A-Pass

A Tech platform for a secure return to work
after COVID-19 confinement situations

ICT
June 2020

INDEX

Context

In March 2020 the Spanish Government, with the support of the Congress, established the State of Alarm as provided for by the Spanish Constitution, in order to restrict the mobility of people to try to slow down the infection rate of the new SARS-CoV-2 virus that causes the COVID-19 disease, which was rapidly starting to saturate the countries' public health systems.

Mobility restriction measures impacted on every sector of the economy, including the production of goods and services and working life to different degrees throughout the different State of Alarm extensions, with a peak on mobility restriction during the two weeks between March 30th and April 9th, in which only essential activity was permitted.

Similar situations were observed in other countries and handled with similar measures by their Governments.

Due to this, Acciona created a Crisis Committee in early March and a Crisis General Management by end of March to coordinate internal and external initiatives in Health, Security, Prevention, Human Resources, IT, Communication and Business activities, with the unique goal of safeguarding the integrity and health of every employee, and maintain the continuity of our activities depending on the situation and evolution of the situation in each sector and country.

One of those activities nurtured in the Crisis Committee and fueled by the Crisis General Management was the creation of a tech platform that would help us control the return of workers to Acciona's workplaces following the guidelines of relevant authorities.

Premises

A series a premises were mandated and assimilated into the design principles:

- Establish a permanent alignment with Acciona's different protocols for COVID-19, with special focus on the Responsible Health Declaration
- Flexibility to onboard employees, but also external workers and contractors, either national or international
- Adaptability to frequent protocol changes, which derive from the growing knowledge in the community on the traits of both SARS-CoV-2 and COVID-19
- Maximum respect for the privacy of the users of the platform, even beyond the minimum legal requirements sanctioned by privacy directives in the countries in which we have activity
- Strict security in the treatment of information and in the access to it

The platform

The platform consists of two different mobile applications, a web application, an identity management service and API accessed backend services for all of them.

A-Pass is the end user application. It handles the daily Responsible Health Declaration and communicates with the backend services to update the information and receive a passport, which the user can show to security personnel on premises to get secure access to the workplace. It's also designed to handle notifications and messages to those that have symptoms, had close contact with infected people or have tested positive for COVID-19.

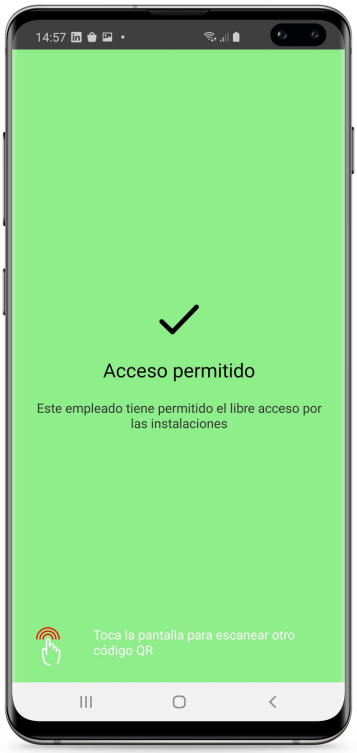
A-Pass Security is the scanning application used by the security personnel to verify that the passport shown by a user willing to access the premises is valid. It offers some other features: it can add send a signal to the backend if the user's body temperature scan is positive (above a certain temperature dictated by the protocols) and it can help onboard users that don't have a mobile phone or check a user's passport even if he forgot his mobile phone at home using the user's National ID.

The web app is the working tool for the Medical, Human Resources (HR) or Occupational Safety and Health (OSH) staff. The medical role allows our medical staff to input the results of relevant medical tests (PCR, IgG/IgM, others) and even edit the passport status of users. They can potentially use the web app to track users who have tested positive or declared to have symptoms, depending on the privacy sensibility and the protocols in use. The HR view helps HR workers manage sick leaves and act on the users' passports without needing to know about their health condition. The OSH view helps OSH staff manage passports of workers on sites that don't have an easy access to medical staff with none or very restricted access to sensible information.

