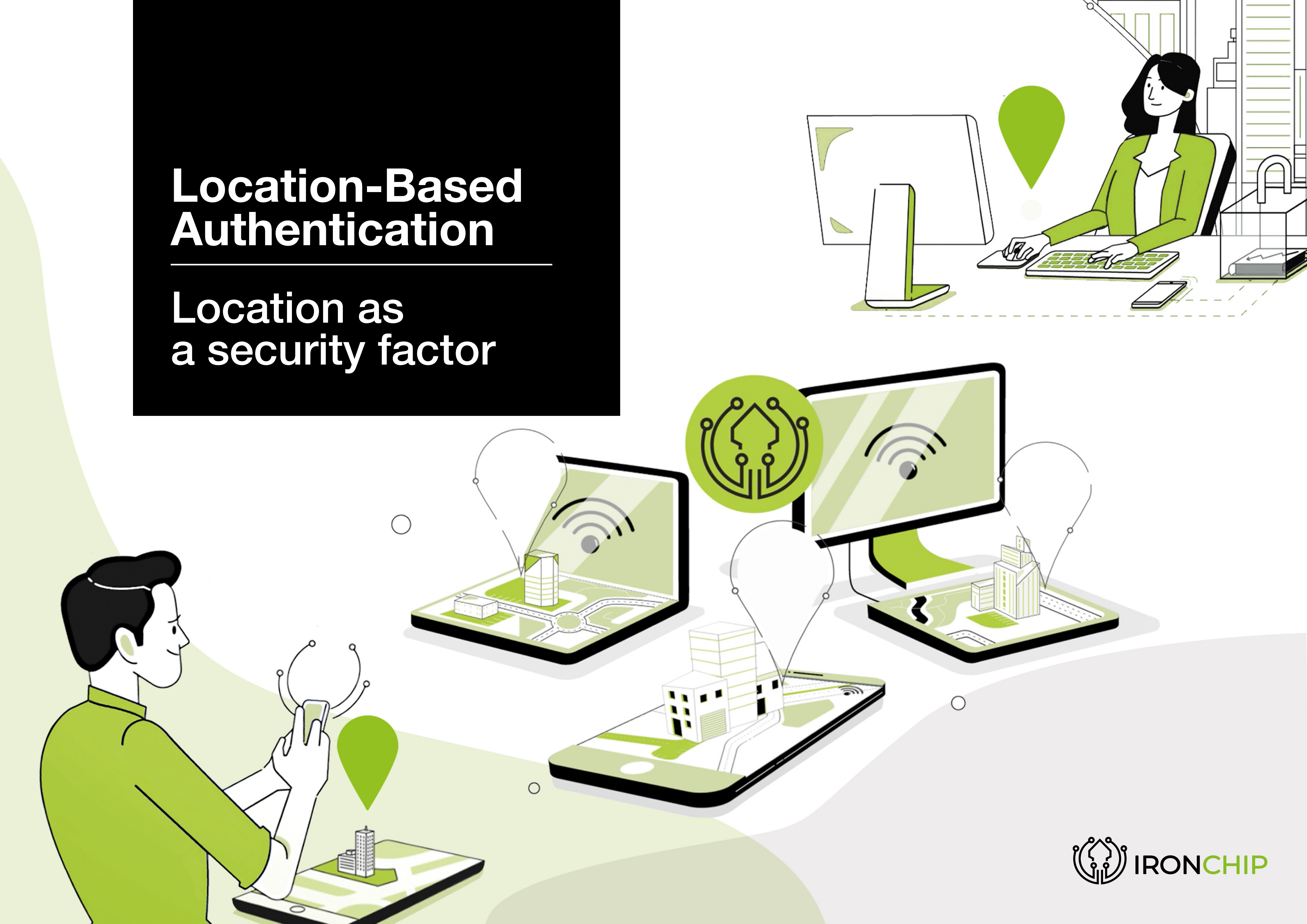
Location-Based Authentication

Location as a security factor



IRONCHIP

index

Introduction

Digitalization, Industry 4.0 and teleworking are increasingly present in our environment, causing many companies and institutions to open their systems, which were previously totally isolated, to the Internet, and hence increasing the risk of compromising their security. This has led to a **significant increase in identity theft attacks in recent years.**

Most cyber attacks are carried out by automated machines, exploiting the typical weaknesses shared by different companies and systems, not very different from the vulnerabilities exploited in the 90s. These automated attacks are based on programs with the sole mission of stealing passwords, such as MIMIKATZ, one of the most used programs by cybercriminals in 2020.

