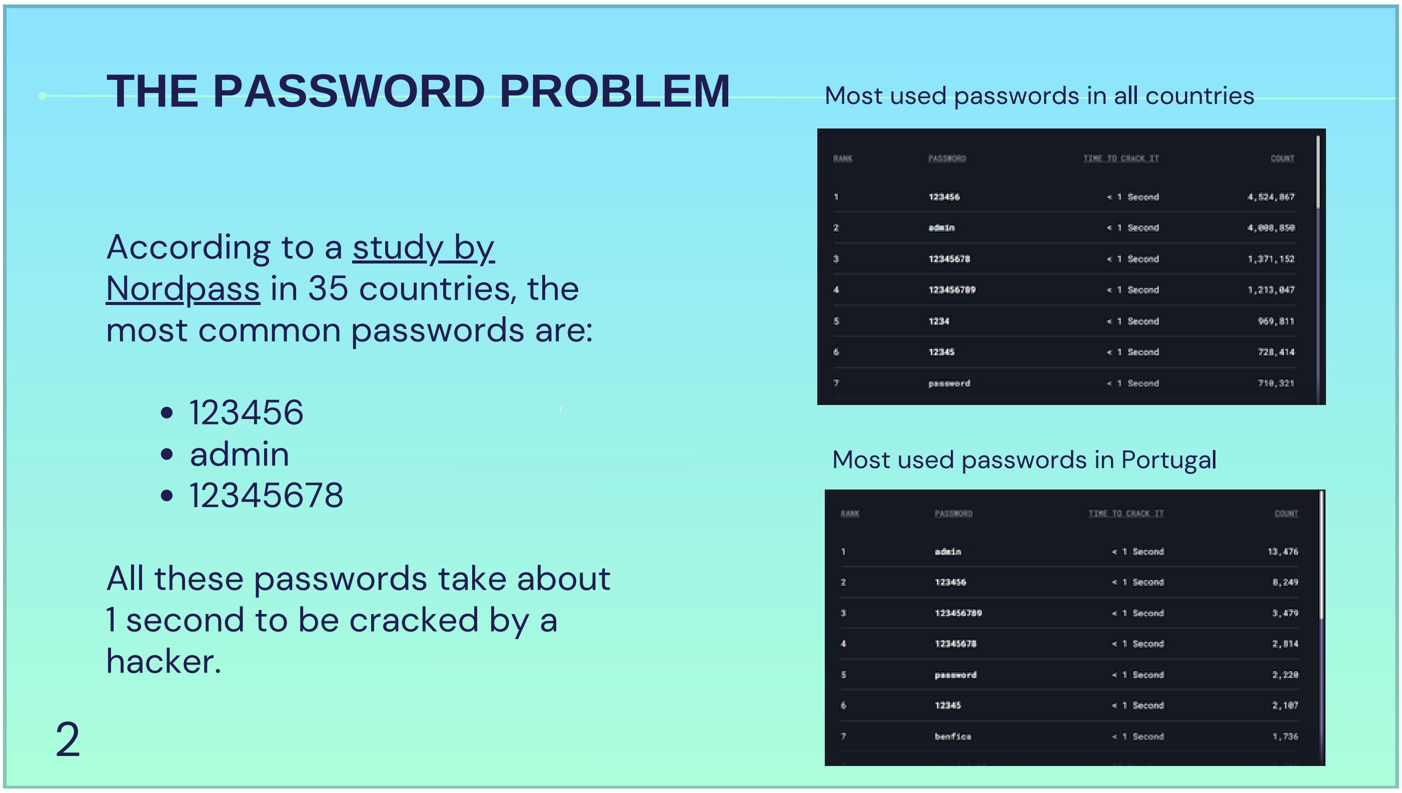
# SafePass

## A secure password management system

Made by:
João Luís, MEC 107403, LEI
Rodrigo Aguiar, MEC 108969, LEI



## THE PASSWORD PROBLEM

According to a study by Nordpass in 35 countries, the most common passwords are:

- 123456
- admin
- 12345678

All these passwords take about 1 second to be cracked by a hacker.

2

Most used passwords in all countries

| RANK | PASSWORD | TIME TO CRACK IT | COUNT |
|---|---|---|---|
| 1 | 123456 | < 1 Second | 4,524,867 |
| 2 | admin | < 1 Second | 4,008,850 |
| 3 | 12345678 | < 1 Second | 1,371,152 |
| 4 | 123456789 | < 1 Second | 1,213,047 |
| 5 | 1234 | < 1 Second | 969,811 |
| 6 | 12345 | < 1 Second | 728,414 |
| 7 | password | < 1 Second | 710,321 |

Most used passwords in Portugal

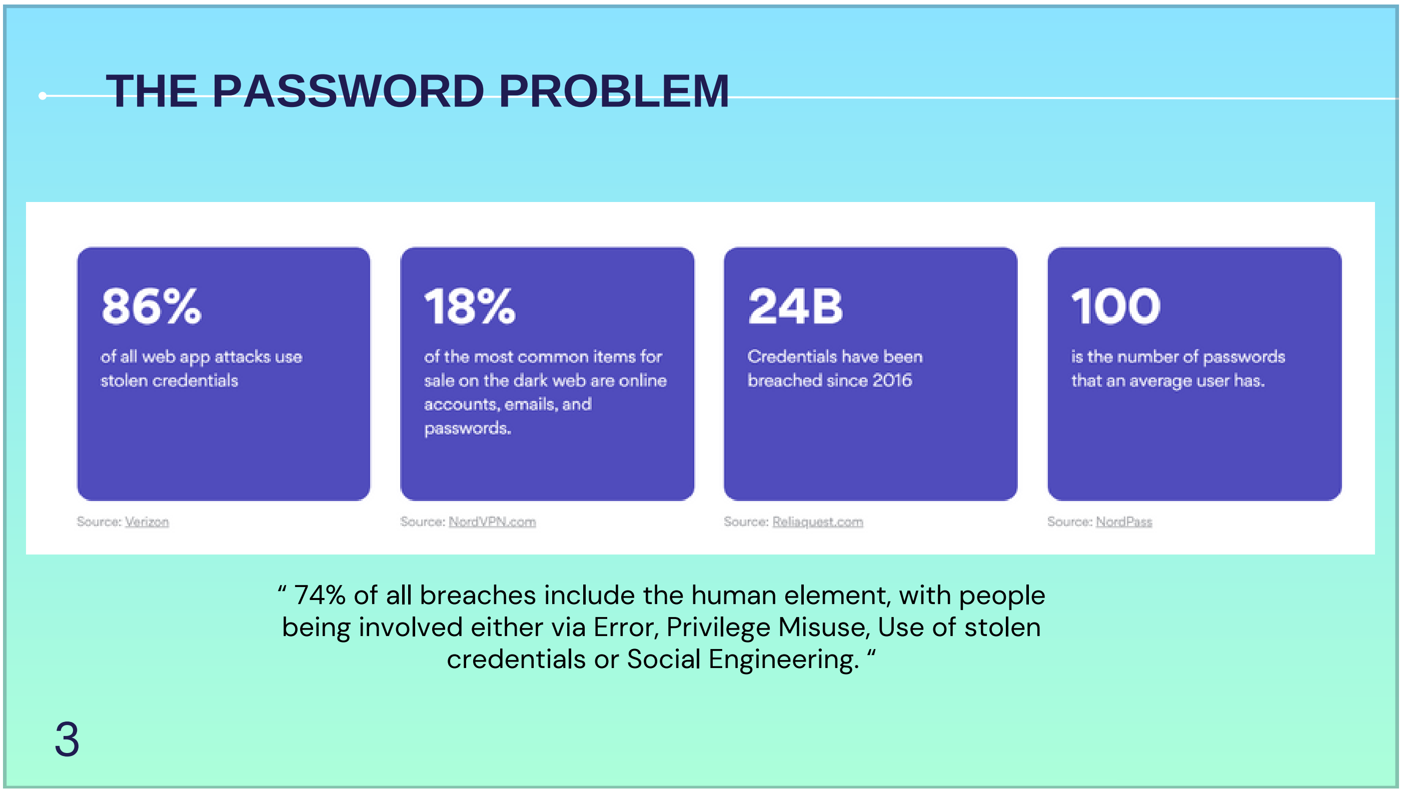
| RANK | PASSWORD | TIME TO CRACK IT | COUNT |
|---|---|---|---|
| 1 | admin | < 1 Second | 13,476 |
| 2 | 123456 | < 1 Second | 8,249 |
| 3 | 123456789 | < 1 Second | 3,479 |
| 4 | 12345678 | < 1 Second | 2,814 |
| 5 | password | < 1 Second | 2,220 |
| 6 | 12345 | < 1 Second | 2,107 |
| 7 | benfica | < 1 Second | 1,736 |

In a study conducted by NordPass in 35 countries, the researchers found out that the most common passwords were the following :

- 123456
- admin
-12345678

The results were based on a 6.6 TB Database of passwords that we're stolen using various types of malware.

