# LASTPASS

Your one stop shop for password / credit card management !

# Table of contents

# 01

# Introduction

# INTRODUCTION

Did you know that roughly 6.85 million accounts get hacked every single day?

According to “First Contact”, about 51% of people use the same passwords for work and personal accounts, and 53% rely on their memory to manage passwords making it much easier for cyber criminals to infiltrate our accounts.

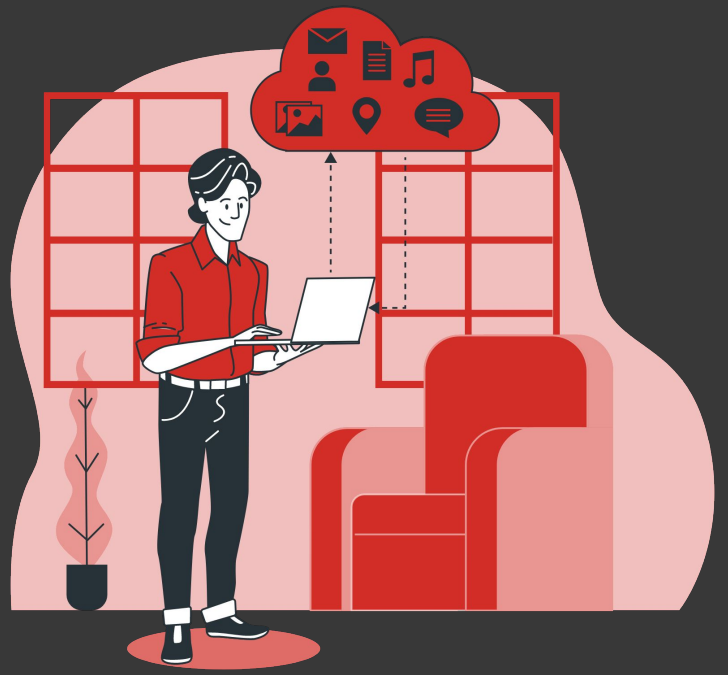
# INTRODUCTION

However, With the help of LastPass password manager, we can solve all those problems.

LastPass is helping people achieve effortless security, at home and in the workplace.