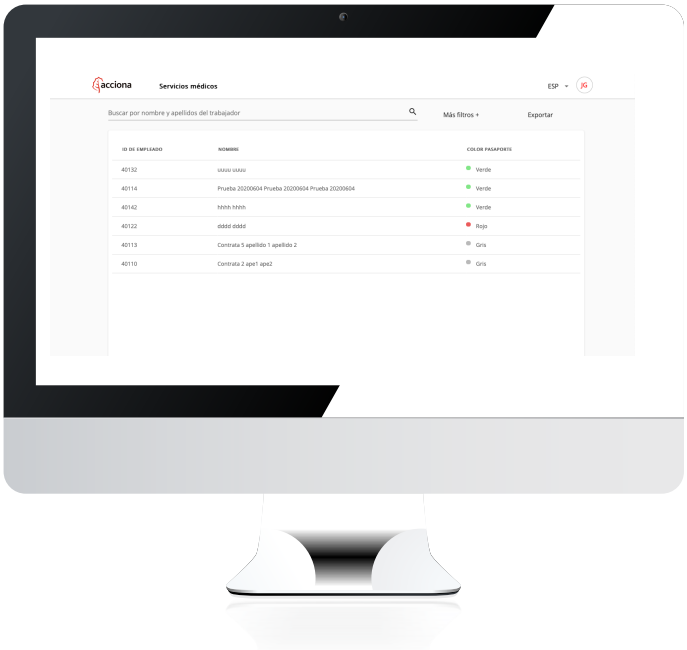
The Identity Service manages the onboarding of users into the platform, as well as the authentication and authorization of users into the different apps. It relies on the corporate identity service for authentication of users that already have a corporate account (which ensures single sign-on and MFA capabilities) and manages its own authentication for users that don't.

The WEB API exposes the backend services to the apps. Those backend services are responsible of generating the passports for each user, calculating health states (which are only managed by the medical staff in the web app), assigning passport colors (which are then used by the A-Pass Security app to decide whether a user could enter the premises or not), etc. Integration with other systems or validation of onboarded users is also managed by these services (HR employee lists or contractor user lists are uploaded periodically)