The most common passwords are highly insecure, being extremely easy for bad agents or hackers to brute force ( taking about 1 second ).



## THE PASSWORD PROBLEM

**86%**
of all web app attacks use stolen credentials

Source: Verizon

**18%**
of the most common items for sale on the dark web are online accounts, emails, and passwords.

Source: NordVPN.com

**24B**
Credentials have been breached since 2016

Source: Reliaquest.com

**100**
is the number of passwords that an average user has.

Source: NordPass

" 74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering. "

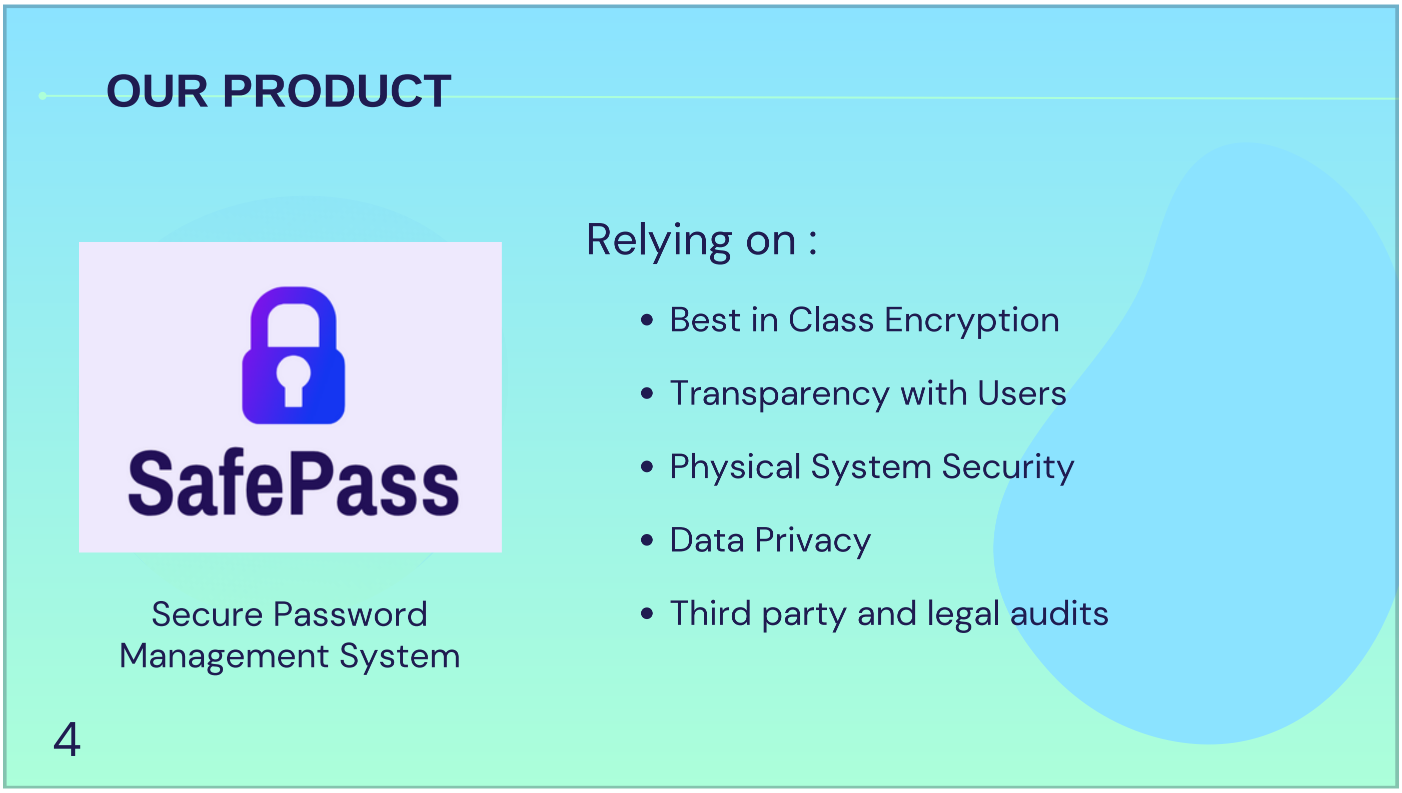
3

Furthermore, the study concluded that the average amount of passwords a user has is 100.

Since it is a high enough number, it could be one of the causes of people using simple and insecure passwords, since harder passwords may need to be stored somewhere else or force people to remember them.

In most attacks to web applications ( 86% ) stolen credentials are used which reveals the importance of protecting user credentials.

In general, this study reveals how important it is for users to protect their credentials and the impact their misuse may have.



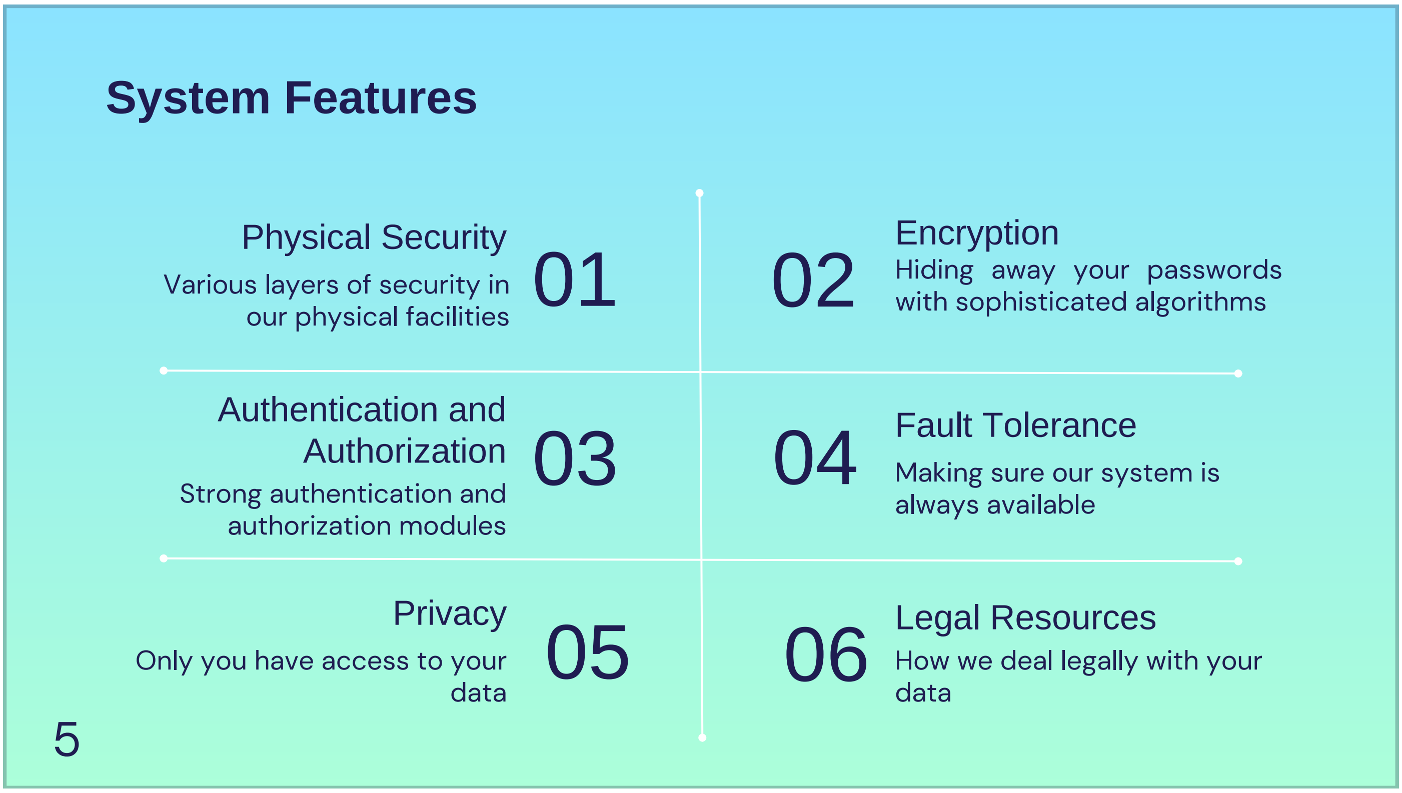
## OUR PRODUCT

SafePass

Secure Password
Management System

Relying on :