And how do we put an end to all these problems?

The best way is to add innovative security factors that take into account the identity of the device from which the service is accessed, and that use secure communication channels and factors that are more difficult to spoof than a password. If they also ensure that both users and companies have an easy and secure user experience, we would end up with four out of five attacks.

Taking into account that **90% of cyber attacks** classified as critical come from **foreign governments**[1], and that the majority of attacks originate from countries in Eastern Europe and Asia, it becomes obvious that using geolocation as a security factor can protect us from most attacks.

Moreover, if it was already vital to ensure the security of “anywhere operations” in the past, it has become essential after the digital acceleration and teleworking caused by the pandemic.

With teleworking, millions of companies have been forced to use remote access tools and, in March 2020 alone, Spain recorded more than 19 million attacks on RDP (Remote Desktop Protocol), one of the most widely used tools.

However, “anywhere operations” do not only apply to teleworking. In order to put an end to the systems security breach, it is necessary to implement methods that ensure all types of secure operations from any location, and therefore verify that the location from which an operation or attempt is being made to access any information or services, is an authorized or usual location for the user.

Using location as an access key, it would only be possible to connect to the company’s services from a secure location, thus putting an end to most attacks.

The question is:

Why has it not been used until now?

Location, as we know it until now, presents many security and usability problems, which has made it not to be present in security systems until now. **That is why Ironchip, with its electromagnetic wave location technology, is born; to make location a reliable security factor.**

[1] https://elpais.com/politica/2016/11/22/actualidad/1479843658_666221.html

Location-Based Authentication

"Authentication based on location"

Ironchip's Location-Based Security technology generates a digital identity based on a secure location.

Location-Based Authentication is a solution for **high-security authentication requirements**, adds strong authentication security mechanisms to your systems and provides fully out-of-band authentication with asymmetric elliptic key cryptography and mechanisms that prevent replay and man-in-the-middle (MitM) attacks.

Our authentication product offers a solution **certifying the identity of users and machines based on the device, biometrics and the location of the device.** In other words, we replace other security factors such as passwords, SMS, codes... (or we reinforce as a second authentication factor) by the following identity proofs:

Device identity proof

We certify that the device from which the user is authenticating is his own, and not that of an attacker.

Biometrics proof

We use the dactilar fingerprint/faceID sensor to certify that the authenticating user is the user and not an attacker. This can be replaced by a password on computers that do not have a biometric sensor.

Location proof

It uses Location-Based Security technology, which allows authentication using a secure location.

Advantages of the product

Device's proof of identity and biometry

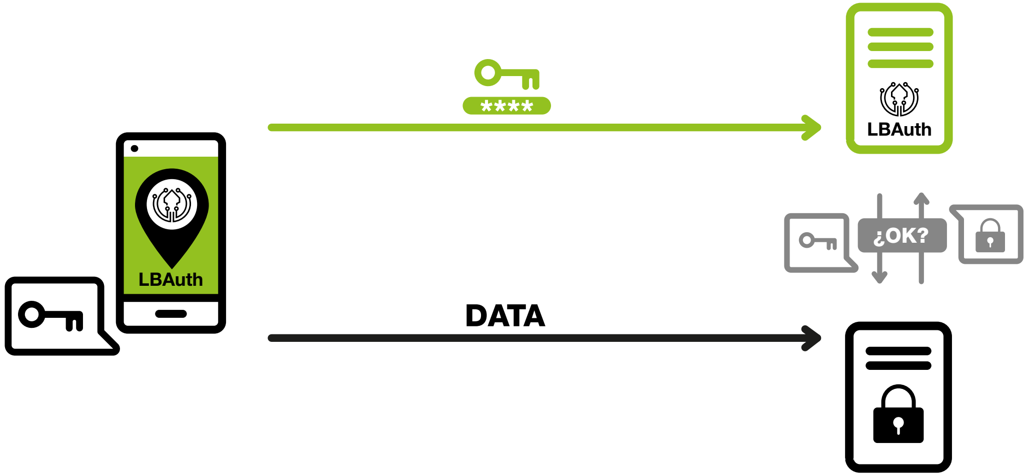
Our technology **identifies the device that sends the authentication information**, certifying whether it is an authorized device or not.

In order to achieve this, we use a PKI architecture. This architecture is based on asymmetric cryptography, based on the use of two cryptographic keys: a private key and a public key.

