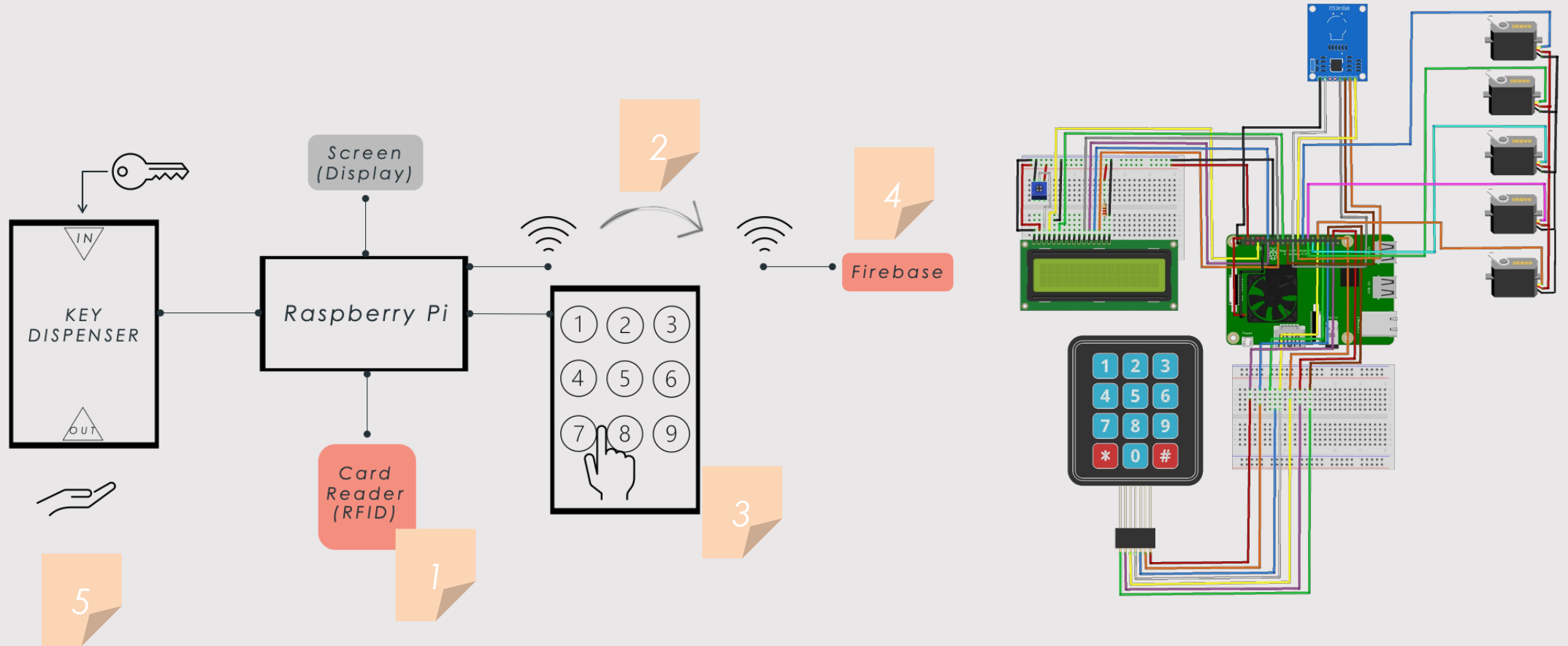
SEKEYRITY

A key box with a card reader system that operates by accessing a centralized database that contains information about access privileges for each user, and delivers the keys accordingly.

TECHNOLOGICAL SOLUTION



HOW IT WORKS (KEY REQUEST)



TECHNOLOGICAL SOLUTION



HOW IT WORKS

1

When a **user interacts with the card reader**, they swipe their card, which is associated with their profile in the database

2

After scanning the card using **RFID technology**, the system **communicates with the database in real-time** to verify the user's identity and access permissions.

3

The user **interacts with the keyboard** to input the number of the desired key.