- Best in Class Encryption
- Transparency with Users
- Physical System Security
- Data Privacy
- Third party and legal audits



## System Features

01 Physical Security

Various layers of security in our physical facilities

02 Encryption

Hiding away your passwords with sophisticated algorithms

03 Authentication and Authorization

Strong authentication and authorization modules

04 Fault Tolerance

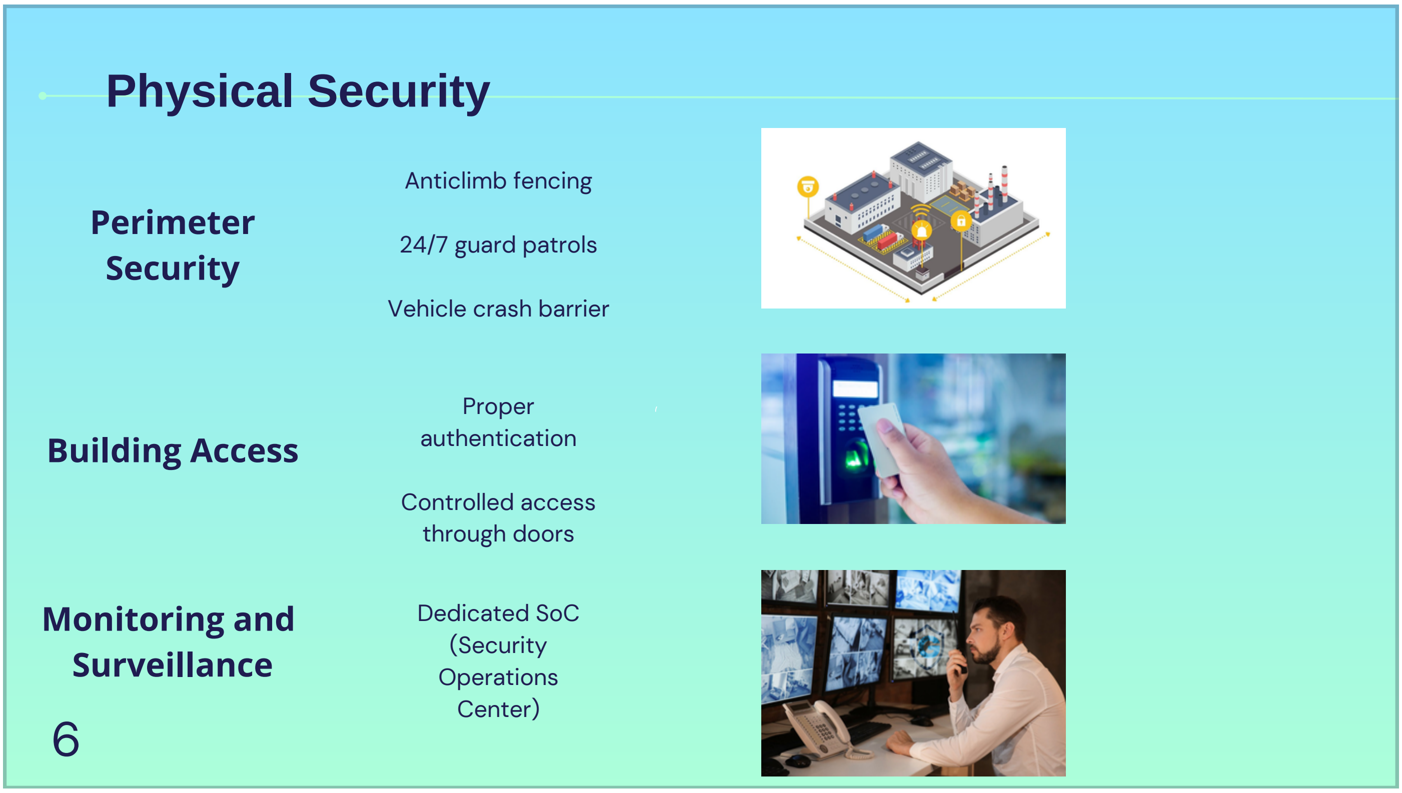
Making sure our system is always available

05 Privacy

Only you have access to your data

06 Legal Resources

How we deal legally with your data



## Physical Security

**Perimeter Security**

Anticlimb fencing

24/7 guard patrols

Vehicle crash barrier

**Building Access**

Proper authentication

Controlled access through doors

**Monitoring and Surveillance**

Dedicated SoC (Security Operations Center)

6

Physical Security of data centers is paramount to ensure the safety of our users data.

SafePass  data centers have the following security levels:

Perimeter Security

- Signage and anti climb-fencing along the property boundaries.

- Overlapping thermal and standard cameras;

- 24/7 guard patrols ;

- Vehicle crash barrier;

Building Access

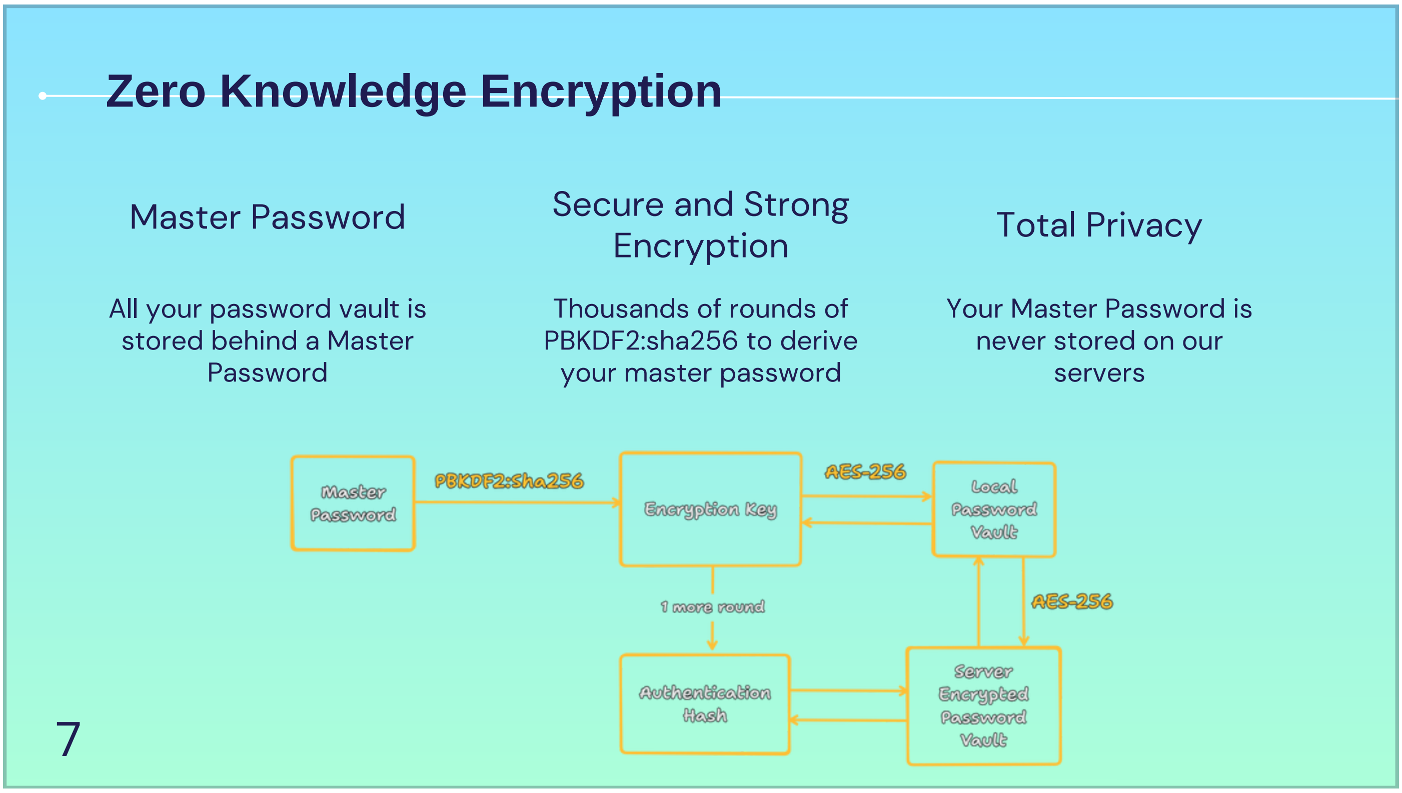
- Authentication with Iris scan to confirm ID.