The private key is the digital identity, which is stored in the device encrypted by fingerprint (or passcode alternatively), **and the public key of the certificate is used to validate the digital identity**. The public key is stored on Ironchip's servers, so neither Ironchip nor any attacker can steal your identity.

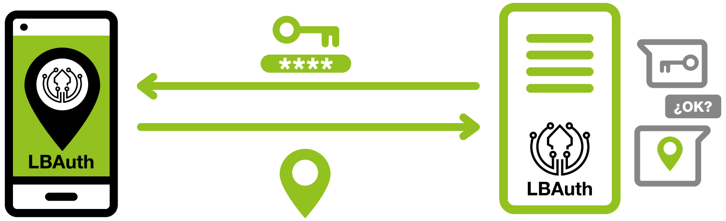
The public and private keys work as a pair. For example, when the private key is authentic, the public key verifies the authentication; when the public key encrypts, the private key decrypts; and when the private key signs digitally, the public key verifies the signature.

The communication for the authentication is established via a double encrypted channel, which implements TLS plus e**lliptic curve cryptography**. In addition, the authentication protocol includes mechanisms that make each authentication unique and it can only be used once, as if every time you log in you changed your password, ending with man-in-the-middle and replay attacks. Moreover, the authentication is totally out-of-band, ending phishing attacks once and for all. Using this secure channel, we send geolocation information, preventing the theft of wave information when it is sent to our servers.



Device registration based on a secure location

Our innovative device authorization process (enrollment) protects your administrator account with a secret location. This way, to authorize a new device, that is, for the device to get its identifier, it is necessary to know the secret location of the administrator.



Anti Data-Leakage

Currently, the vast majority of security systems save passwords on the server, in order to be able to check them later when the user wants to access the service. This means that any cybercriminal who manages to access the server can obtain and even leak user passwords on the Internet.

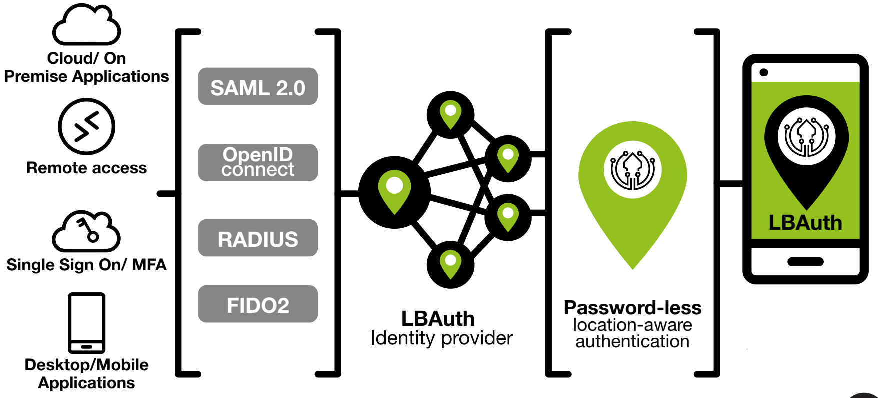
Location-Based Authentication d**oes not save the secret locations that allow the device to be authorized, neither on the server nor on the client.** Thanks to our Artificial Intelligence, we can train our algorithms first, to save later only the mathematical model, instead of saving the waves.

By not storing any information, we became **one of the first solutions capable of certifying the identity of a user without the need to save their access information.**

Standard-based integration

Location-Based Authentication is designed and programmed with security and interoperability as fundamental pillars, so we support the majority of integrations based on authentication protocols: SAML, OpenID Connect, FIDO2, RADIUS or a custom integration based on HTTPS.

Besides, our plugin for Active Directory Federated Services (ADFS) allows you to enjoy our technology in Microsoft environments, being able to use your Active Directory (AD) as a user database.



Operating modes

Mobility is one of the main problems presented by access control systems. When access needs to be protected from a single point on the planet, it is easy to control who and when accesses. **However, the proliferation of mobile devices and the needs of teleworking, have made mobility a requirement for many of the business services.**

Obviously, mobility makes it more difficult to maintain control of who and when accesses our services. Not just that, but sometimes employees need to connect to the service as soon as possible, and non-mobility can be an impediment.

To solve the problems above, Location-Based Authentication allows two types of authentication to be carried out depending on the mobility needs required by the system that is being protected. Although location is the most important and differential factor of our technology, all the security features of Location-Based Authentication allow us to offer a mode of operation that does not take location into account.