4

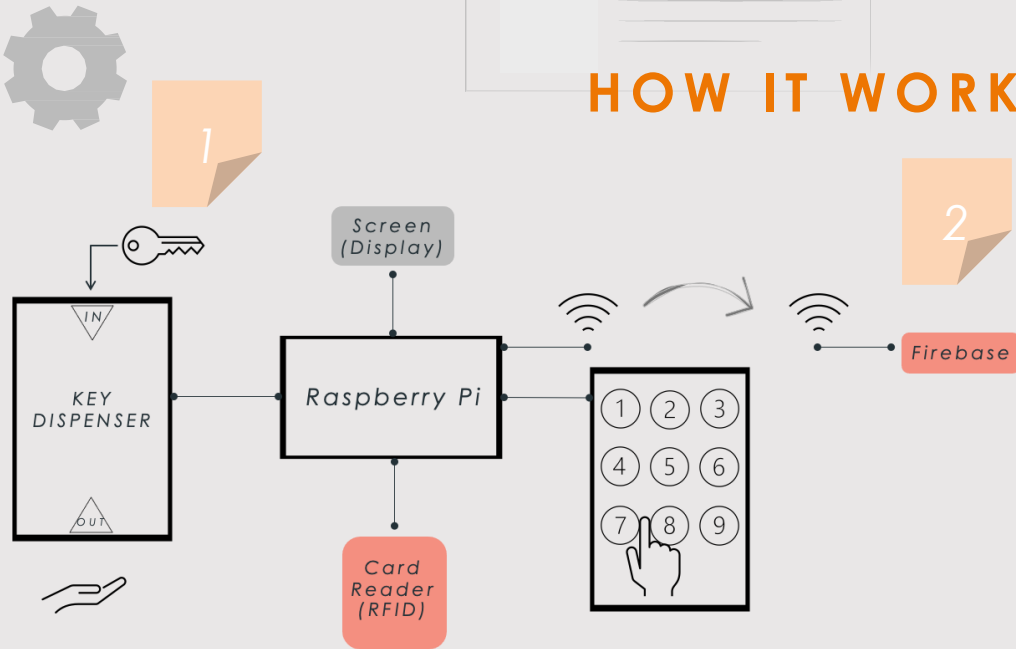
The database indicates if the **user is granted access** to the selected room or area, or, conversely, if the **user does not have the necessary access privileges**

5

According to the information received from the database, the system either **immediately authorizes entry and activates the release mechanism** for the corresponding key or **denies entry and prevents the key from being released.**

TECHNOLOGICAL SOLUTION

HOW IT WORKS (KEY RETURN)

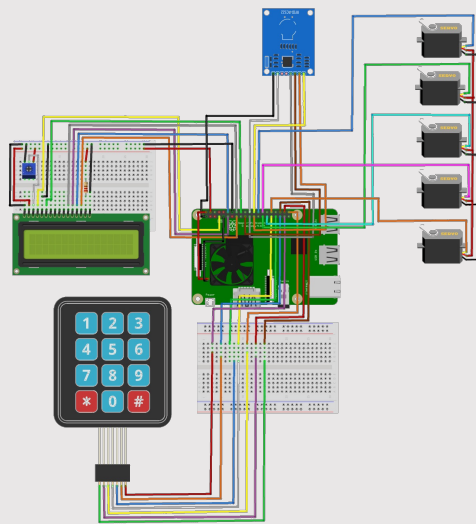


1) When a **user returns the key**, to ensure the delivered key is correct, we use the same RFID reader employed for card identification to ensure the correct key is delivered.

2) The system verifies in the database if the user returning the key has access to it.

A) If they do, the key is marked as returned, and servos move it to its designated place inside the box.

B) If the key is not recognized, the user does not have access to it, or it is an unknown object, the key is rejected.