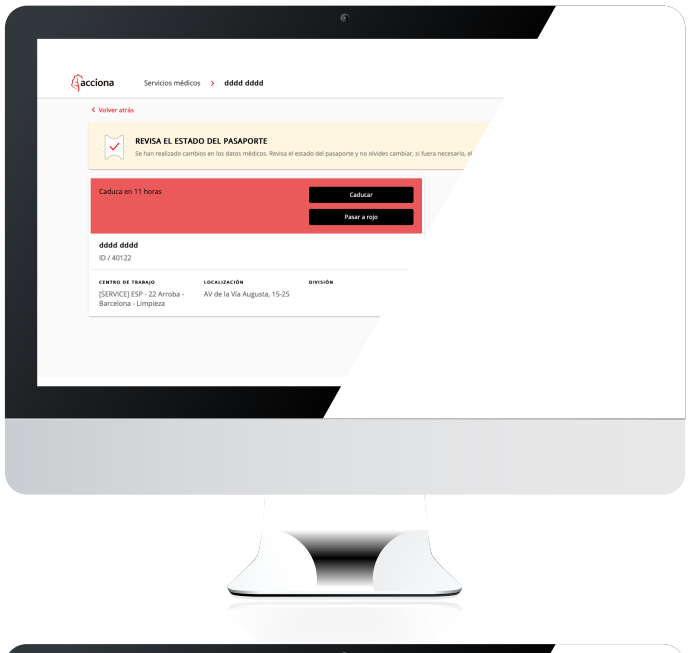
A-Pass



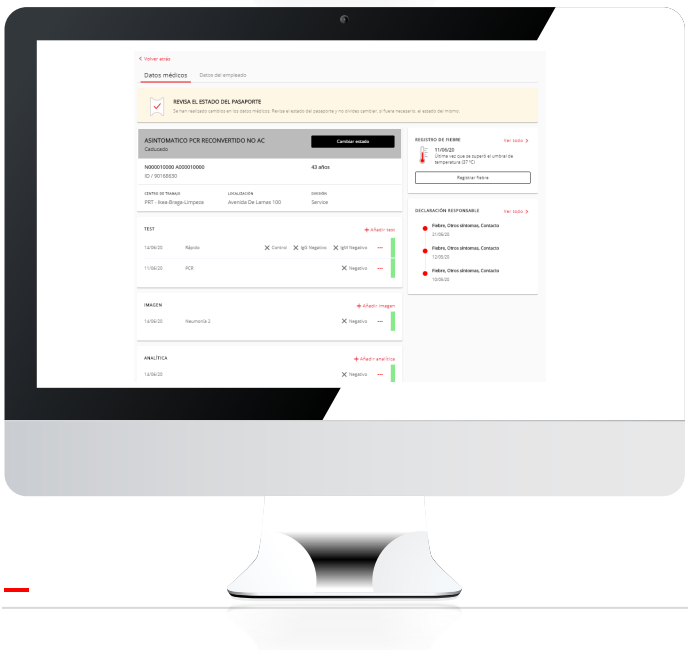
A-Pass Security



→ Web app



→ OSH view



→ Medical view

A-Pass

As stated before, A-Pass is the end user application. It's available in English and Spanish. A process will show if newer versions of the app are available and will force the download if that version is mandatory or will just let the user select to download it if the version is just recommended.

User interaction starts with the onboarding process, which is handled by the Identity Service and will be explained later. This process takes place just once.

Once the user is registered in the system it can login to be able to send Responsible Health Declarations (RHD) and receive his passport, which will show a scannable QR and will turn the back color of the app either green (Access allowed) or red (Access denied)

Acciona's protocols mandate that every user should renew their RHD daily, and that users should renew it before commuting to work. Thus, when the RHD expires (at the end of the day) the back of the app will turn grey, and will remain so until the user clicks on the "Renew statement", which will generate a new RHD and passport and turn the back of the app green or red in accordance to the user's new and previous info.

If a passport is not expired, a local copy is held in the app just in case the user's device loses connection when trying to access Acciona's premises. Passport information is encrypted and held to a minimum. The copy will be expired by the system at the end of the day and won't grant access even if manipulated to show green when the A-Pass Security app scans the passport. Offline passport was a great feature to add due to the vastly heterogeneous nature of Acciona's premises and our users' device universe.

Notifications could help managers know that any of their team members have a red passport and have been told to stay home. They could also be used to lead users into medical advice or information.

Another important feature is the "I feel unwell" button, right in the lower middle of the main screen. It helps users create a new RHD whenever they feel they need to, which will force the creation of a new passport. Either if they feel suddenly sick, they have fever or have just been told that they have been in close contact to a COVID-19 positive, they can update their information in any moment.

The video consultation button shows instructions to appoint a video consultation session with the medical services that Acciona offers to employees.

A-Pass Security

This application is used by security personnel on the premises' access zones. It does not substitute any other security checks or validations; it works as a totally supplementary tool in accordance to Acciona's protocols. It's available in English and Spanish. A process will show if newer versions of the app are available and will force the download if that version is mandatory or will just let the user select to download it if the version is just recommended, though in this case versions are usually mandatory.

This app is often installed on a fixed device next to the security desk, but it can also be used in a handheld device to provide all the mobility that the entrance to a workplace could demand.

The app's basic use is to scan the QR from a user's device which will turn the screen of the scanning device green or red. Depending on the protocols in each moment, security personnel will act accordingly and grant access, send people home or show them the way to the medical booth so that further action can be taken. A grey screen will indicate an expired passport so the user will be instructed to renew their RHD in that moment.

The app can read online or offline passports and will always verify validity and expiration date. Color shown on the user's app and security app can be different in singular moments due to changes that couldn't be refreshed on the user app, so security personnel will always trust their app against the user's app if there are mismatches.

The app can keep working if it loses connection and will buffer interactions and send them to the backend once it gets back online.