Thus, the operating modes are:

- **Authentication with mobility:**
  Checks both the identity of the device and that of the user's fingerprint.

- **Authentication without mobility:**
  In addition, to ensure that the source device and fingerprint are correct, it uses our secure location to determine if the user is authenticating from a permitted location.

How it works

Location-Based Authentication allows devices and users to be identified using a protocol designed to ensure the identity of the source, the identity of the destination, and the integrity and encryption of authentication data.

Mainly, Location-Based Authentication consists of two processes: The user registration process and the authentication process.

Enrollment process

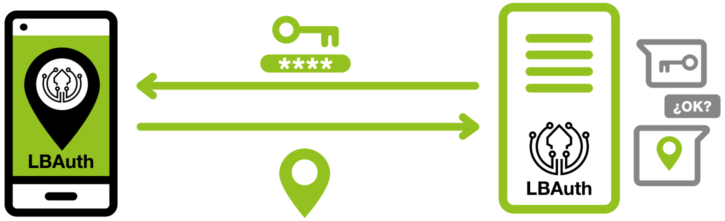
What differentiates our device authorization process is that instead of relying on SMS, security questions or one-time passwords, **we use a location that allows a device to make future authorizations.**

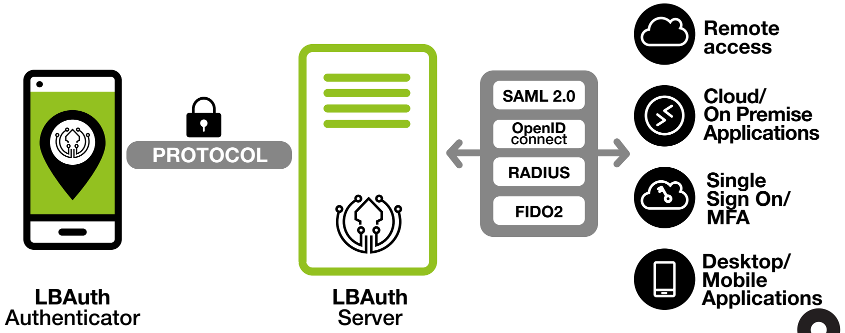
Once the user has enrolled a device in its secure area, it will generate an asymmetric encryption that will allow the device to be identified using its unique identifiers as a private key. In addition, the device will obtain various secrets and one-time tokens, which it will use to apply the last layer of encryption and will renew on each identity request.

For this process, we do not use GPS coordinates that are easy to falsify, but rather our artificial intelligence algorithm analyzes the radio waves that the device detects. With these fingerprints, the device creates a unique fingerprint, which the server analyzes, certifying whether the user is in the authorized place and providing a KPI of the correlation obtained between the different signals.

Authentication Process

For this process, the user must submit a proof of identity, which is sent over a channel with **military grade encryption. An encryption that joins a TLS encryption layer to another layer with elliptic curve cryptography,** which allows both the server and the client to sign and encrypt their requests, in addition to a last anti-replay mechanism incorporated in the authentication protocol.