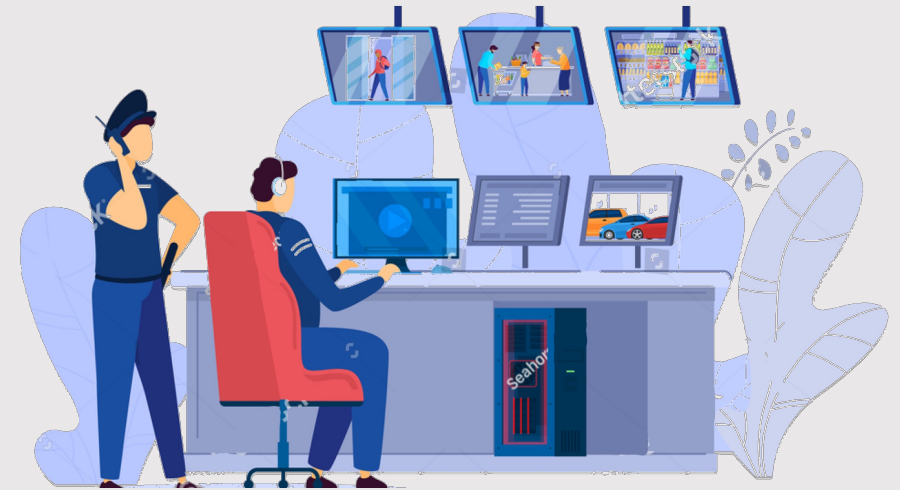
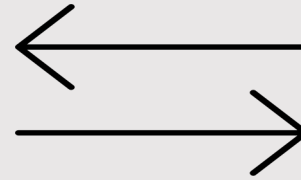
SOLUTION BENEFICIARIES

Implementing an automated key and access management system would provide tangible benefits to multiple beneficiaries.



STUDENTS, TEACHERS, AND STAFF

would experience streamlined access processes, reducing administrative burdens and improving efficiency.



SECURITY PERSONNEL

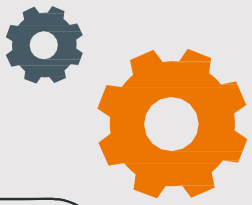
would benefit from enhanced monitoring capabilities, gaining better control over access permissions

COMPETITORS AND PREVIOUS WORK

SMART LOCK

In the domain of access control and management solutions, one prevalent alternative in the market are **smart locks**, offered by established entities such as **iLockey, Allegion Plc, and Onity, Inc.**

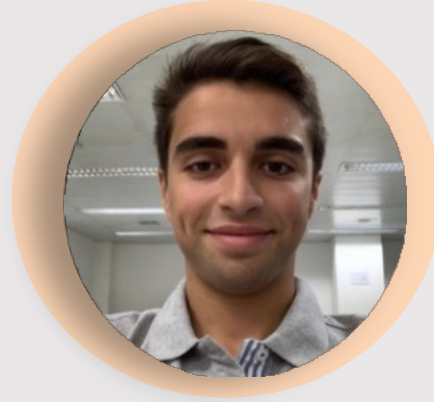




MEET THE TEAM



BRUNA FERREIRA



MIGUEL ANDRADE



AFONSO COELHO



ANTÓNIO RIBEIRO



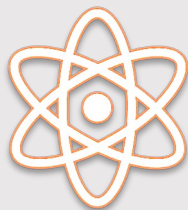
MIGUEL AMEIXA



JOÃO BARROS



ADVISORS AND MENTORS



**Prof. Luís Caldas
de Oliveira**

Scientific Advisor



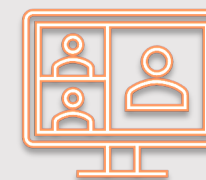
**Prof. Marko
Beko**

Scientific Co-
advisor




**Prof. Luís Caldas de
Oliveira**

Coordinator



**Rafael
Cordeiro**

Mentor



Achieved Results

WEB APP

Miguel Andrade and Bruna Ferreira designed a platform that serves as a **multifunctional tool**;

