



**POLITECNICO  
DI TORINO**

# Project and Laboratory on Communication Systems: Secure Pass

Group 9 - Final Report

Authors: Edoardo Mazzella, Luca Mocerino,  
Ramon Messinetti

POLITECNICO DI TORINO, A.Y. 2016/2017

# Problem

## Why *SecurePass* ?

Security has been one of the most controversial topics for the last few decades, in particular in the computer science field. Considering security as the possibility to guarantee a secure access to a private and protected environment, the main problems are:

- Classic authentication system (username + password) is easily hackable;
- In a work environment, a badge based system to access the office does not guarantee the real identity of the person;
- Working frauds are commonplace;
- An autonomous access to a protect environment (houses, condominium, etc.) by a limited group of people is not easy without a human surveillance;

Currently all these problems are not addressed by a unique, secure and integrated application. For this reason, our proposal is SecurePass.

*In our project as case of use, we have developed a system that allows employees to access their work environment. The other problems mentioned above are easily addressed by this technology and its system architecture.*



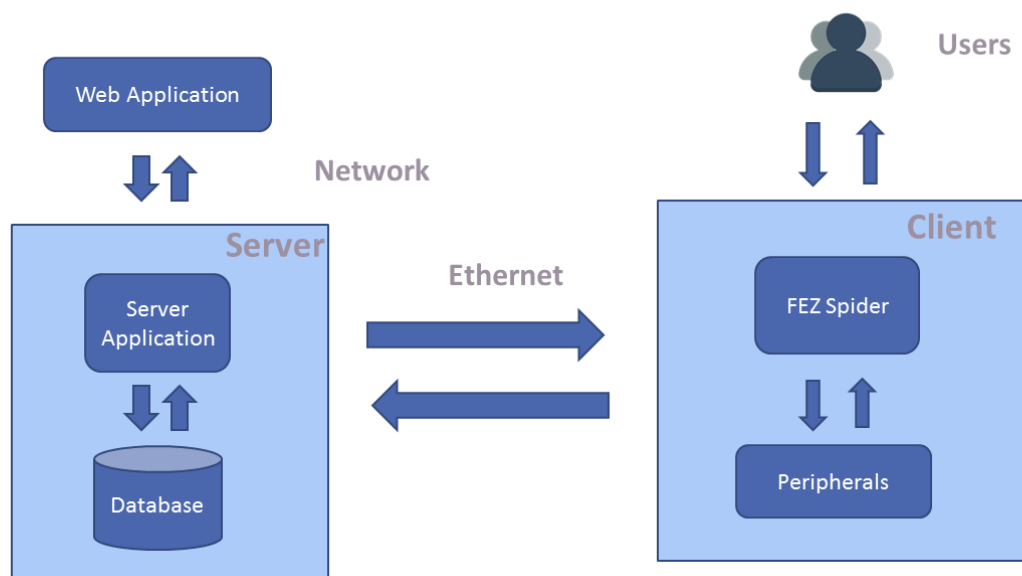
# Solution

## What is *SecurePass*?

The product developed during the course is called **SecurePass**.

SecurePass is:

- A product in charge to handle secure access to every kind of private and protected environment;
- The way to protect your company or your house using a **double key verification**;
- A client-server, web based application.