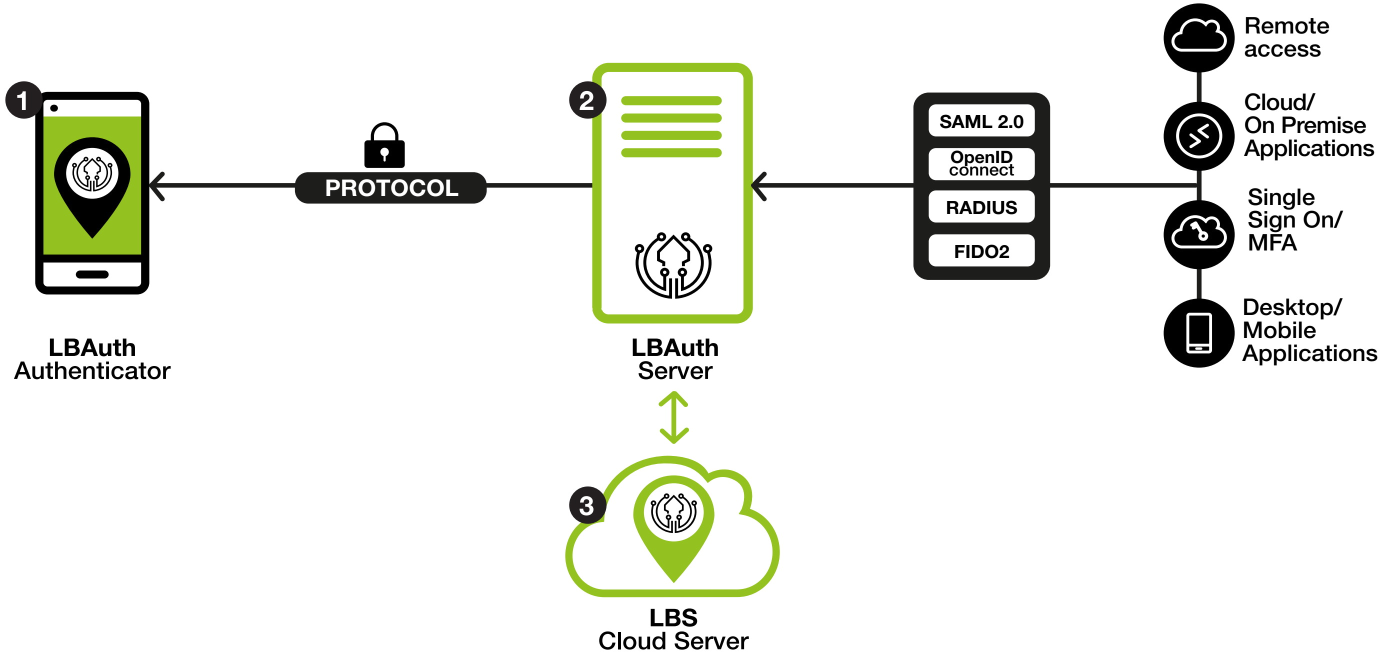
Architecture and components

Location-Based Authentication presents a software architecture based on microservices, each one in charge of a part of the authentication. **There are three main components:** Location-Based Authentication Authenticator, Location-Based Authentication Server, LBS Cloud Service.

1 **Location-Based Authentication Authenticator** is the application that gives your users access, replacing passwords for one click.

2 **Location-Based Authentication Server** is responsible for managing users, accesses and communications, using Location-Based Authentication Protocol, guaranteeing the security, integrity and encryption of all authentication communications. In addition, Location-Based Authentication Server includes a control panel that allows you to visually manage and control what happens in your company, knowing and configuring who, when and from where users access.

3 **LBS Cloud Server** is the component where the magic of our product is made, providing our exclusive artificial intelligence certification in form of SaaS, which certifies the geographical location of the device.



Location-Based Authentication Authenticator

It is a multiplatform application and it can be downloaded from the main application stores, which allows users to authenticate.

Location-Based Authentication authenticator simplifies access for your employees, replacing passwords for a single click.

You can use our out-of-the-box application to authenticate any user with our exclusive security layer.

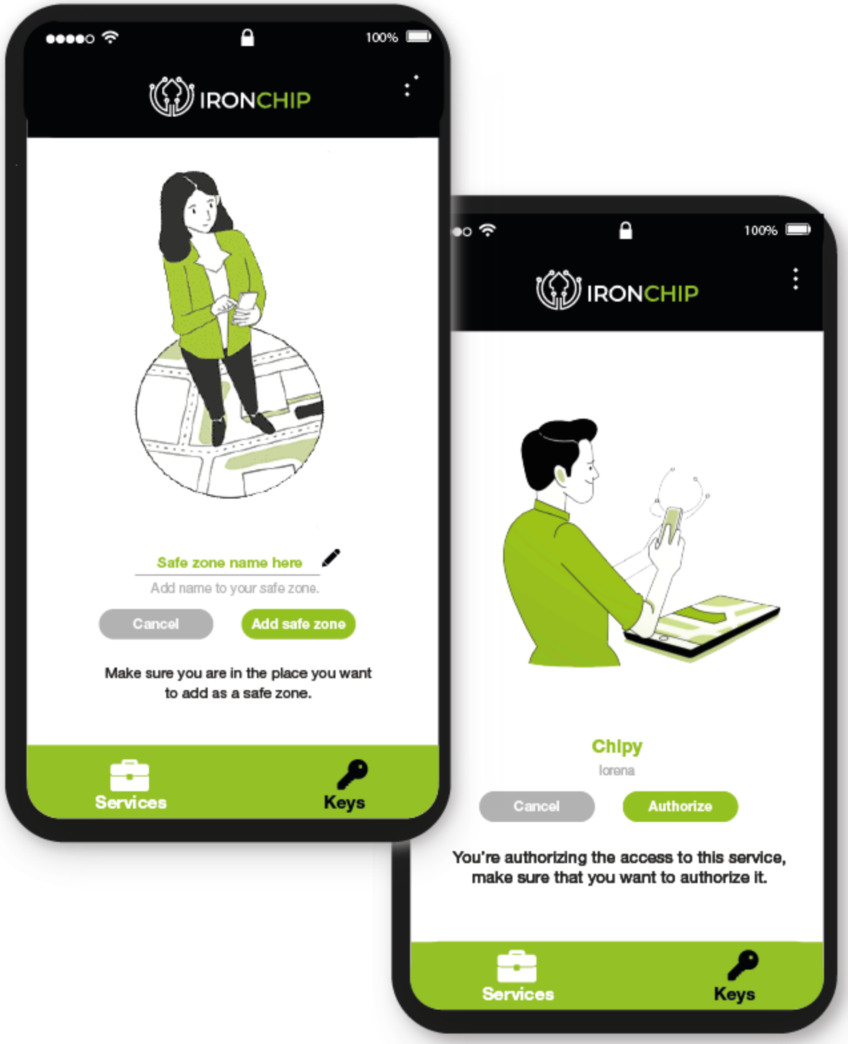
The application takes care of both the enrollment process and the authentication in the service, without the need to integrate anything on the client's side.