USERS

ADMIN

Register

Grant access

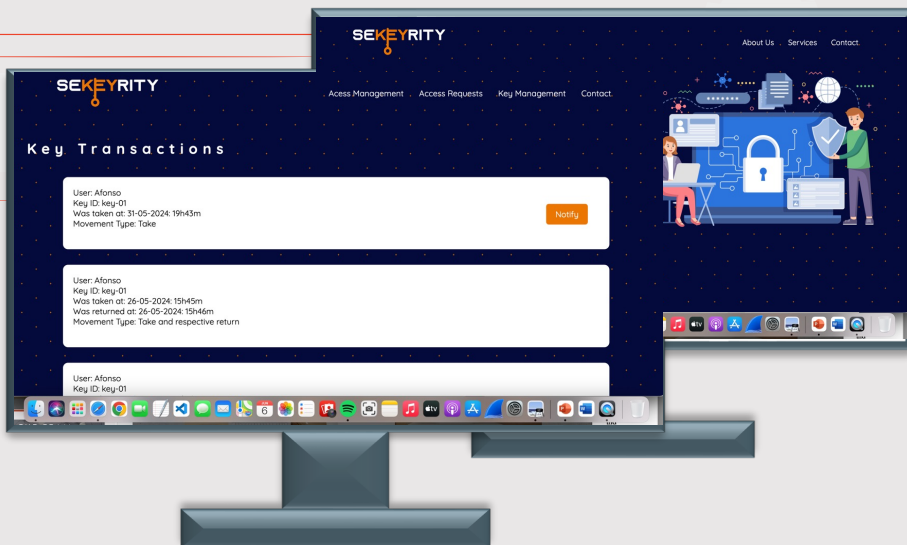
Log in

Deny access

Request access to
keys

Monitor key status

Notify users

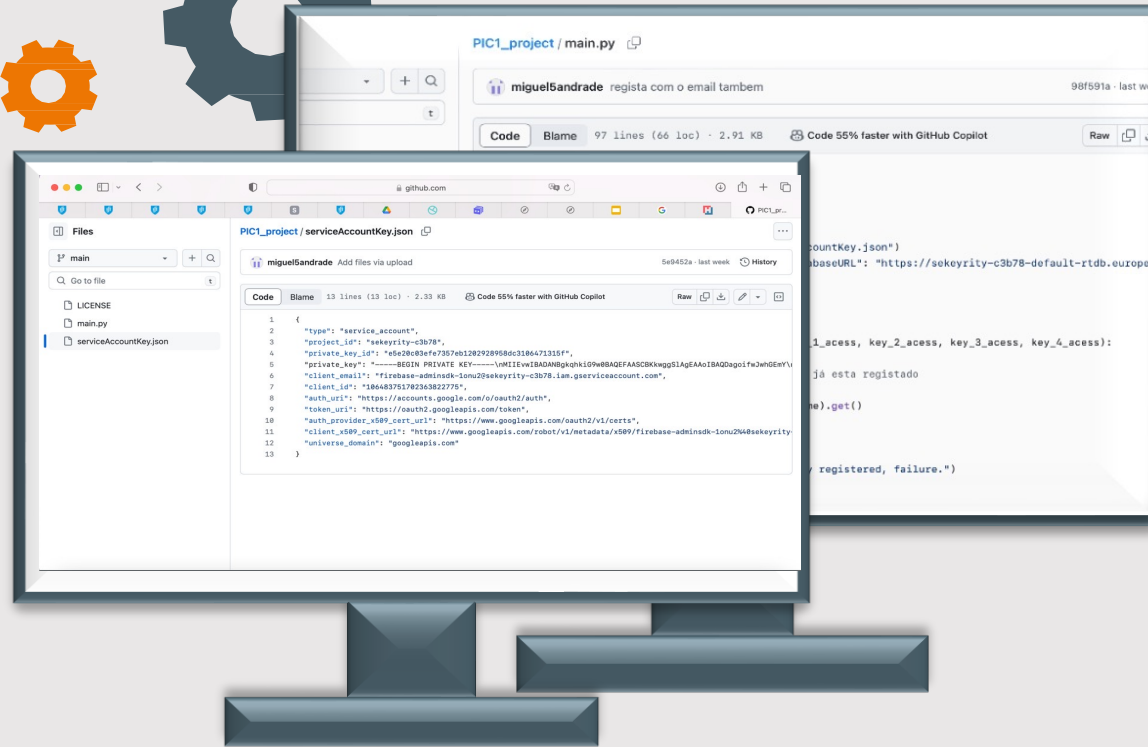


ACHIEVED RESULTS

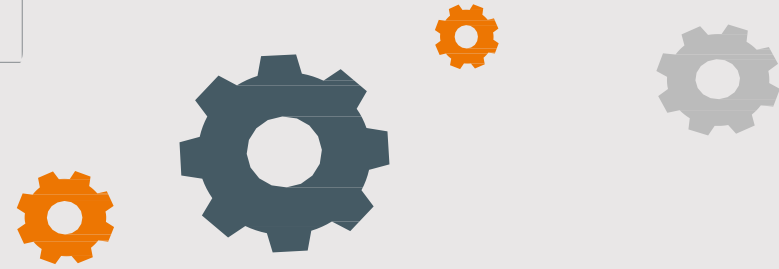
DATA BASE

Miguel Andrade created an **on-line DataBase** using Firebase, where we