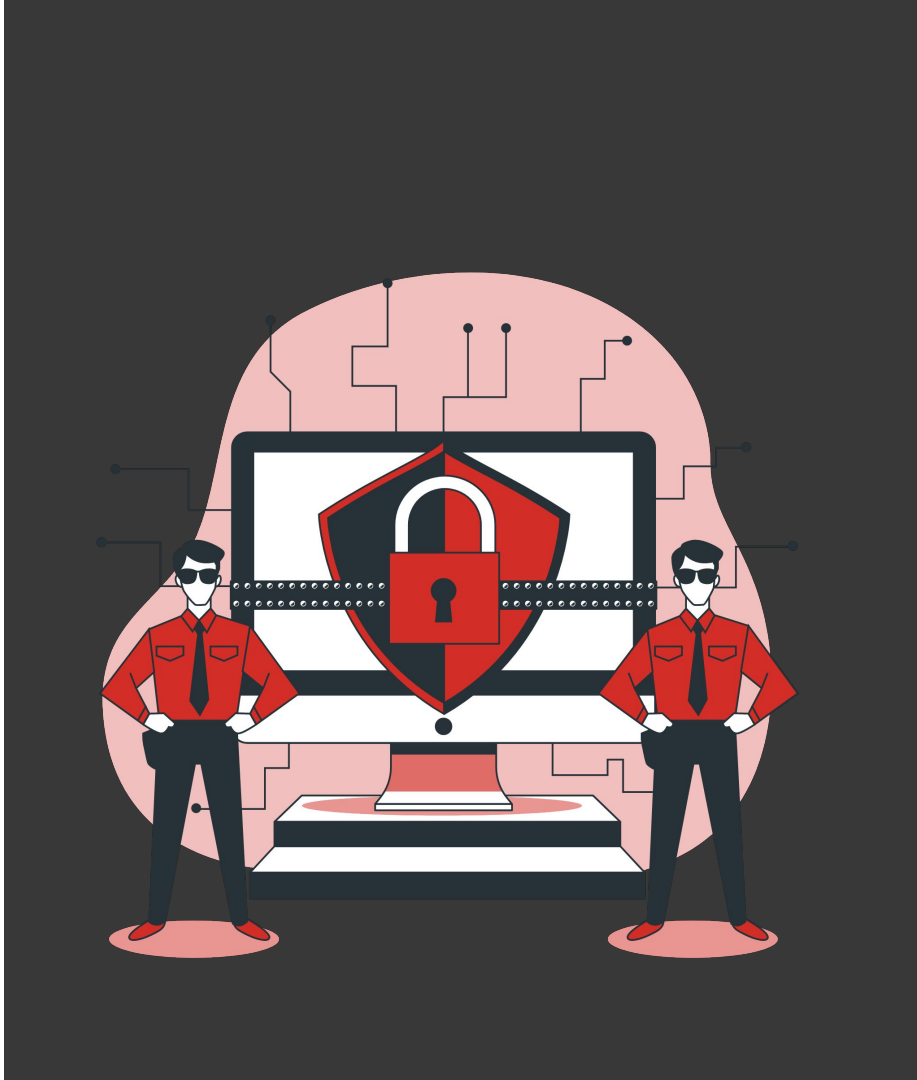
# INTRODUCTION

As our business and personal worlds intersect on an increasing scale in our cloud-centric world, a strong foundation of secure authentication and access is critical to keeping systems, data and assets safe.



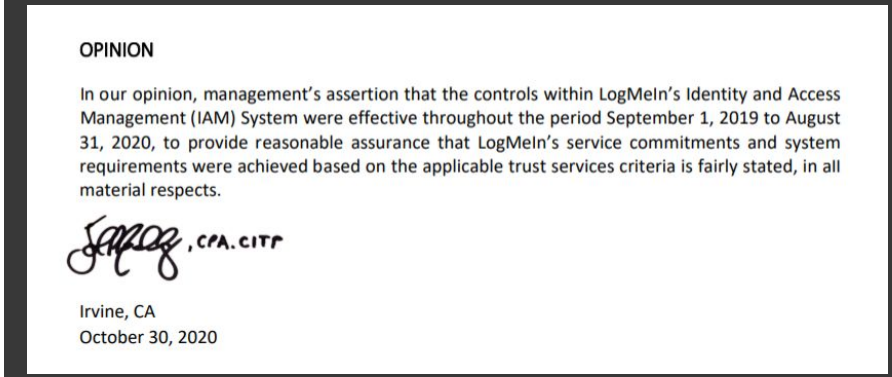
# INTRODUCTION

With lastPass, we can simplify online shopping with their built-in secure digital wallet, generate strong passwords, store sensitive records in a secure vault and even share your passwords / documents effortlessly and securely with family and friends.



# INTRODUCTION

LastPass also has SOC 2 Type ll / SOC 3 attestation reports done by a reputable auditing firm to further prove the company's dedication to Security, Privacy & Confidentiality and offering a reliable service to their user base.



**OPINION**

In our opinion, management's assertion that the controls within LogMeIn's Identity and Access Management (IAM) System were effective throughout the period September 1, 2019 to August 31, 2020, to provide reasonable assurance that LogMeIn's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