- In critical areas, only one person can pass through the door at a time, passing his card on the sc an;

- In the data center floors, only the technicians and engineers that need to work on that site are  allowed to enter. The user's password vaults are always encrypted, and only the client can access them with their master key.

Monitoring and Surveillance

- SoC (Security Operations Center) operating 24/7 to ensure our data centers meet the highest standards of security



## Zero Knowledge Encryption

### Master Password

All your password vault is stored behind a Master Password

### Secure and Strong Encryption

Thousands of rounds of PBKDF2:sha256 to derive your master password

### Total Privacy

Your Master Password is never stored on our servers

In SafePass, all your passwords are stored within a password vault.

This is not the standard physical vault, but a software representation of one, where to access it  you need a key, in this case, your Master Password.

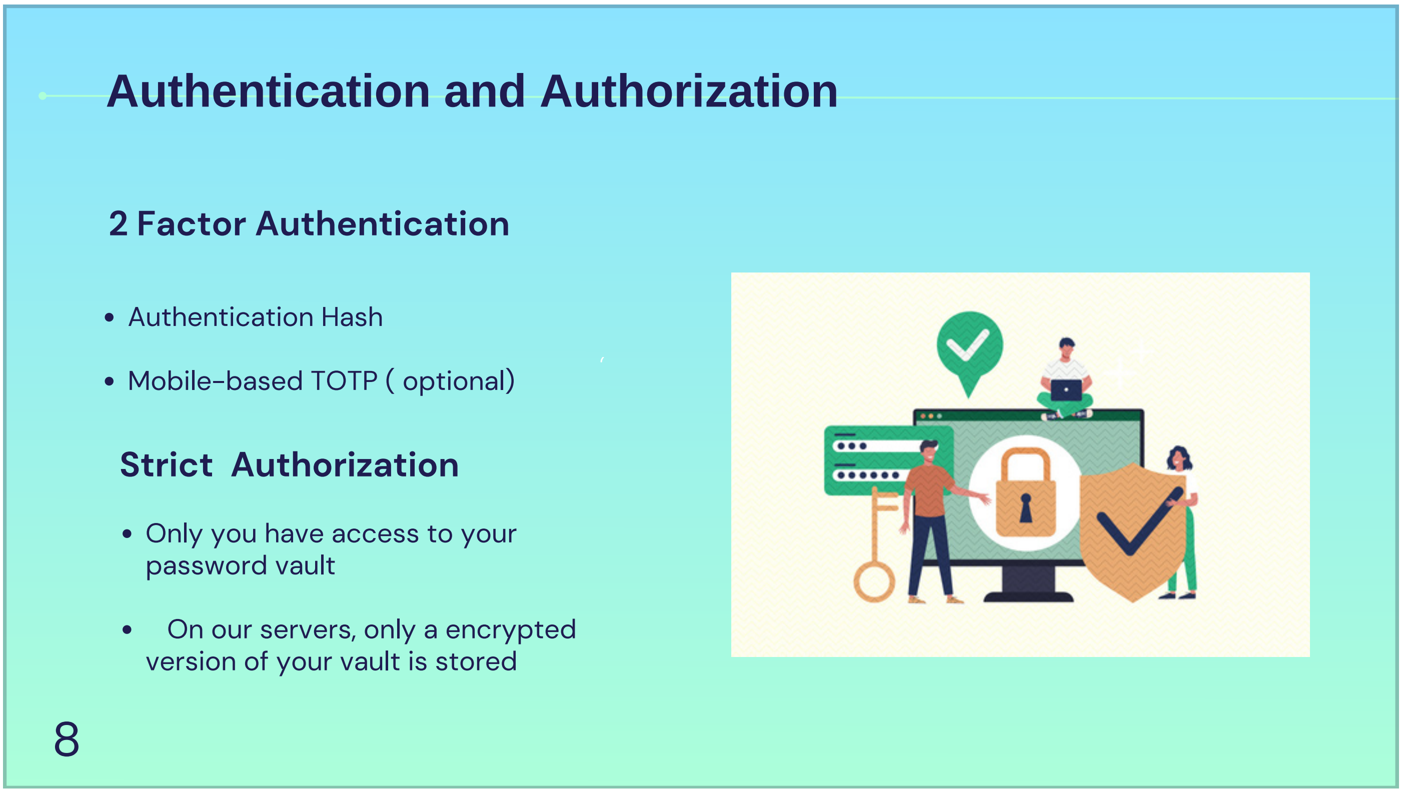
This Master Password is defined by you when you create a account in our system, and its supposed to be as secure as possible.

This Master Password is your only way to access your password vault, so its paramount that you  do not forget it.

To ensure the security of your passwords within the vault, it is encrypted using the Advanced  Encryption Standard (AES) 256, one of the current strongest encryption algorithms, being  unbreakable to this point.

This algorithm uses the concept of symmetric keys, which means that only the same key used to  encrypt your password vault may be used to decrypt it.

To note that the process of encrypting your master password and password vault is done locally  on your computer and, as such, SafePass does not have access to your master password or your  decrypted password vault.



## Authentication and Authorization

### 2 Factor Authentication

- Authentication Hash
- Mobile-based TOTP ( optional)

### Strict  Authorization

- Only you have access to your password vault
- On our servers, only a encrypted version of your vault is stored

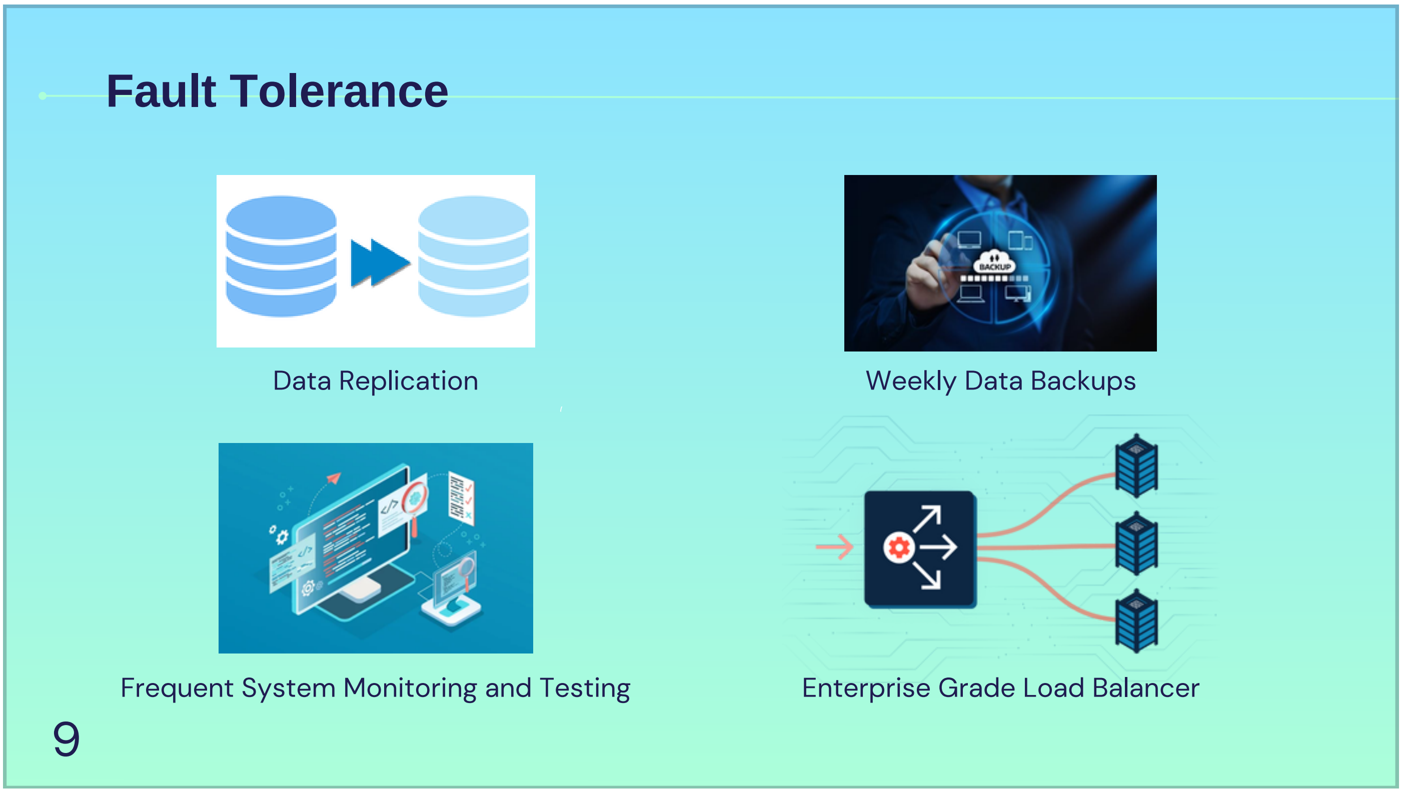
8

To ensure maximum security and privacy for our users, a authentication hash is derived from their master password which is used to authenticate users in the system.