Install and use. As simple as that!

If, on the contrary, you do not want to use our application, with our Authenticator SDK, you will be able to integrate all the functionalities that our Location-Based Authentication application offers in your own application.

Available in its versions:

- **REST API**
- **Go SDK**
- **Java SDK**
- **Android SDK**
- **iOS SDK**
- **Ionic SDK**



Make sure you are in the place you want to add as a safe zone.

You're authorizing the access to this service, make sure that you want to authorize it.

Location-Based Authentication Server

This is the component that offers the authentication API, the integration API and the management dashboard. Although this server is offered directly as SaaS hosted in our cloud, it is also possible to host it on your own infrastructure.

Location-Based Authentication Server is made up of three main services, which are:

1. Location-Based Authentication Server

It is the service that contains all the authentication functionality. Mainly, it is an API that performs two main processes: User enrollment and identity certification.

2. Location-Based Authentication Identity Server:

It provides integrations with most of the market standards, allowing the protection of any existing service. The supported protocols are:

- OIDC
- SAML 2.0
- FIDO2
- RADIUS
- HTTPS/GRPC
- MICROSOFT ADFS
- MICROSOFT NPS

3. Location-Based Authentication Control Panel:

It allows to visually manage and control what happens in your company, knowing and configuring who, when and from where your users access. *(Image available on next page)*