, CPA. CITP

Irvine, CA
October 30, 2020

# 02

# FR / NFR REQS

# FR / NFR

## OVERVIEW

| Lastpass Requirements | Improved / extra Lastpass requirements | Reasons the platform survived the pandemic |
|---|---|---|
| **Functional** | | |
| Free user can upgrade to premium | Premium users can self host their own private server for storing passwords instead of relying Last Pass's own server | Platform has good brand image and a robust security system |
| Free user can access their password from only one device type | Premium users can choose to use their own hosted server or Last Pass's server on their accounts | LastPass's Marketing strategy is great and effective |
| Free / premium User can register an account via any of the client applications | Free/ Premium users can enable travel mode on devices to remove all local instances of passwords when travelling to ensure no one can access passwords in case break in/ | LastPass before the pandemic was recognized as one of the best if not the best Password manager out there. It was easy for customers to choo |
| Free / premium User can login to his/her account via any of the client applications | Free/ Premium users can disable travel mode and get access of password on devices once again | LastPass is one of the older, established companies for password management which give them first comer advantage compared to newer optio |
| Free / premium user can import / export their data from other password managers | System should run basic security tests on self hosted servers to ensure it is eligible for use for password storage | The need for credit / password security increased drastically as everyone was creating purchases online during lockdown |
| Free / premium user can add different sub users / accounts ( home , business , work ) with separate vaults to promote separation of concerns | | |
| Free / premium user can Install LastPass mobile application | | |
| Free / premium user can Install web browser extension | | |
| Free / premium user can save / generate password for websites/applications in a secure vault | | |
| Free / premium user can save sensitive documents in secure storage such as legal documents, ID cards, etc... | | |
| Free / premium user can save addresses to the vault | | |
| Free / premium user can add a 2nd authentication layer such as OTP, google auth, microsoft auth, etc... | | |
| Free / premium user can save and auto-fill passwords / data on different websites/applications when needed | | |
| Free / premium user can save their credit cards in a digital wallet | | |
| Free / premium user can only send their password / documents with only one other trusted person but potentially receive from multiple people | | |
| Free / premium user can search their entire vault | | |
| Free / premium user can favourite passwords / documents in their vault | | |
| Free / premium user can add recovery phone number in case they forget their master password | | |
| Free/ Premium user can add their bank accounts | | |
| Free/ premium user can change advanced settings such as extra security email, session destruction, lastpass data detection, country restrictions, etc... | | |
| Free / premium user only has access to basic support on their questions | | |
| Premium user can access their password from any device type | | |
| Premium user can access their passwords on all their devices | | |
| Premium user can send / receive their passwords / documents with multiple trusted people | | |
| Premium user has access to priority support with their questions going to the top of the questions queue / premium email support | | |
| Premium user can see emergency contacts that they trust / contacts that trust them | | |
| Premium user can use Lastpass to autofill passwords in desktop / mobile applications | | |
| Premium user has Dark Web monitoring features to protect their account from data breaches | | |
| Premium user can add advanced multifactor options such as fingerprint authentication, Sesame, YubiKey | | |
| Premium user share credentials across equivalent domains | | |
| Premium user can add trusted devices to skip the login step | | |
| Premium user can control which mobiles devices have access to the last pass account through a UUID | | |
| Premium user can set URL rules to create a smoother experience | | |
| Premium user exclude certain websites from using lastpass ( like super sensitive bank accounts ) | | |
| Premium user can upgrade to team / family account | | |
| Premium user has a security score in his dashboard that overall accounts security and checks for reused passwords | | |
| System does 200,101 rounds of PBKDF2-SHA256 + scrypt hashing on the master key to make bruteforce attacks infeasiable | | |
| System is regularly audited and pen tested | | |
| System encryption happens using 256-bit AES and happens only at the device level | | |
| System implements 2048-bit RSA algorithm to share folders between 0 / * users | | |
| System encrypts encrypted key vault with 128-AES in CBC mode in case of account recovery | | |
| System refuses account recovery on mobile devices in case biometrics are disabled | | |
| System confirms users identity through an OTP before proceeding with account recovery | | |
| System deletes old Master key from LastPass servers in case of master key recovery | | |
| System implements a local application firewall to prevent against SQL injection and XSS (cross site scripting) attacks | | |
| System caches user vault data in the browser extension so they can access it in case of no internet connection or lastpass server downtime ( user most have logged at least once before and communicated fetched data from last pass server's ) | | |
| System authenticates login with ADFS ( Active Directory Federated Services ) to ensure zero knowledge model | | |
| System generates 3 keys for master key entered and stores them in 3 separate ADs (company/user AD, lastpass.com, local AD) | | |
| System combines keys if authentication against ADFS is successful to form master key, decrypt user vault and log them in | | |
| System contacts Lastpass server after encryption using TLS 1.2 and enforces it using HSTS (HTTP strict transport security) | | |
| **Non-Functional** | | |
| Lastpass's system is highly available through their 2N ( fully redundant ) datacenters | | |
| Lastpass's system is regularly pen tested to ensure lack of vulnerabilities | | |
| Lastpass's system user data is backed up daily on the cloud using a cloud provider such as AWS S3, or Azure services | | |
| Lastpass's code base is regularly reviewed by a technical team for security, privacy, and compliance with company policies and procedures | | |
| Lastpass's system has a SOC 2 type II / SOC 3 attestation tests which ensure that they're systems are audited for security, privacy and confidentiality | | |

# FR / NFR

## FREE / PREMIUM

| |
|---|
| Free user can upgrade to premium |
| Free user can access their password from only one device type |
| Free / premium User can register an account via any of the client applications |
| Free / premium User can login to his/her account via any of the client applications |
| Free / premium user can import / export their data from other password managers |
| Free / premium user can add different sub users / accounts ( home , business , work ) with separate vaults to promote separation of concerns |
| Free / premium user can install LastPass mobile application |
| Free / premium user can install web browser extension |
| Free / premium user can save / generate password for websites/applications in a secure vault |
| Free / premium user can save sensitive doucments in secure storage such as legal documents, ID cards, etc... |
| Free / premium user can save addresses to the vault |
| Free / premium user can add a 2nd authentication layer such as OTP, google auth, microsoft auth, etc... |
| Free / premium user can save and auto-fill passwords / data on different websites/applications when needed |
| Free / premium user can save their credit cards in a digital wallet |
| Free / premium user can only send their password / documents with only one other trusted person but potentially receive from multiple people |
| Free / premium user can search their entire vault |
| Free / premium user can favourite passwords / doucments in their vault |
| Free / premium user can add recovery phone number in case they forget their master password |
| Free/ Premium user can add their bank accounts |
| Free/ premium user can change advanced settings such as extra security email, session destruction, lastpass data detection, country restrictions, etc... |
| Free / premium user only has access to basic support on their questions |