Users may also choose to activate 2FA. In the case they do, after accessing their account normally, a time-based code will be sent to a chosen application that supports TOTP codes, such as Google Authenticator or Twillio Authy. This code must then be entered in the user interface to enter the account.

2FA presents itself as a strong second layer of security in user authentication, prevent possible user data breaches when the master password may be compromised.

Only a user through his master password should have access to his vault.  At this point in the system, vault sharing is not possible, only through the sharing of the master password which is highly not recommended.



## Fault Tolerance

Data Replication

Weekly Data Backups

Frequent System Monitoring and Testing

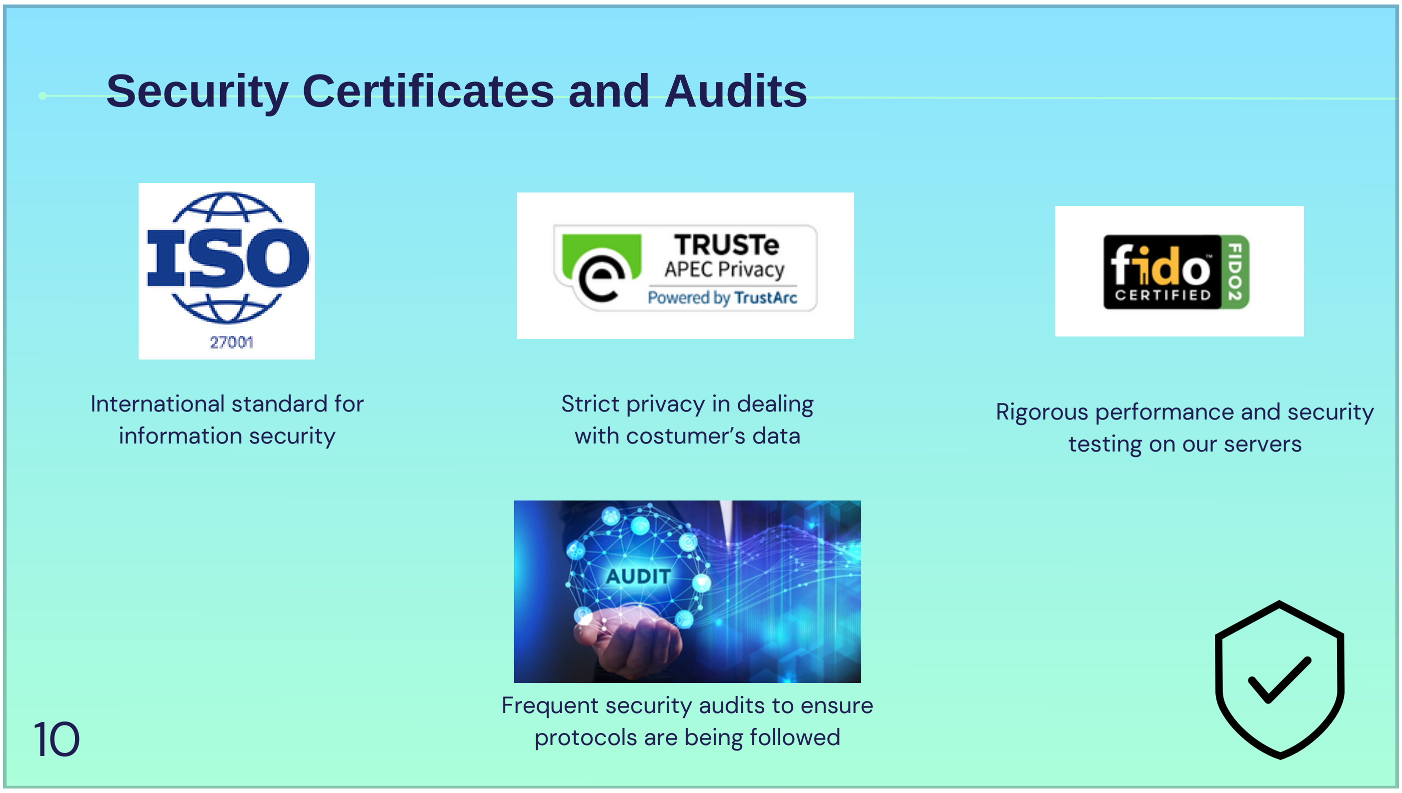
Enterprise Grade Load Balancer

9

SafePass aims to be available anywhere and at all times.
With this goal, we frequently monitor the system performance and logs to find out if something is wrong or not working as expected.

In order to ensure that we don't compromise user's data,
actions such as Data Replication between various storage nodes and Weekly Data Backups are done, making sure that users do not lose their password vaults in case of a failure in a data center or disk.

SafePass also has a sophisticated load balancer, meant to distribute user's request through multiple data nodes, ensuring that no node gets too overcharged, which can lead to a point of failure or unavailability.



## Security Certificates and Audits

International standard for information security

Strict privacy in dealing with costumer's data

Rigorous performance and security testing on our servers

Frequent security audits to ensure protocols are being followed

10

ISO
27001
TRUSTe
APEC Privacy
Powered by TrustArc
fido
CERTIFIED
FIDO2
AUDIT

SafePass top priority is the security of its service, being it a distinguish factor from its competitors.
As such, strict measures and protocols have been implemented in dealing with user's data and information in general.
The following certificates are a accomplishment of our work in making sure that our service is as secure and as reliable as possible.

ISO 27001 - Industry standard for information security and management.

As per ISO 27001 requirements, SafePass has its own ISMS ( Information Security Management System ), responsible for the continuous development and improvement of risk assessment plans to ensure the maximum security in the handling of user information.