store **registered users**, along with **their information and the keys they have access to.**

Lastly, we implemented a feature that **registers key movements**, so the admin has access to the information of whoever took and/or returned each one of the keys.

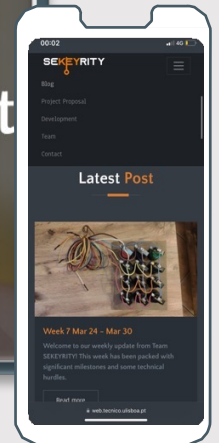
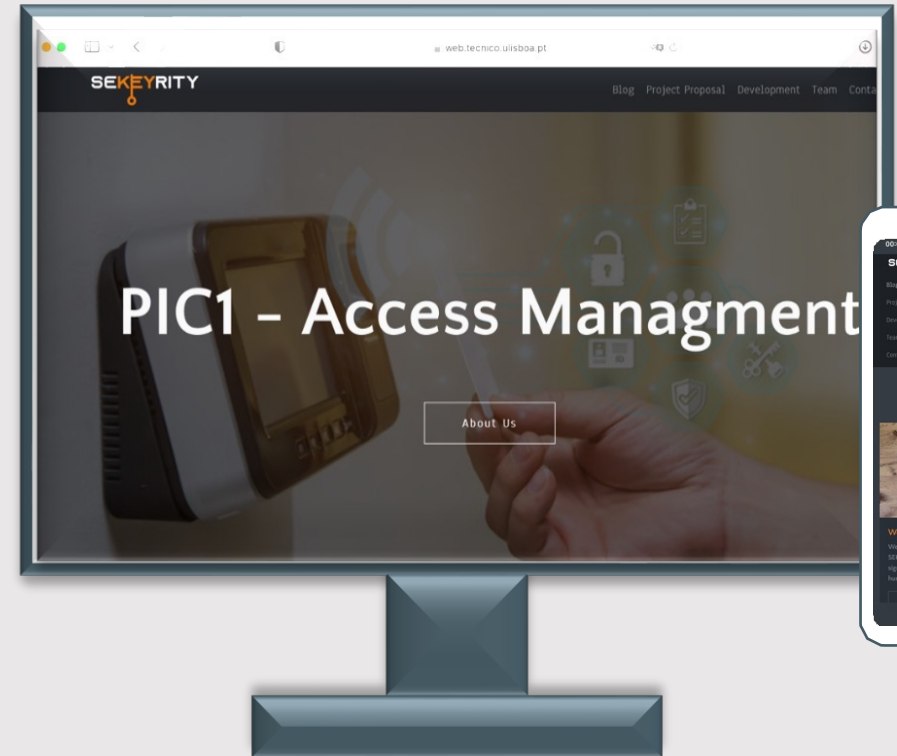