Also, if the app stops working at all, and as a last line resource, security personnel could trust the user's app's passport color if the active protocol allows them to.

A series of additional features have been added to add value to this app. For example, a number of users don't use the A-Pass app. They rather fill the RHD on paper daily. A-Pass Security can help security personnel handle paper RHDs by "onboarding" users into the system using their National IDs and uploading the RHD information for them.

Another use case would be if a user renewed their RHD at home but forgot the phone at home. Using the user's National ID, A-Pass Security can retrieve the user's valid passport's color and grant them access to the premises.

Additionally, A-Pass Security allows security personnel to add the info of thermal cameras. After scanning a passport if the thermal camera shows the user's temperature is below the threshold defined by the protocols, they will press the green "no fever" button. If it's above the threshold they will press the red "fever" button, which will turn the screen red and will generate a new passport for the user and turn its app's back red.

The web app

The web App is used by three different corporate groups to help manage employees and workers in a safe and coordinated way:

- **Corporate Medical Department:**
  They are in charge of the workforce medical service. They will use this web app to introduce and manage workforce COVID-19 related medical data.

  This department will have access to query all workforce medical data related to COVID-19 and update and include additional medical test results. As a result of employee/worker medical diagnosis, they will be able to change employee/worker passport states. It is important to emphasize that only this department will have access to query and manage workforce medical data.

  Users in this department will identify a certain employee or worker using several filter criteria available in the web app. Once the employee/worker has been identified or selected, users will be able to manage medical data related with COVID-19:

  1. General employee/worker data: display gender, age, working localization as additional data to help the user in medical diagnosis and categorization
  2. Employee/worker historical RHDs information: display historical RHDs in which the employee/worker identifies COVID-19 risk factors
  3. Employee/worker fever historical data: display historical fever data. Medical users will be able to introduce fever symptoms
  4. Employee/worker COVID-19 test results: display historical test results. Medical users will be able to introduce COVID-19 additional test results, including PCR and antibody IgM/IgG tests
  5. Employee/worker thoracic x-ray: display historical thoracic x-ray pneumonia results. Medical users will be able to introduce additional pneumonia results
  6. Employee/worker blood tests: display historical blood tests. Medical users will be able to introduce additional blood test results including COVID-19 PCR and antibody IgM/IgG blood test results

- **Human Resources (HR) corporate department:**
  They are in charge of all HR management processes. They will use the web app to register COVID-19 medical leaves and discharges received from health authorities.

  Users in this department will identify a certain employee or worker using several filter criteria available in the web app. Once the employee/worker has been identified or selected, users will be able to:

  1. General employee/worker data: list basic data
  2. Expire a passport: useful in case an employee/worker makes a mistake when filling up the RHD

3. Manually force a passport color to red. This will change the passport state but won't overwrite backend logic.

- **Occupational Safety and Health (OSH):**
  They are in charge of practical aspects of Safety and Health at the workplace. These users will use this web app with two main purposes in mind:

  1. Have a clear idea of the distribution of people with forbidden access to corporate offices because of COVID-19 corporate procedures
  2. Expire a passport: useful in case an employee/worker makes a mistake when filling up the RHD
  3. Manually force a passport color to red. This will change the passport state but won't overwrite backend logic.

Note that neither HR nor OSH staff have access to medical data.

The Identity Service

Authentication and authorization of users in the platform is ruled by this service. It is the core of the onboarding and login processes.

Users can be employees or external workers who were previously enrolled to our corporate identity systems or even workers or partners which don't have any kind of Acciona IT identity.

The service will prompt A-Pass users the first time they use the app to choose if they have existing corporate credentials on centralized Acciona domains or if they don't, registering them into the system through a corporate credential validation or a local credential creation process depending on their choice. The onboarding process will check if the user exists in a preloaded user list which is updated periodically by the backend services from multiple sources (our HCM system or a contractors' database, for example)

Once registered, users willing to access A-Pass will be prompted again and they can login into the system using the corporate login process (which includes MFA or whatever security measures our corporate identity system dictates) or the local credentials depending on their case. This will grant the app a self-contained token containing the claims for the user. This expiring token will be used on the variety of calls to the different resources. Authentication is thus stateless, which reduces the overall number of interactions with the Identity Service.