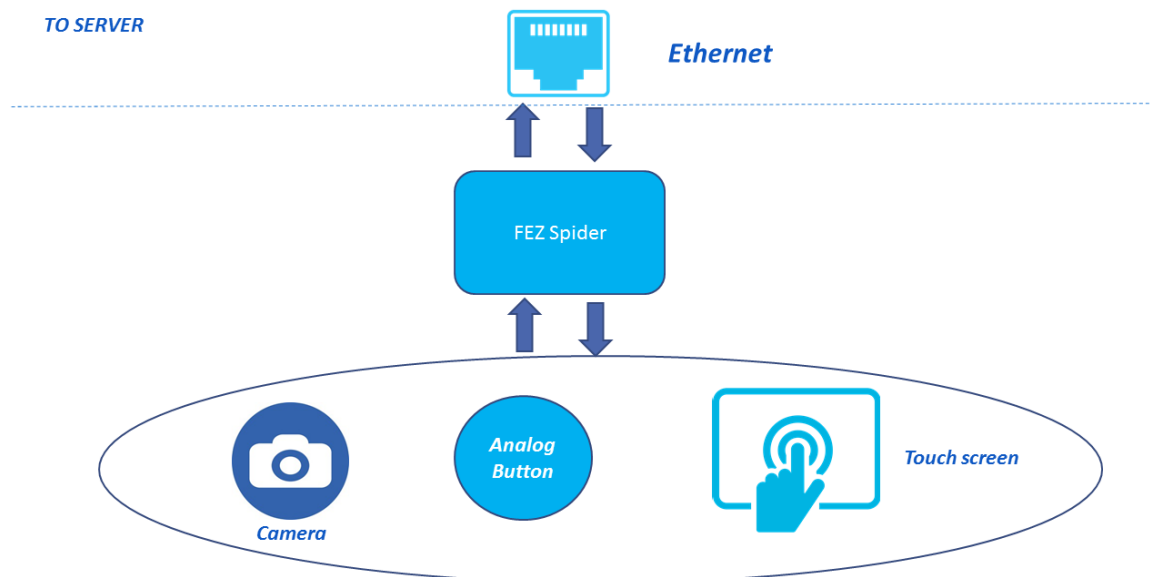
**Figure 1:** System overview

The **SecurePass** system is composed of three key elements:

- Client using FEZ Spider and its peripherals (ethernet cable, camera, user button and a touch screen);
- Server that manages the access to the database and the Microsoft Face API web service;
- A web site intended to manage and check the user and the timetables of the users

# Knowing *SecurePass*

## Client Side

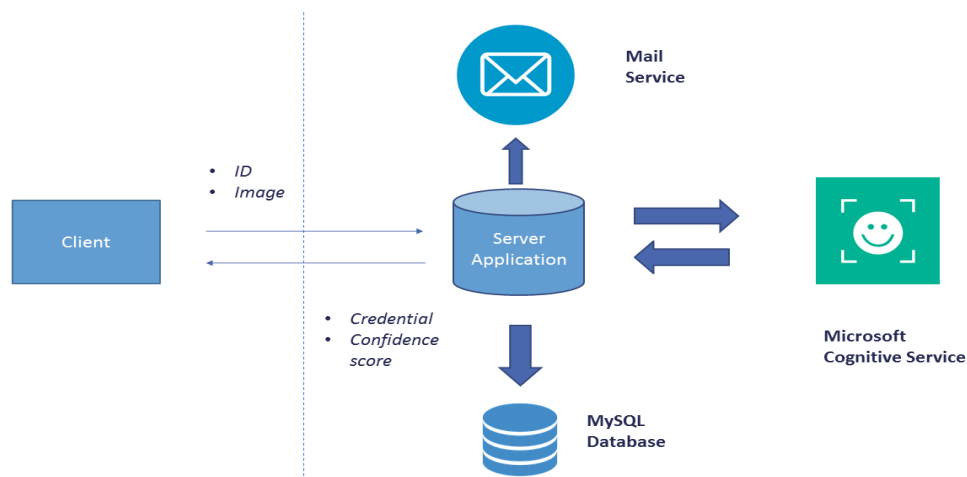


**Figure 2:** Client

This client interface allows the user to:

- Insert the unique identifier through touch screen interface;
- See the camera streaming on the screen;
- Press the button to take the photo;
- Send the photo to the server through ethernet.

## Server Side



The server provides the following services:

- TCP/IP connection client-server
- Database management (employee credential and image, timetable for each employee)
- Request to Microsoft Cognitive Service<sup>1</sup>, for matching the image from camera with one sample stored in the database.

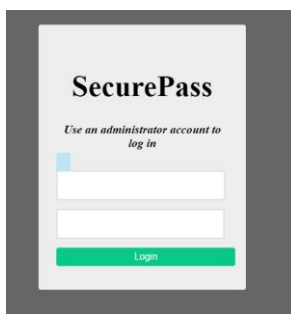


**Figure 4:** Face matching examples

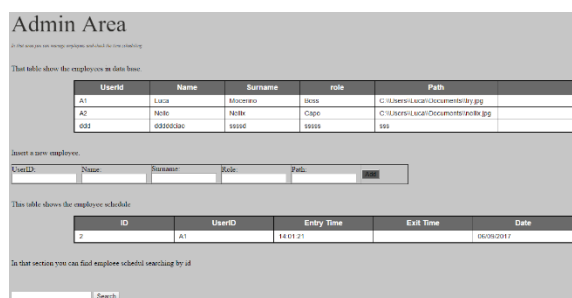
- When the maximum of matching attempts are reached (3 in our case) an email is sent to the system administrator with the attached log file of the system (user credential and timestamps)

## Web site

In order to manage the employee's credentials and photos a web site is available:



1. Log in with admin credential



2. CRUD user and view exit/entry time

<sup>1</sup> <https://azure.microsoft.com/it-it/services/cognitive-services/>

# SecurePass: How it works?

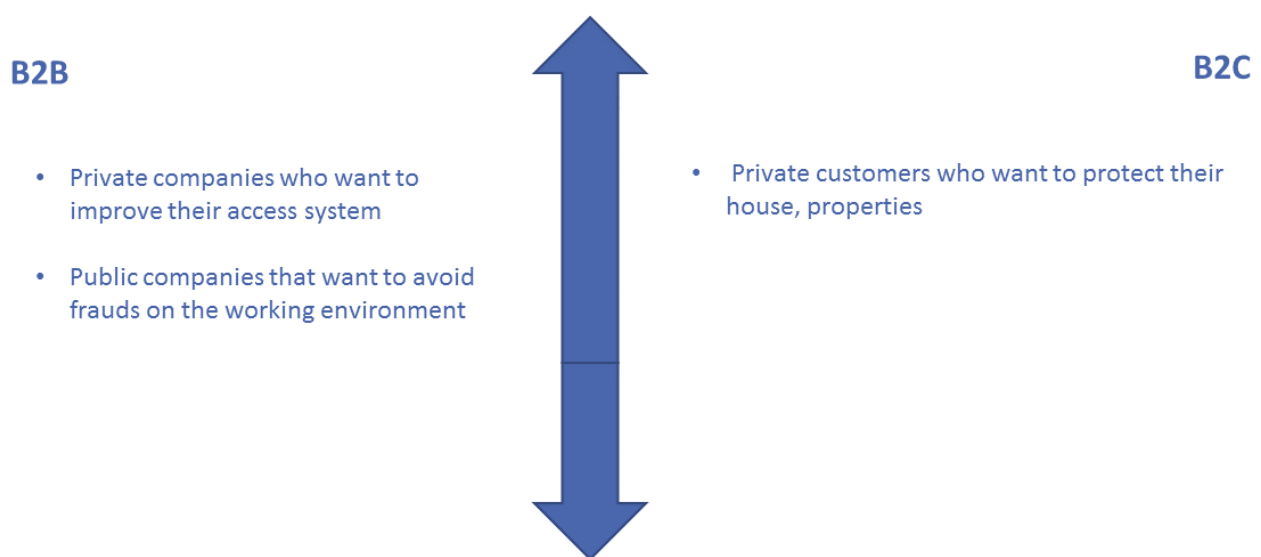
## Use case: Employee access

Let's see a typical case of use in the work environment.

1. The employee inserts using the GUI on the touch screen its unique ID provided by the system administrator and stored in the database;
2. The system checks if the identifier matches a real employee in the system database;
3. After that, employee credentials are showed on the screen;
4. Now the employee takes a photo pressing the user button framing its face for matching;
5. The face is sent to the server that, using the Microsoft Cognitive service matches that photo with the sample stored in the database
  - a. If the confidence coefficient is higher than a certain threshold, the user can access to the environment and the entry/exit<sup>2</sup> time is stored in the database;
  - b. If the two photos don't match, the user can retry for 3 times: after that the system send an email to the administrator with the system log file.

## SecurePass on the market

After having showed what SecurePass is and how it works, it is necessary to analyze the market prospects of such a product. Similar solutions are provided as the research works. The main possible market targets are illustrated in the following graph:



---

<sup>2</sup> The system can distinguish between entry and exit time

The cost for the prototype is:

- Fez Spider Kit used (LCD, button, camera, ethernet): 150 \$
- Microsoft Cognitive Service: 41,50 \$ per month

Total cost: **191 \$**

**N.B.** *The final product does not include the same hardware of the prototype. A lower performance CPU could achieve the same results. Another key point is the production scale (greater the scale lower the hardware cost) and the cost on the server side for Microsoft API can be splitted among several users.*

No direct competitors are on the market. In the following table, there is a comparison with similar products (security systems with face recognition):

Product	Multiple cameras support	Face Recognition	Other validation keys	Notifications (repeated access)	Price
<i>Face recognition by Axis Communications</i>	Yes	Yes	No	No	250€ per camera
<i>WV-ASR500 by Parasonic</i>	Yes	Yes	No	No	On request
<b>SecurePass</b>	No	Yes	<b>YES</b>	<b>YES</b>	150 \$ <sup>3</sup>

## *SecurePass: Why?*

### Why choose us?

The key points that make **SecurePass** a unique product are:

- Double key verification makes the difference;
- Integrability with management systems;
- Email notification when too many attempts are done;
- Solution scalability;
- Cost reduction.

---

<sup>3</sup> Estimated cost for one camera client-server application