A C H I E V E D R E S U L T S



WEBSITE + PROJECT BLOG

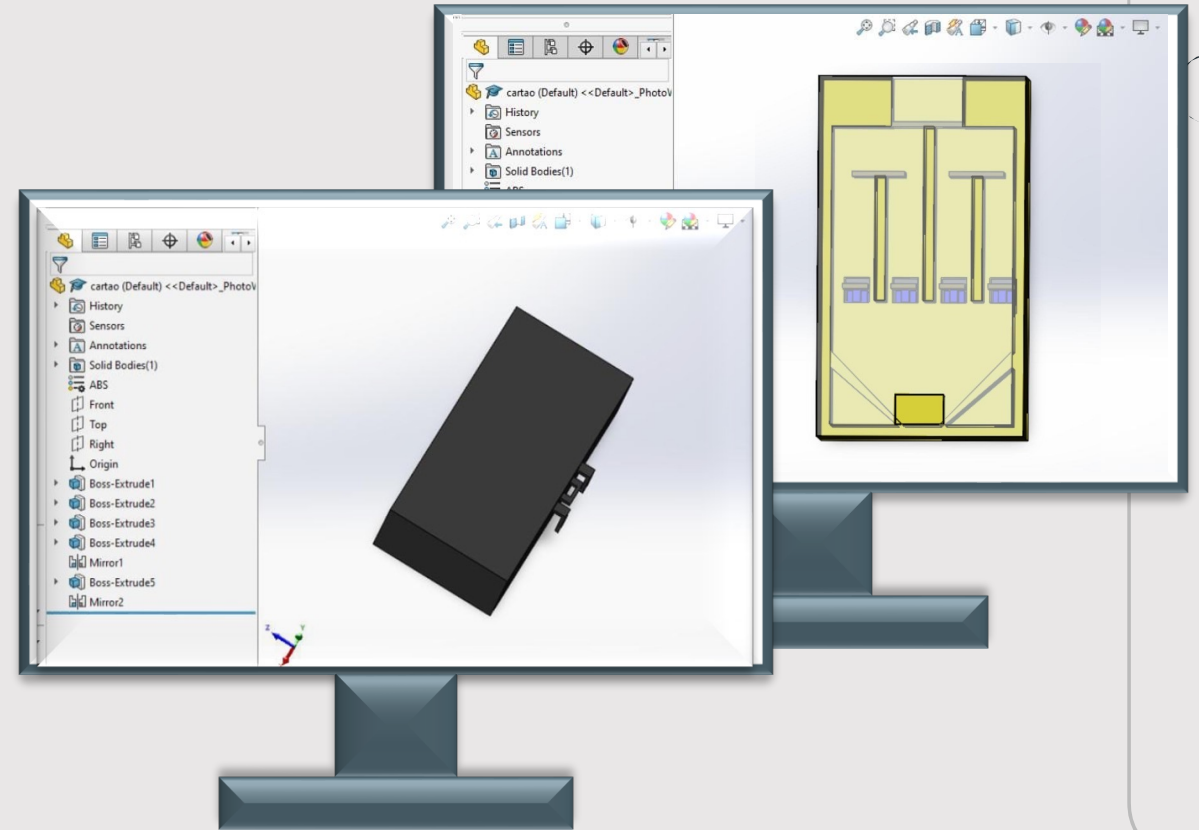
Bruna Ferreira and Miguel Ameixa designed and launched a **public website** to centralize project information, encompassing our **project proposal** and **weekly blog updates** regarding our project's progress.



A C H I E V E D R E S U L T S

3D M O D E L I N G

João Barros 3D modelled the **servo barriers**, which was a crucial step in our project. Due to the specific nature of the servos we were using, we needed **extreme precision** to ensure the correct functioning of the mechanism