# FR / NFR

## PREMIUM

| |
|---|
| Premium user can access their password from any device type |
| Premium user can access their passwords on all their devices |
| Premium user can send / receive their passwords / documents with multiple trusted people |
| Premium user has access to priority support with their questions going to the top of the questions queue / premium email support |
| Premium user can see emergency contacts that they trust / contacts that trust them |
| Premium user can use Lastpass to autofill passwords in desktop / mobile applictions |
| Premium user has Dark Web monitoring features to protect their account from data breaches |
| Premium user can add advanced multifactor options such as fingerprint authentication, Sesame, YubiKey |
| Premium user share credentials across equivalent domains |
| Premium user can add trusted devices to skip the login step |
| Premium user can control which mobiles devices have access to the last pass account through a UUID |
| Premium user can set URL rules to create a smoother experience |
| Premium user exclude certain websites from using lastpass ( like super sensitive bank accounts ) |
| Premium user can upgrade to team / family account |
| Premium user has a security score in his dashboard that overall accounts security and checks for reused passwords |

# FR / NFR

## SYSTEM

System does 200,101 rounds of PBKDF2-SHA256 + scrypt hashing on the master key to make bruteforce attacks infeasiable
System is regurarly audited and pen tested
System encryption happens using 256-bit AES and happens only at the device level
System implements 2048-bit RSA algorithm to share folders between 0 / * users
System encrypts encrypted key vault with 128-AES in CBC mode in case of account recovery
System refuses account recovery on mobile devices in case biometrics are disabled
System confirms users identity through an OTP before proceeding with account recovery
System deletes old Master key from LastPass servers in case of master key recovery
System implements a local application firewall to prevent against SQL injection and XSS (cross site scripting) attacks
System caches user vault data in the browser extension so they can access it in case of no internet connection or lastpass server downtime ( user must have logged at least once before and communicated fetched data from last pass server's )
System autenticates login with ADFS ( Active Directory Federated Services ) to ensure zero knowledge model
System generates 3 keys for master key entered and stores them in 3 separate ADs (company/user AD, lastpass.com, local AD)
System combines keys if authentication against ADFS is successful to form master key, decrypt user vault and log them in
System contacts Lastpass server after encryption using TLS 1.2 and enforces it using HSTS (HTTP strict transport security)

# FR / NFR

## NFR

| Non-Functional |
| --- |
| Lastpass's system is highly available through their 2N ( fully redundant ) datacenters |
| Lastpass's system is regurarly pen tested to ensure lack of vulnerabliities |
| Lastpass's system user data is backed up daily on the cloud using a cloud provider such as AWS SC3, or Azure services |
| Lastpass's code base is regurarly reviewed by a techincal team for security, privacy, and compliance with company policies and proceduers |
| Lastpass's system has a SOC 2 type II / SOC 3 attestation tests which ensure that they're systems are audited for security, privacy and confidentiallity |

# 03

# Reasons of Survival

# Reasons of survival

- Platform has good brand image and a robust security system
- LastPass's Marketing strategy is great and effective
- LastPass before the pandemic was recognized as one of the best if not the best Password manager out there. It was easy for customers to choose it over competition
- LastPass is one of the older, established companies for password management which give them first comer advantage compared to newer options like bitwarden ( which was founded in 2016 )
- The need for credit / password security increased drastically as everyone was creating purchases online during lockdown

# 04

# IMPROVED FR / NFR

# Improved FR / NFR

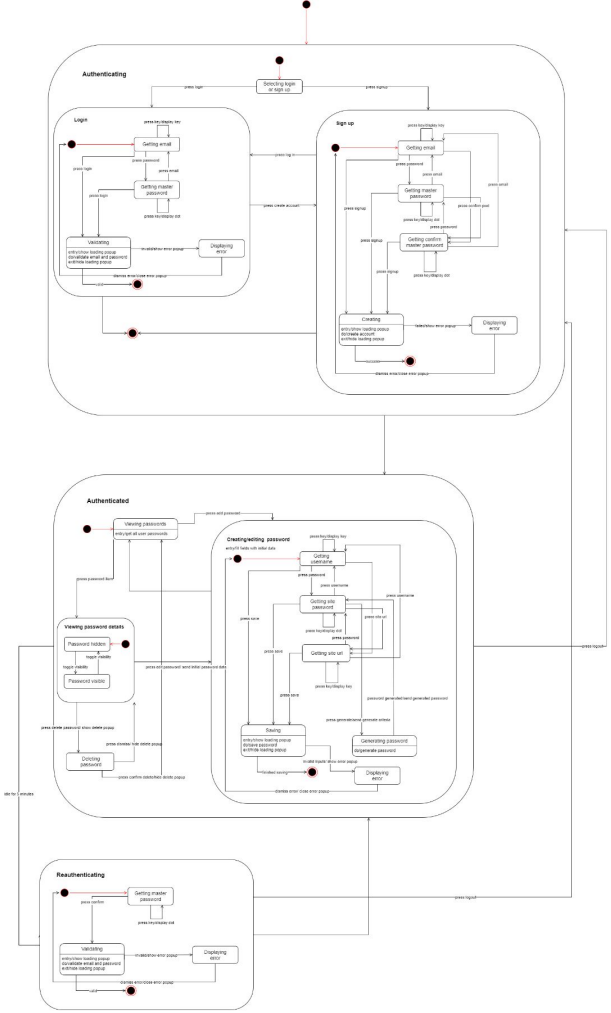
- Premium users can self host their own private server for storing passwords instead of relying Last Pass's own server
- Premium users can choose to use their own hosted server or LastPass server on their accounts
- Free/ Premium users can enable travel mode on devices to remove all local instances of passwords when travelling to ensure no one can access passwords in case break in/ theft of device
- Free/ Premium users can disable travel mode and get access of password on devices once again
- System should run basic security tests on self hosted servers to ensure it is eligible for use for password storage