The web app makes use of this same authentication strategy, though only users with corporate credentials will be allowed into the service in this case.

The WebAPI and backend services

Every backend service other than the Identity Service is exposed by a WebAPI that consists of a series of methods grouped by functionality:

- Admin methods
  - Used to gather info for the different apps
- Employee methods
  - A variety of methods used by A-Pass to obtain some user variables as well as the user's passport and notifications, and to renew the RHD
- Master methods
  - A variety of methods used by the apps and backend services to retrieve or modify general or core info
- MedicalServices methods
  - A variety of methods used by the web app to retrieve user info or add different test results, modify the status of a user's passport, etc.
- SecurityScan methods
  - Used by the A-Pass Security app to retrieve passport info or to send paper RHD statements

Backend services host most of the business logic of the platform. Part of the core logic relies on a state matrix that was built to link the different COVID-19 health states with the applicable actions for such health states. We designed this matrix due to two main reasons:

- The scientific community didn't have a clear notion yet of how SARS-CoV-2 immunity worked (which is still true to date), so we had to take into account valid states for people who could be infected for a second time
- Acciona's protocols were changing very fast and were expected to keep changing, and there was a big uncertainty of the actions that would be associated to each state, so we decided to separate "passport state" from "passport color"
    - Passport state is a numeric value that is related to the worker's COVID-19 health status, and it depends on a series of factors:
        - The value of the last PCR test
        - The value of the last serological test's indicators (IgG and IgM)
        - A transition from a previous positive PCR test to a negative PCR test
        - If users report to have compatible symptoms in their daily RHD in A-Pass
        - If users report to have been a close contact to a COVID-19 positive in their daily RHD in A-Pass
        - If users report to have been a traced contact to a COVID-19 positive[1] in their daily RHD in A-Pass
        - If the temperature scan when a user tried to access Acciona's premises was positive and the security personnel reported so in A-Pass Security
        - If users report compatible symptoms or to have been a close contact to a COVID-19 positive in their daily paper RHD and the security personnel reported so in A-Pass Security
    - Passport color is a numeric value that is related to the actions that we want to associate to that user. To date, only access to Acciona's premises action is in place (used as red, green, grey)

The association between "passport state" and "passport color" is configurable so that protocol changes can be implemented without the need to redeploy neither the apps nor the backend services.

Ideally the Medical, HR and OSH staff will only action on a series of levers that could potentially change the state and color of a user's passport, depending on their role:

- Expire a passport (just in case a user makes a mistake in their daily RHD)
- Force a red passport (which will change the passport state to a temporary state until a medical staff member reviews the case)
- Introduce new testing results

[1] When we designed the app, we had the idea to use the DP-3T decentralized BLE tracing protocol to trace users of the app and notify close contacts of a user that would test positive in COVID-19, but we ended up discarding this idea

If this were true, the system would automatically calculate passport states and preserve its integrity state wise, making sure transitions made sense (you wouldn't be able to go from infected to immune without the needed testing evidence). Unfortunately, the level of uncertainty made us go through an intermediate scenario in which the Medical staff (and only them) can manually set any passport state to any worker.

To illustrate this situation, just imagine if someone in the medical staff would manually set someone to an "asymptomatic, IgG negative, IgM positive" state but wouldn't introduce a new serological test with these same values into the system. This would turn the passport color to red, but as all passports expire at the end of the day, if the user were to report no symptoms or contact in the next RHD the platform would recalculate the passport state to something like "asymptomatic, no PCR, no test" if they don't have any stored tests in the database and thus the passport could turn green.

This eventually forced us to implement a series of additional rules to guarantee nobody could transition from a "red passport" to a "green passport" which would not be necessary if that manual input weren't needed.

It's important to note that once the information about how immunity works against SARS-CoV-2 grows, more and more states of the matrix could be deemed to be unnecessary so the logic could eventually be simplified.