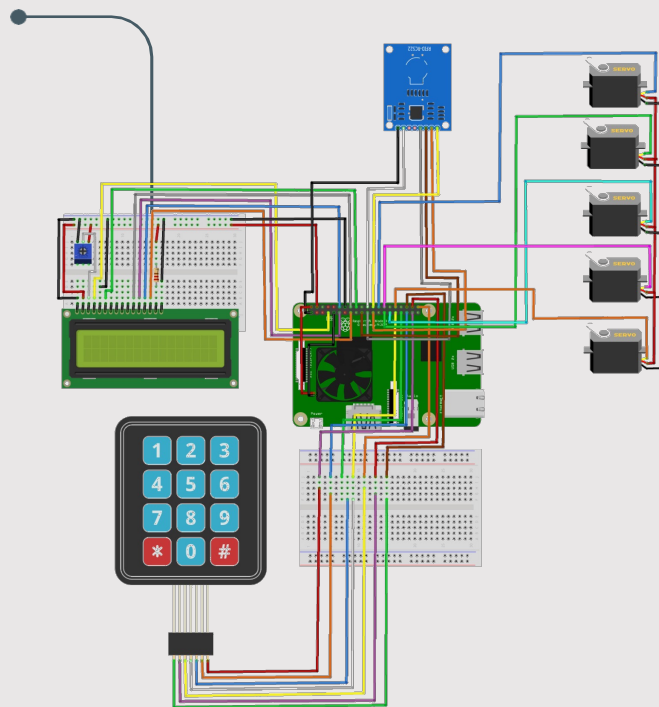
A C H I E V E D R E S U L T S



HARDWARE (1/2)

At the hardware level, Afonso Coelho used a **Raspberry Pi**, connected to a **RFID reader** that reads the users' card IDs.

We implemented features so that after reading the card, it **accesses our database** (Firebase) and if the user is not registered, the **display prompts for registration**.

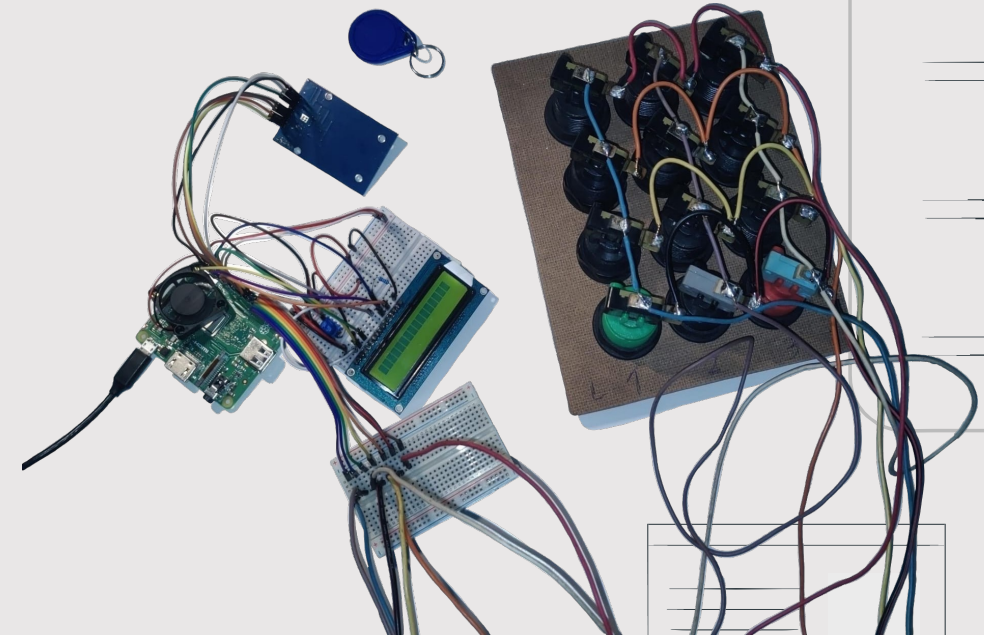


A C H I E V E D R E S U L T S

HARDWARE (2/2)

For the **key acquisition** process we use a **numeric keypad**, made by Afonso Coelho, to identify which key the user wants to acquire, and the key is given to the user by **servo movement**.

For **key returns**, to ensure the delivered key is correct, we use the same **RFID reader** that was used for cards **to identify which key was returned** and place it correctly also using **servo movement**.