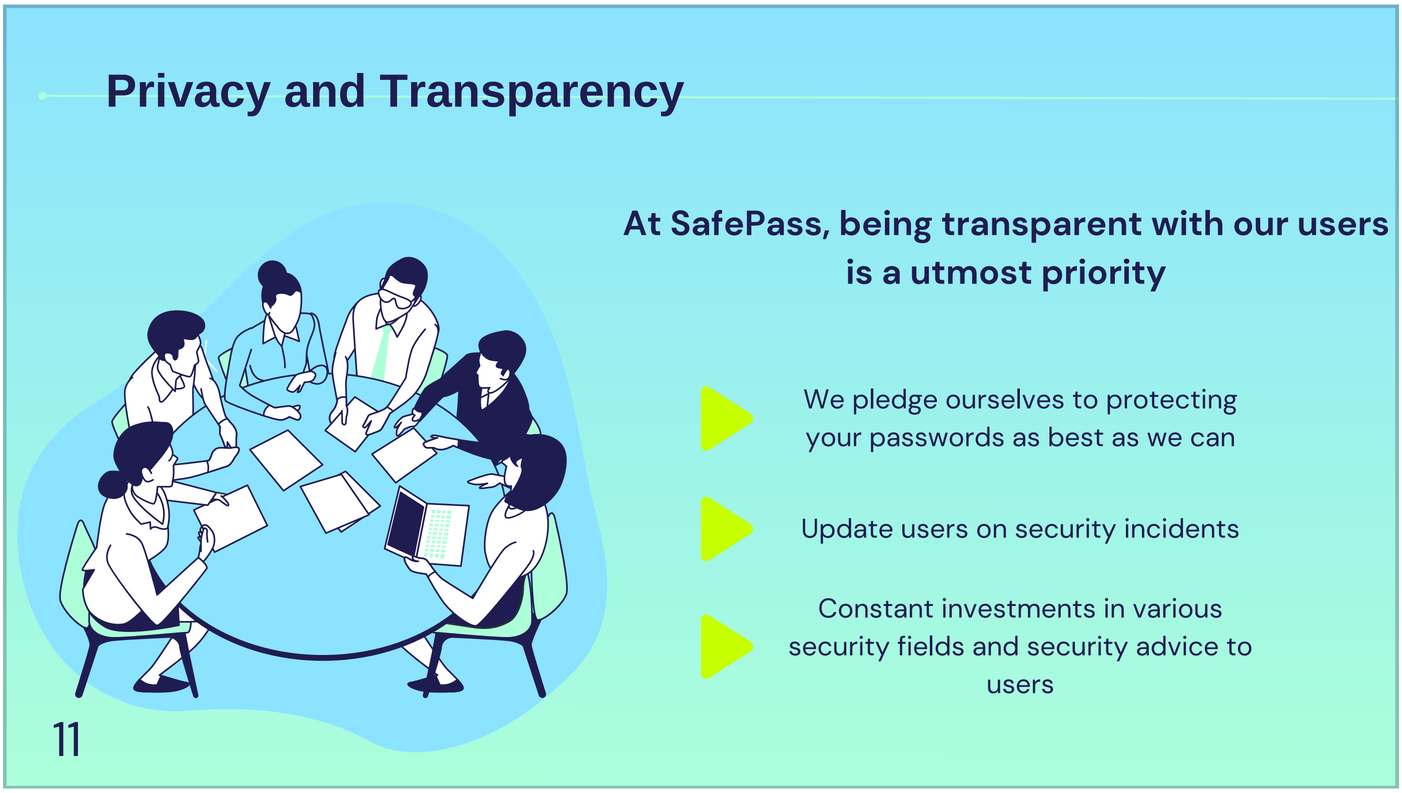
TRUSTe APEC Privacy Certificate - Privacy Standards for companies comprising the Asia-Pacific Economic Cooperation, such as the USA, China, Philipines, ...

Per the certificate requirements, SafePass programs and privacy practices are constantly monitored and improved to ensure there are no data breaches or leaks of users data.

FIDO2 Certification - Adhering to globally recognized FIDO specifications and requirements.

SafePass implements and adheres to globally recognized secure authentication algorithms to ensure it is not possible for a user to access another's password vault.

SafePass employs world-class security organizations to conduct regular audits on the system  condition and infrastructure, to ensure its systems are not vulnerable to potential attacks.



## Privacy and Transparency

**At SafePass, being transparent with our users is a utmost priority**

- We pledge ourselves to protecting your passwords as best as we can
- Update users on security incidents
- Constant investments in various security fields and security advice to users

11

SafePass bases its privacy policies on the following keypoints:

- Consentment

SafePass only collects strictly necessary data from the user's to ensure the system's functionality.
Before doing so, the user is asked whether he agrees with this or not.

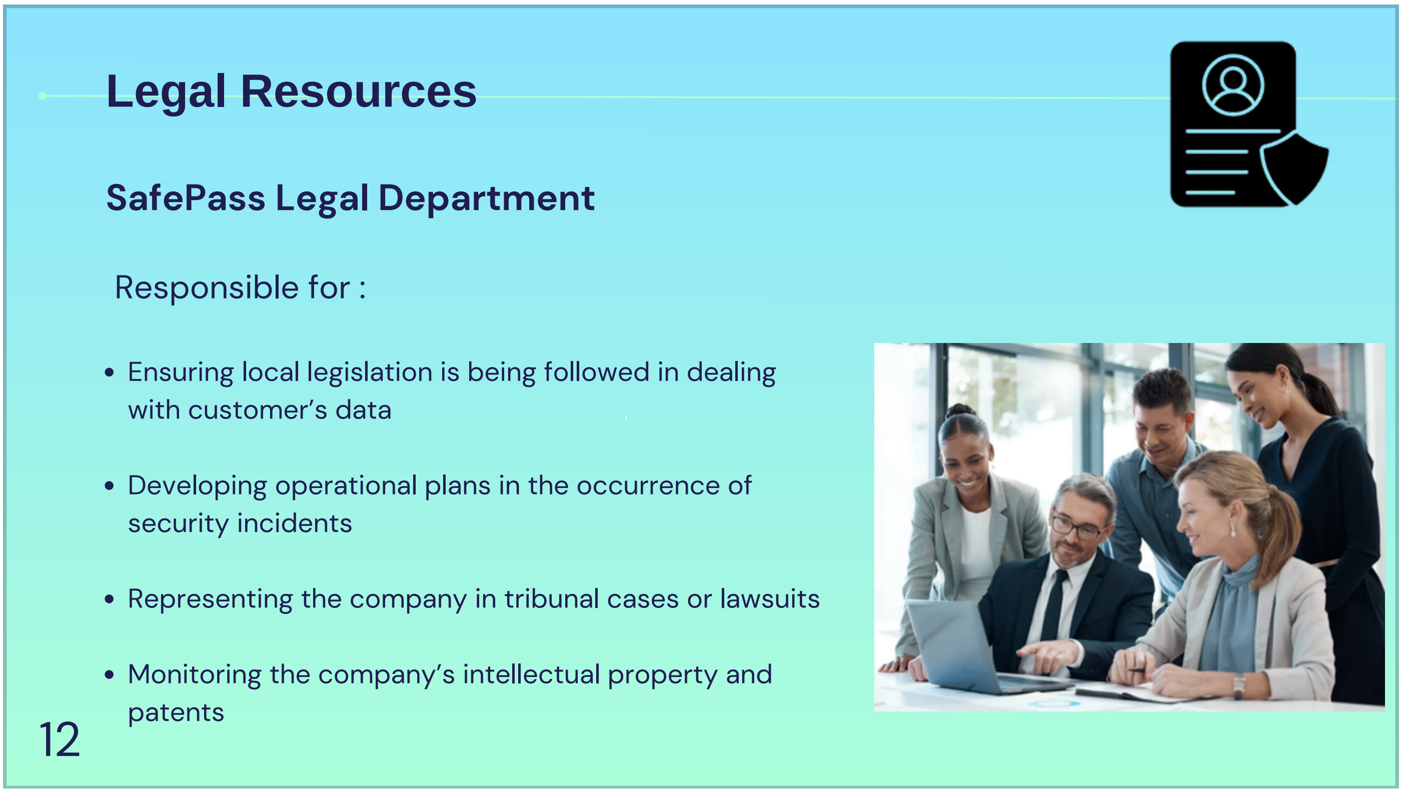
- Awareness

At SafePass, we strive to keep our users safe. As such, we constantly update users with new  security measures that may be taken in order to protect their accounts.

- Transparency

In the case of a data breach or a system failure, SafePass contacts its users in order to inform  them about the problem.

SafePass complies with the EU-U.S. Data Privacy Framework, which regulates and creates a  framework for how data should be sent between countries from the European Union and the USA  and is responsible for the secure management, storage and transfer of the data that it receives.



## Legal Resources

### SafePass Legal Department

Responsible for :

- Ensuring local legislation is being followed in dealing with customer’s data
- Developing operational plans in the occurrence of security incidents
- Representing the company in tribunal cases or lawsuits
- Monitoring the company’s intellectual property and patents

12

Operating a international business requires that various regulations and legislation must be met in servicing our users with SafePass.

The SafePass legal department is responsible for preserving the legal and intellectual property of the company and making sure that our product complies with laws in the countries of operation.