# 05

# FSM APP FLOW

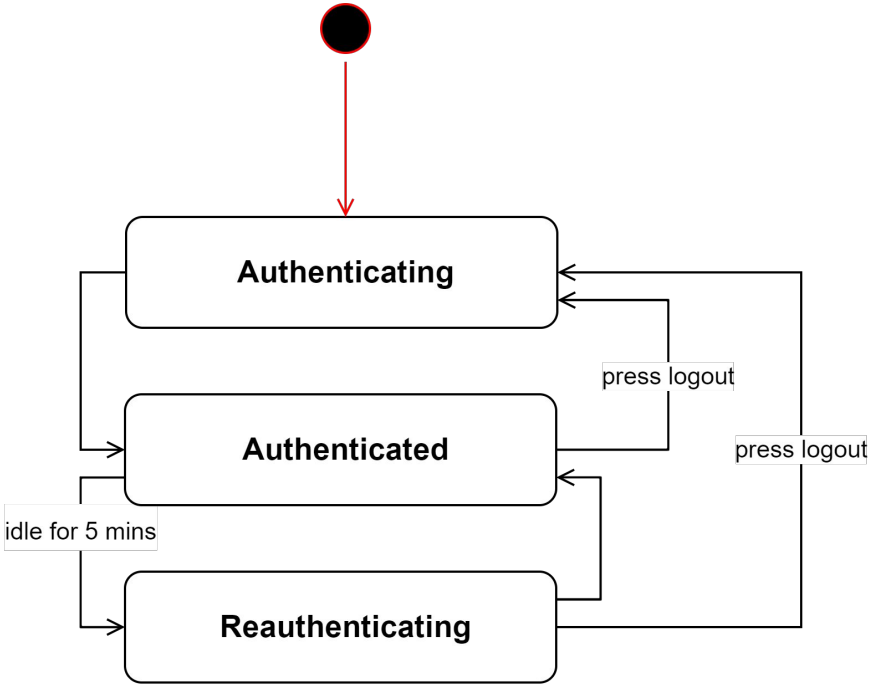
# APP FLOW

## FULL FSM



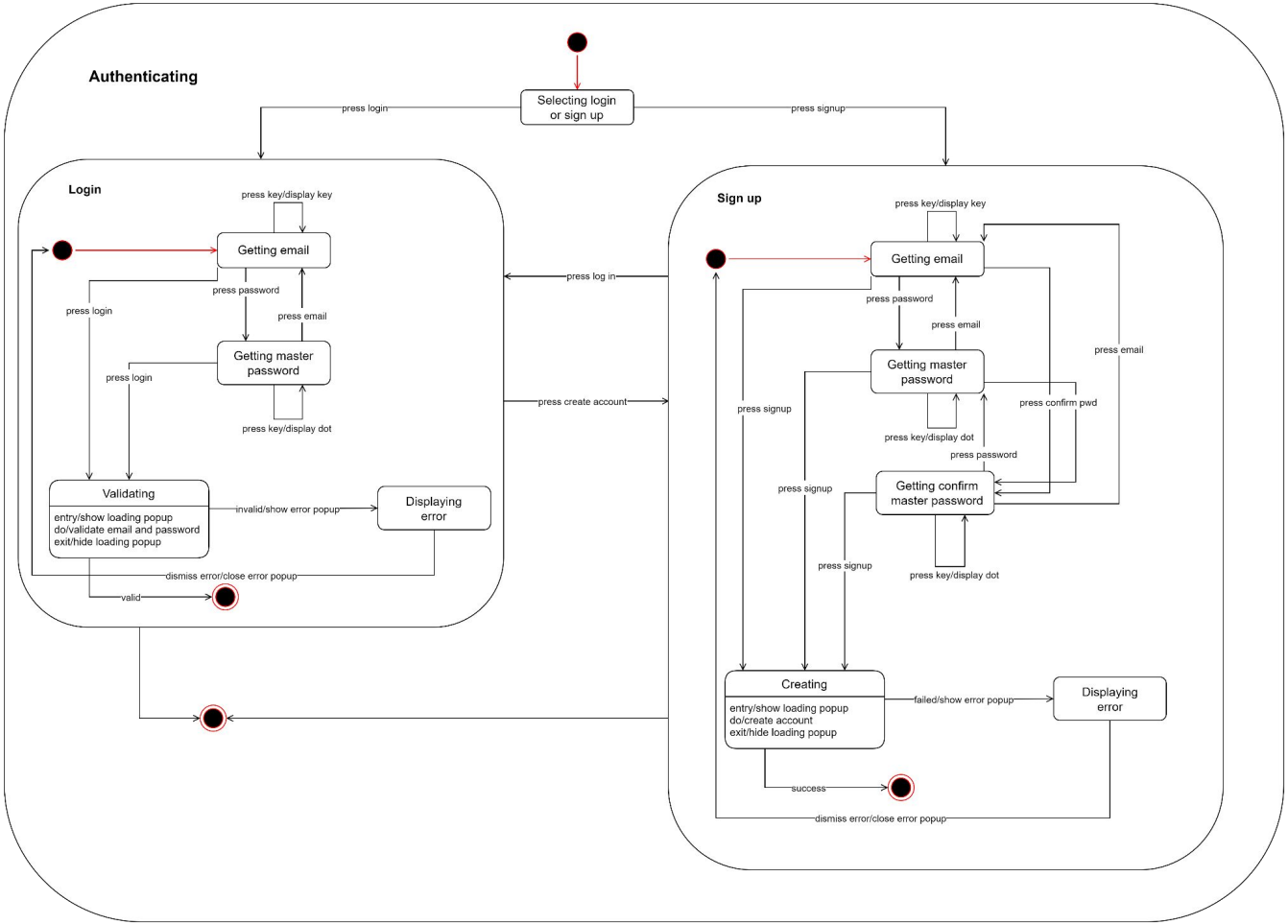
# App Flow

## Overview



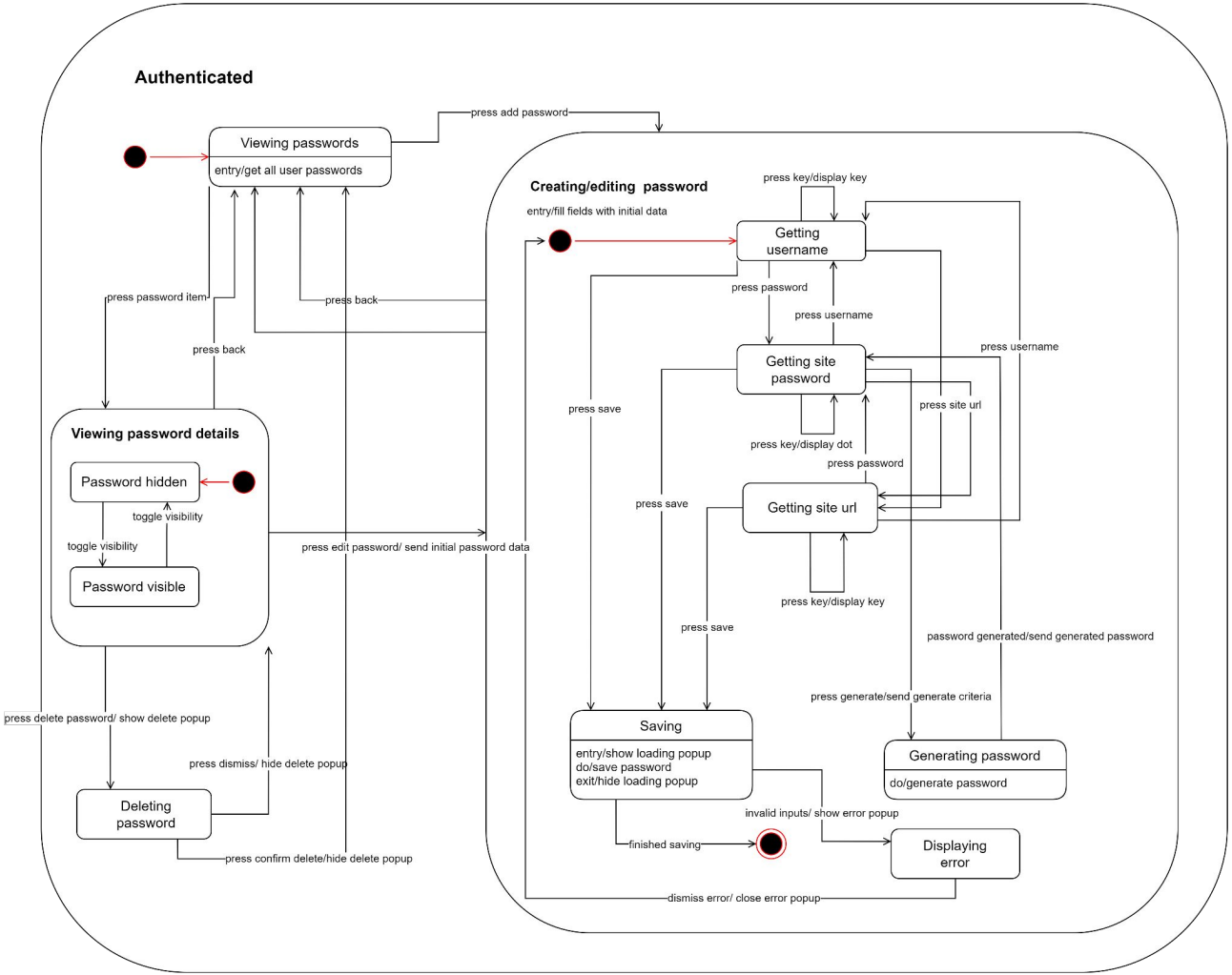