A C H I E V E D R E S U L T S

HARDWOOD STRUCTURE

António Ribeiro, Miguel Ameixa, Afonso Coelho and João Barros all participated in the **building of a wooden structure** to hold the keys.

The box has **multiple levels**: the top **for key insertion**, the second for **servos distributing keys**, the third for **key storage**, and the lower levels for **key retrieval** and housing the Raspberry Pi and other components. It features a front door with a magnetic lock and an acrylic panel for visibility. The servos and components are connected to the Raspberry Pi for **centralized control**.



FINAL PROTOTYPE RESULT

AUTOMATIC STORAGE

When a key is retrieved, the reader identifies the key number and moves the platforms so that the key is stored in the correct place.

NO NEED FOR SUPERVISION

Automatically detects if it's the right key. If the user inserts something it gets rejected.

AUTONOMOUS DISPENSER

The selected key will be dispensed automatically.

SIMPLE USER INTERFACE

The user is given instructions through the LCD screen.

MANUFACTURED KEYBOARD

Easy and intuitive to choose keys.



TEAM MEMBERS' CONTRIBUTIONS

BRUNA FERREIRA

Blog, WebApp and Communication

MIGUEL ANDRADE

Data Base and WebApp

AFONSO COELHO

Hardware

Website Design and Maintenance

Development of Data Base

Configuration of Raspberry Pi

Write weekly Blog Updates

Interface between Hardware and Software

Development of keyboard

Mid-program Pitch Deck

WebApp Design and Implementation

Establish hardware components connection

WebApp Design and Implementation

Demo Day Poster

Demo Day Poster

Pitch Deck Final Presentation



TEAM MEMBERS' CONTRIBUTIONS

ANTÓNIO RIBEIRO

Structure and Design

MIGUEL AMEIXA

Electronics

JOÃO BARROS

3D Modelation

Logo Design

Website Maintenance

Key Locker Design

Key Locker Prototype Structure

Publish Weekly Blog Updates

Key Locker 3D Modelation

Establish Hardware Components
Connection

Servo movement

Key Locker Prototype Structure

Demo Day Video

Demo Day Video

Production Cost Evaluation

Demo Day Video



COSTS AND BENEFITS

WHY CHOOSE SEKEYRITY



Our solution is faster, safer and more efficient than the current manual process. Especially in case of unauthorized access



The production cost of our product is **114€**, which is much lower than other solutions on the market, having in mind that it serves, at least, 4 different keys/locks and requires minimal to no infrastructure changes for implementation



Most smart locks in the market have a limit of 1000 users, while our prototype has no fixed limit of users.

FUTURE WORK

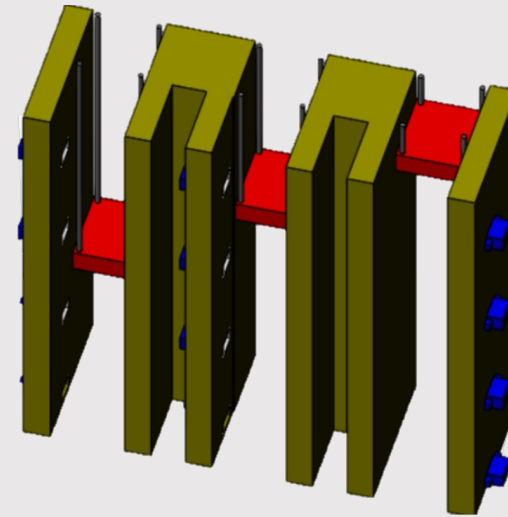
WHAT'S NEXT WITH SEKEYRITY

- **Redesign the dispenser to hold more keys:**

If we use the same method for more keys, the dispenser will become exponentially larger.

- **Obtain permission to access the IST user database:**

This will enable us to implement the solution for the identified problem of accessing rooms in the North Tower.



TÉCNICO
LISBOA

IMPORTANT LINKS

KEEP UP WITH **SEKEYRITY**

[Project Landing Page](#)

[Project Blog](#)

[Project Video](#)



WebApp