SafePass adheres to the following data protection regulations:

- EU General Data Protection Regulation

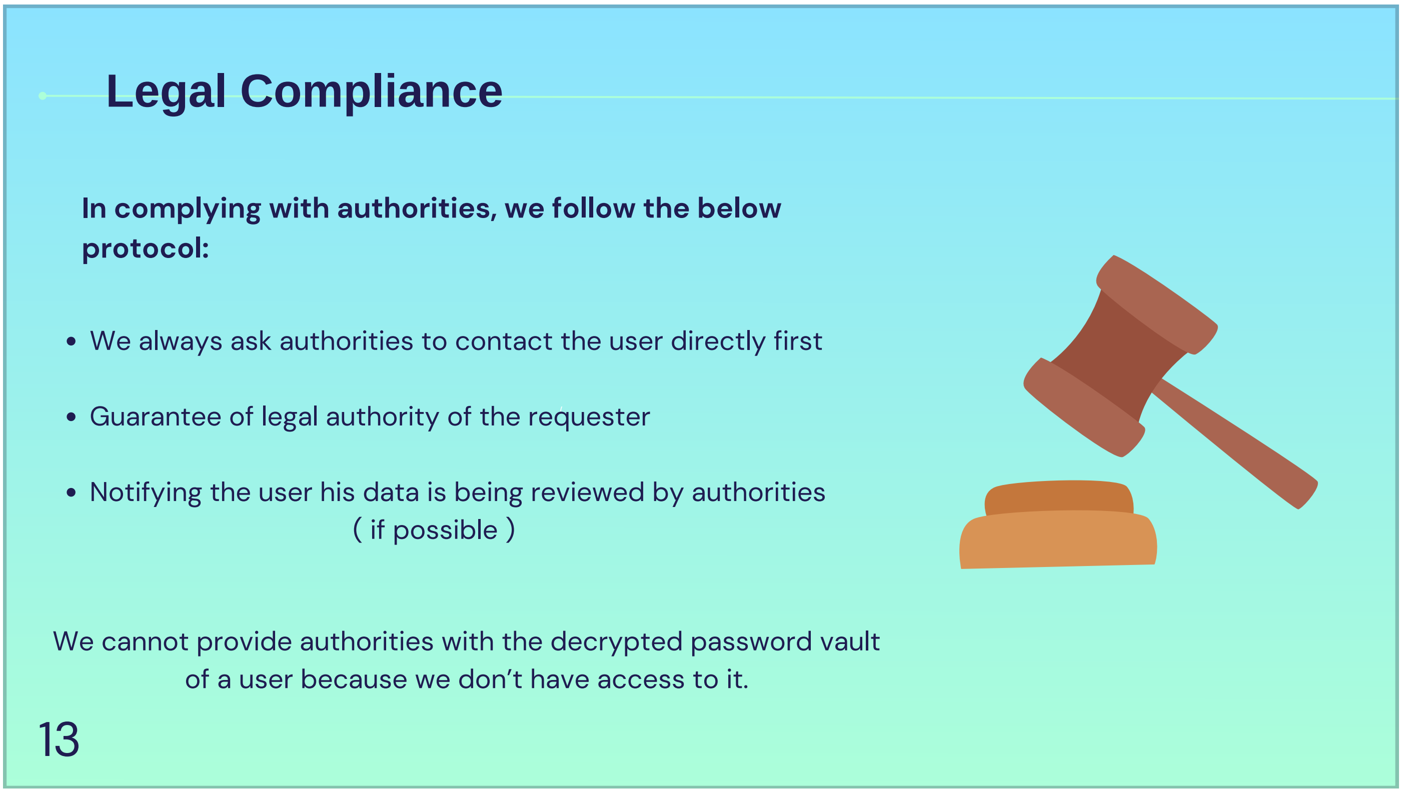
- USA State and Federal Data Protection Regulations ( CCPA, CPRA, VCDPA )

- United Kingdom Data Protection Law

- others...

In accordance with EU GDPR, SafePass has nominated a DPO ( Data Protection Officer ), that works along with the legal department to ensure the highest standards of data protection are being met.

SafePass's Legal Department is also tasked with other work, such as making sure the company's patents are up to date, no intellectual property rights are being infringed ( either our's or from other companies ) and representing the company in legal cases.



## Legal Compliance

**In complying with authorities, we follow the below protocol:**

- We always ask authorities to contact the user directly first
- Guarantee of legal authority of the requester
- Notifying the user his data is being reviewed by authorities ( if possible )

We cannot provide authorities with the decrypted password vault of a user because we don’t have access to it.

13

In complying with legal demands, SafePass still aims to protect it's users privacy as much as possi ble.

In the case of legal requests by authorities, SafePass always takes this first steps before respondi ng:

- We ask authorities to contact the given user first if possible before requesting his information  from SafePass

- Strict checks are put in place to check if the requester is in fact a governmental authority or legal  rights to do the demand of user data in question.
Without a warrant, legal process or judicial order, SafePass may refuse providing information.

- To protect the privacy of our users, we ensure the legal requests are reasonable in scope ( not  demanding information from users who may not be related to the investigation ) and will share the  minimum amount of information in order to comply with the demand.

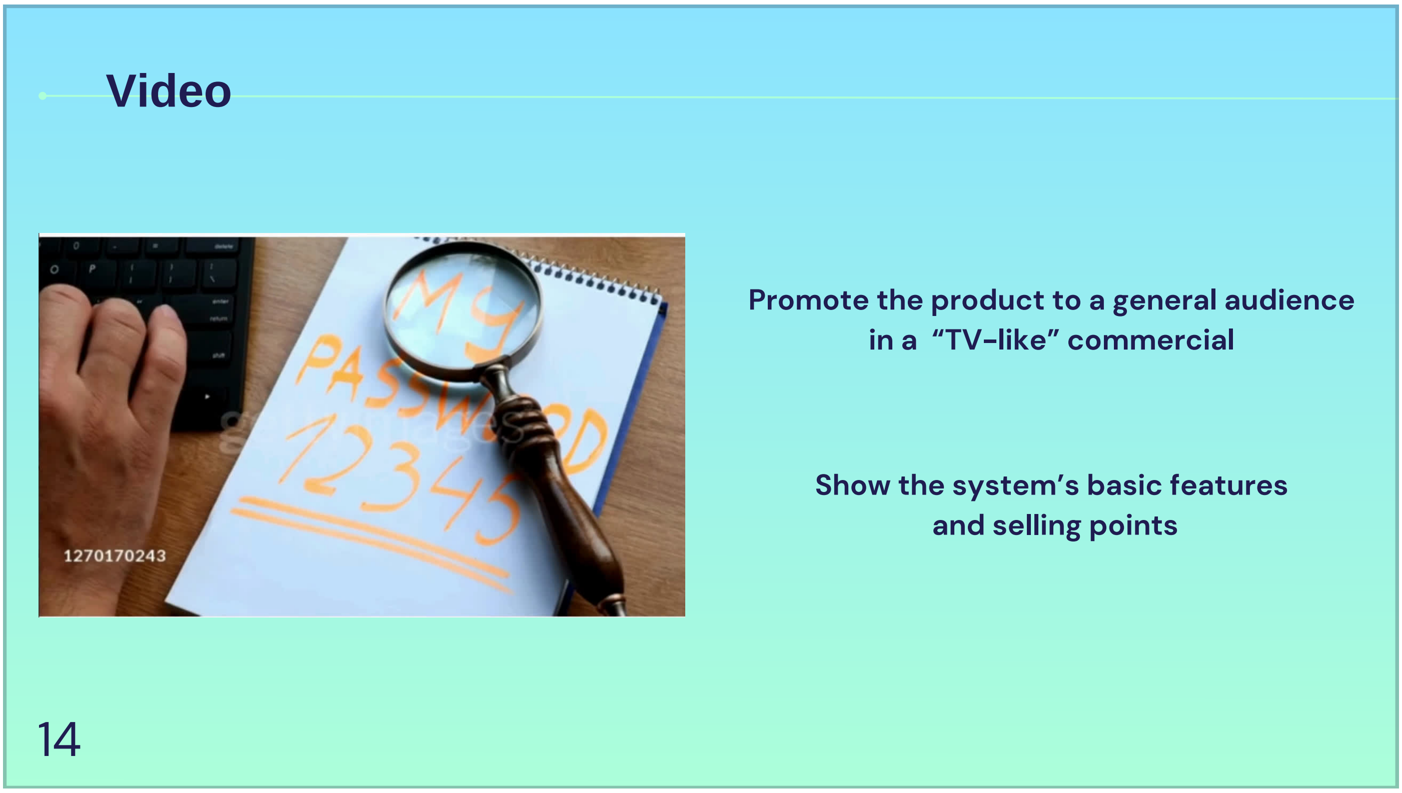
- Noticing the user ( if possible ) . If there are no legal blockades or advisory against it, SafePass  will inform the user that his data is being reviewed by legal authorities.

All requests to SafePass must be issued in accordance with the applicable laws of the region and  must be made through official government/judicial channels such as judicial orders or government  emails.