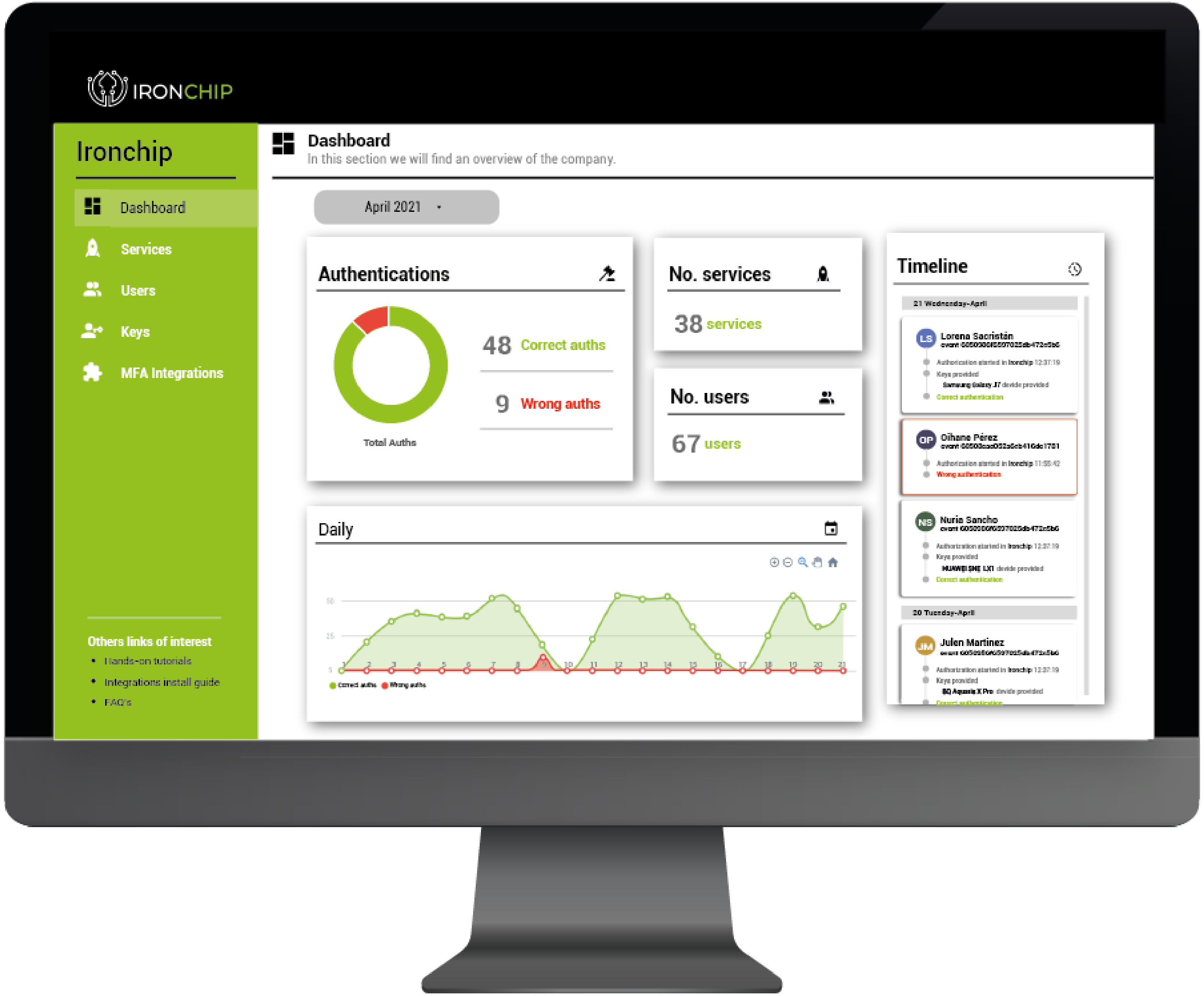
This service is offered as a web application from which the administrator can:

- Add and remove users.
- Add and remove services.
- Add and remove identity factors.
- Configure the accesses and the factors of each user to each service.
- Monitor accesses.
- Configure security alarms.
- Download activity reports.

If, on the contrary, you do not want to use our web application, our Server SDK carries out all the functionalities of the control panel programmatically, so that the administrator can carry out all the management tasks from their own application. Available in its versions:

- REST API
- GoSDK
- Java SDK
- Android SDK
- iOS SDK
- Ionic SDK

(Location-Based Authentication Control Panel image)



IRONCHIP

Ironchip

- Dashboard
- Services
- Users
- Keys
- MFA Integrations

Others links of interest

- Hands-on tutorials
- Integrations install guide
- FAQ's

Dashboard

In this section we will find an overview of the company.

April 2021

Authentications

48 Correct auths

9 Wrong auths

Total Auths

No. services

38 services

No. users

67 users

Daily

Timeline

21 Wednesday-April

LS Lorena Sacristán
event 6050306f5507025db472a5b6
Authorization started in Ironchip 12:37:19
Keys provided
Samsung Galaxy J7 device provided
Correct authentication

OP Oihane Pérez
event 60503cad052a6cb416dc1781
Authorization started in Ironchip 11:58:42
Wrong authentication

NS Nuria Sancho
event 6050306f5507025db472a5b6
Authorization started in Ironchip 12:37:19
Keys provided
HUAWEI SNE LX1 device provided
Correct authentication

20 Tuesday-April

JM Julen Martinez
event 6050306f5507025db472a5b6
Authorization started in Ironchip 12:37:19
Keys provided
BQ Aquaris X Pro device provided
Correct authentication

LBS Cloud Server

It is the component where the magic of our product is made, providing our exclusive artificial intelligence certification in the form of SaaS, which certifies the geographical location of the device.

LBS is the only service that we do not offer under an *on premise* architecture, since our artificial intelligence improves with each authentication, allowing us to continuously improve our product.

Contact Ironchip's sales team

Aitor Zaballa

✉ aitor.zaballa@ironchip.com 📱 617 898 342