# App Flow

## Authenticating State



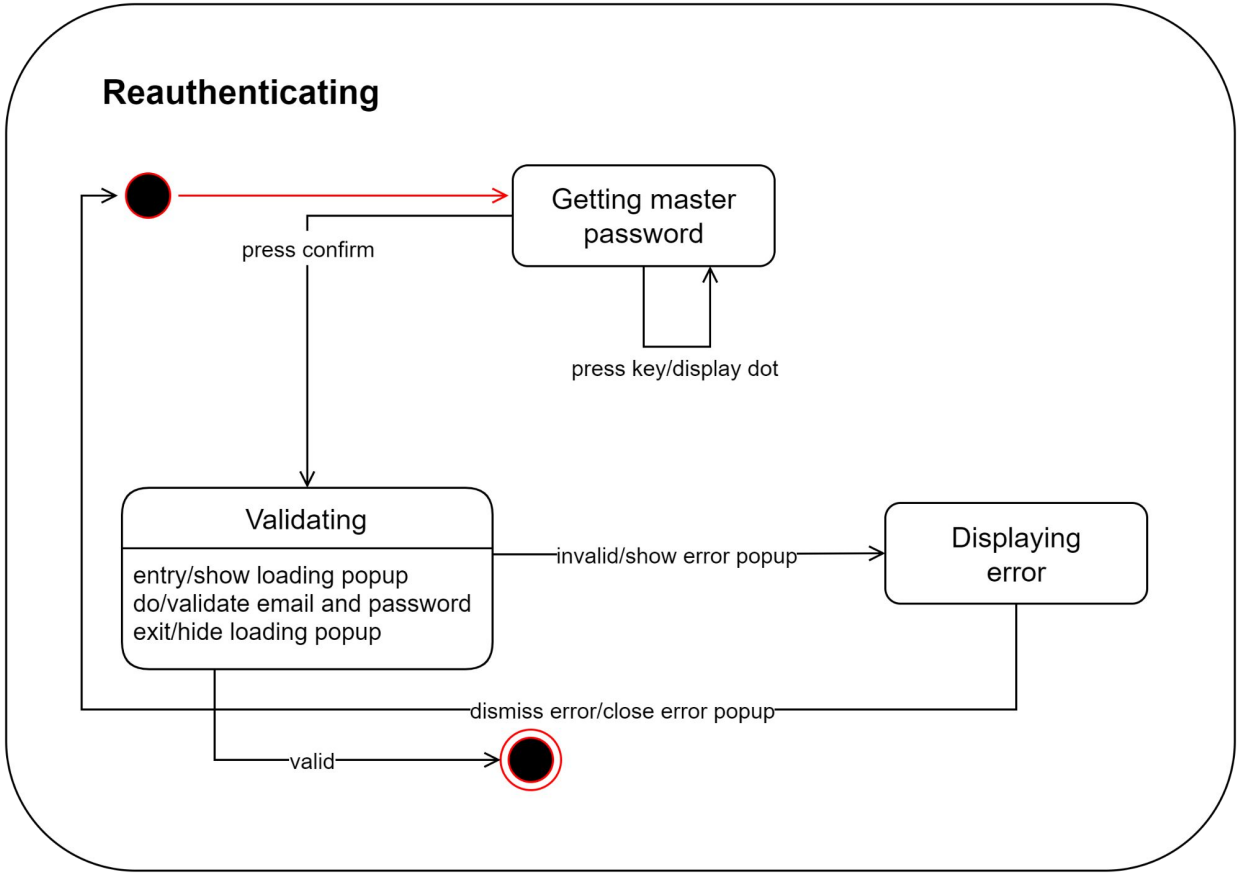
# App Flow

## Authenticated State



# App Flow

## Reauthenticating State

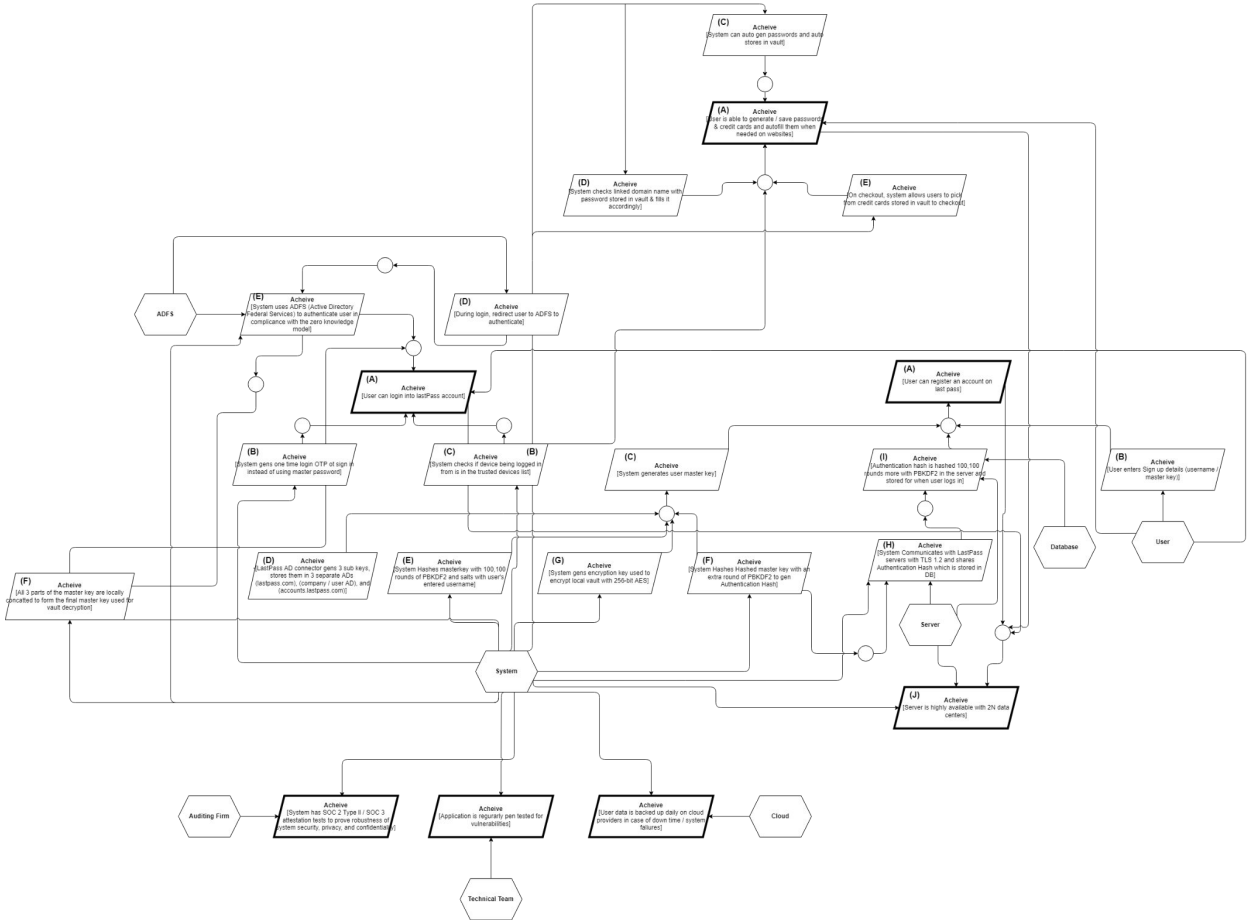


# 06

# KAOS Goal Model

# KAOS Goal Model

## Overview



# THANKS

Do you have any question?

# References:


- LastPass WhitePaper: https://assets.cdngetgo.com/1d/ee/d051d8f743b08f83ee8f3449c15d/lastpass-technical-whitepaper.pdf

- LastPass Website: lastpass.com

- What is ADFS: https://www.youtube.com/watch?v=xWWb7S6OvFI&t=41s&ab_channel=NetworkedMinds

- What is a SOC 2 / 3 attestation report: https://linfordco.com/blog/what-is-soc-2/


slidesgo