Because SafePass utilizes a Zero Knowledge Encryption Model, we do not have access to, and therefore, cannot share with authorities, unencrypted user's password vaults or their master passw ords.
Therefore, most legal requests should be issued with the given user's email, since it is linked to a user's account, or payment information, such as billing address or credit card information, in the case of a user with a paid account.

In order to help us identify the requesting authority, the following information must be provided in legal requests:

- Agency name
- Agent name and badge/identification number
- Agent employer-issued email address
- Agent phone number, including any extension
- Agent mailing address
- Requested response date



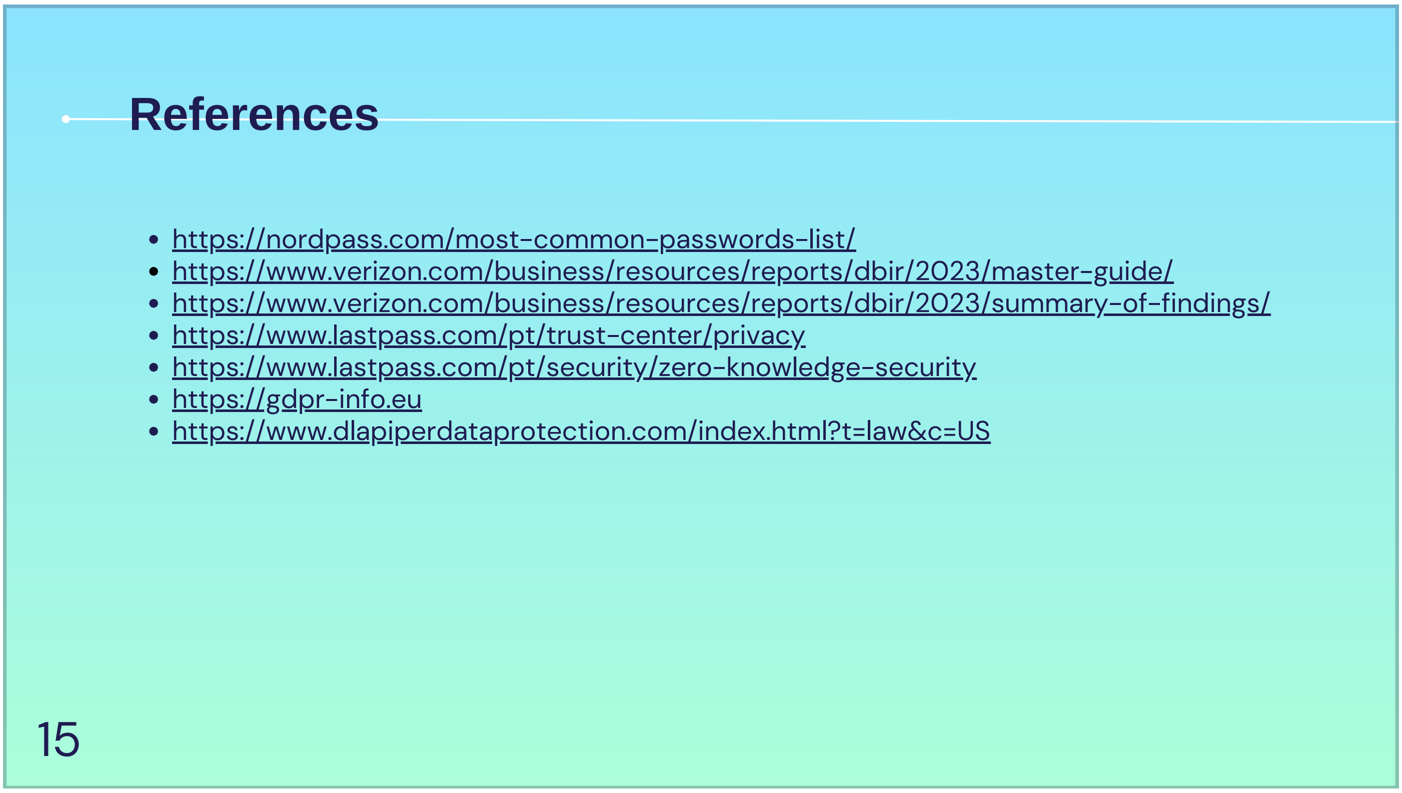
## Video

Promote the product to a general audience in a "TV-like" commercial

Show the system's basic features and selling points

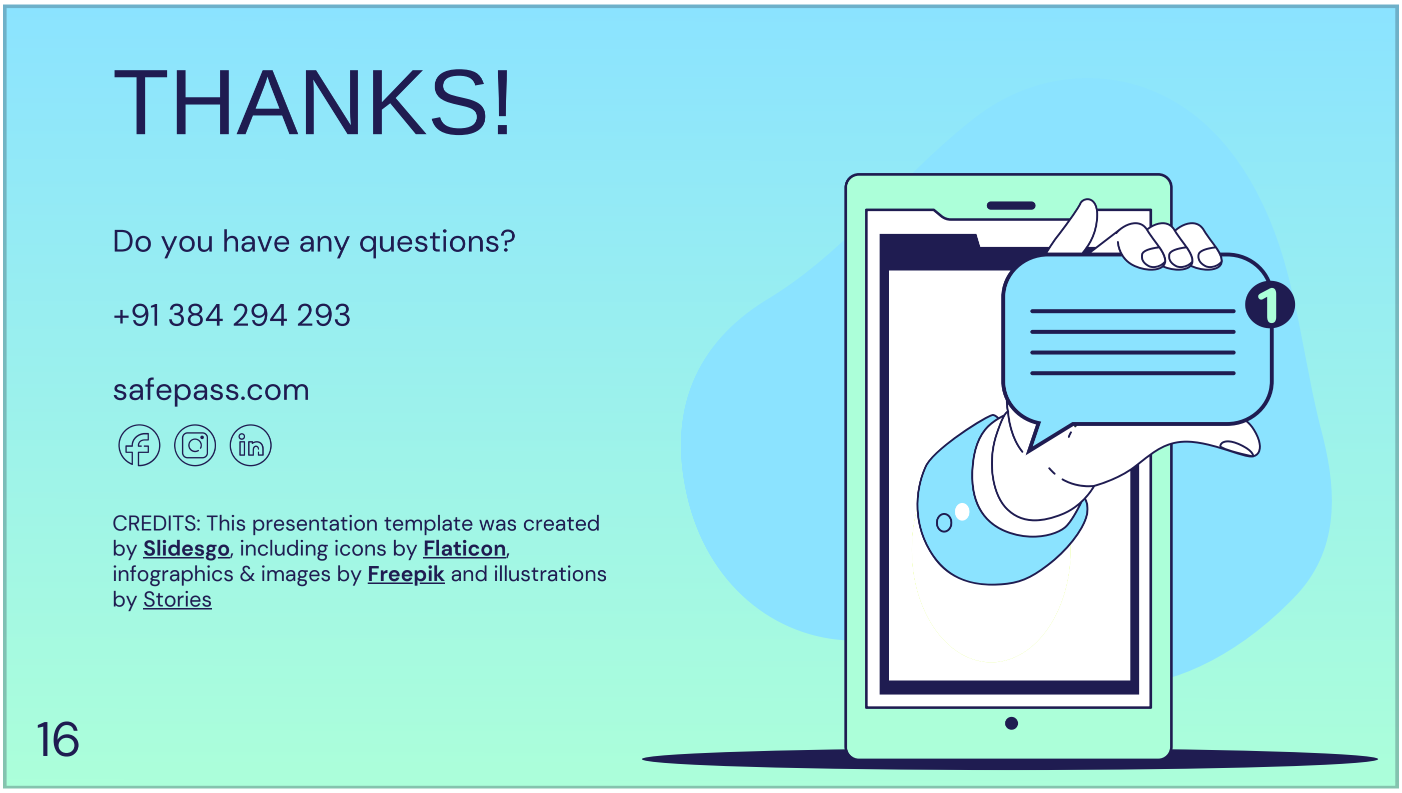
14

- Video developed with the objective of sell the system and it's main points
- Adopted "TV-like" commercial, like EHS.tv or FlexTape



## References

- https://nordpass.com/most-common-passwords-list/
- https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/
- https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/
- https://www.lastpass.com/pt/trust-center/privacy
- https://www.lastpass.com/pt/security/zero-knowledge-security
- https://gdpr-info.eu
- https://www.dlapiperdataprotection.com/index.html?t=law&c=US



# THANKS!

Do you have any questions?

+91 384 294 293

safepass.com

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by Stories

16