Ascenda

STRATEGIES & BEST PRACTICES

# Building a Resilient MFA Framework

HIEU NGUYEN (hieuk09) – AUGUST 2023

# Agenda

01 Introduction: What is MFA and why is it important?

02 Strategy to build an MFA framework

03 Pros & Cons and possible improvements

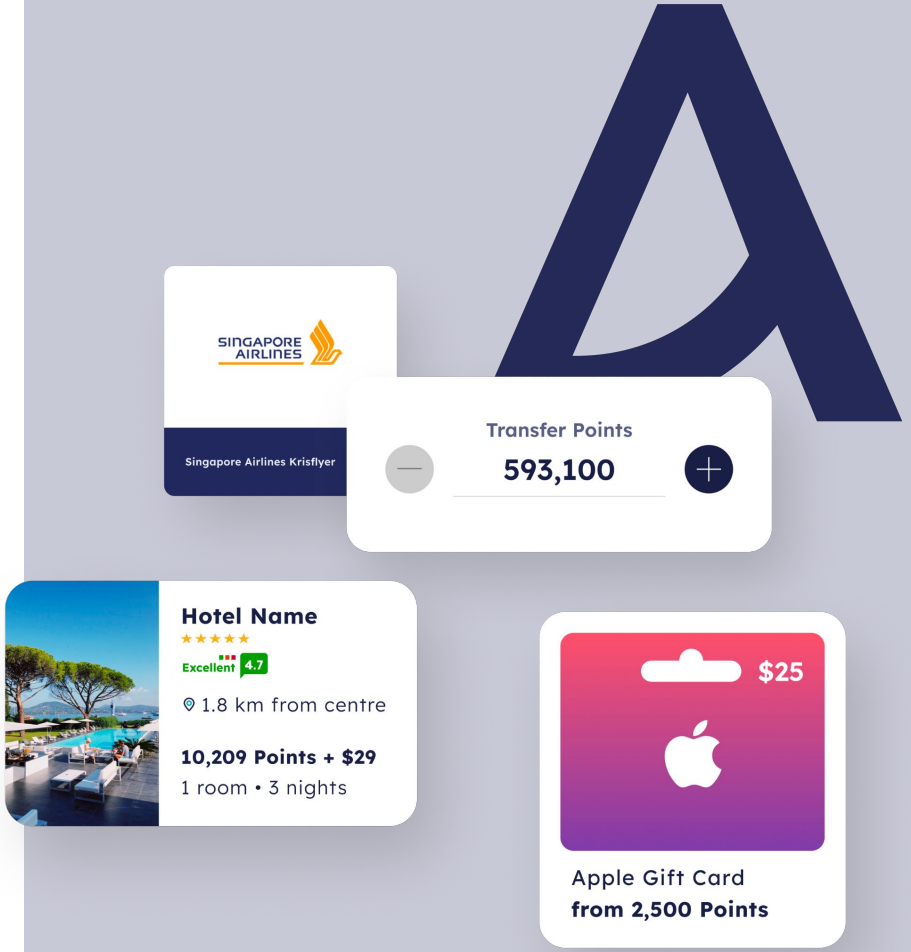
WHO ARE WE?

# About Ascenda

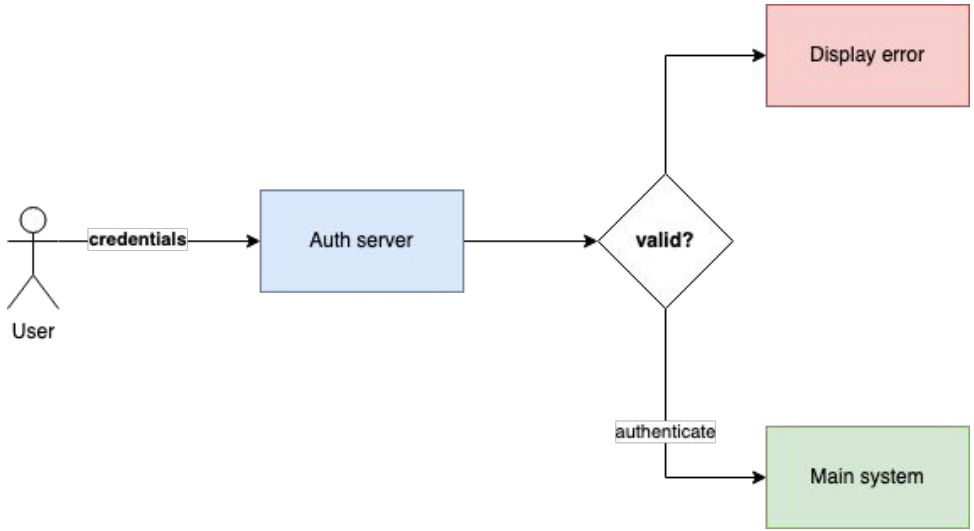
B2B2C

Provide loyalty solutions for financial institutions

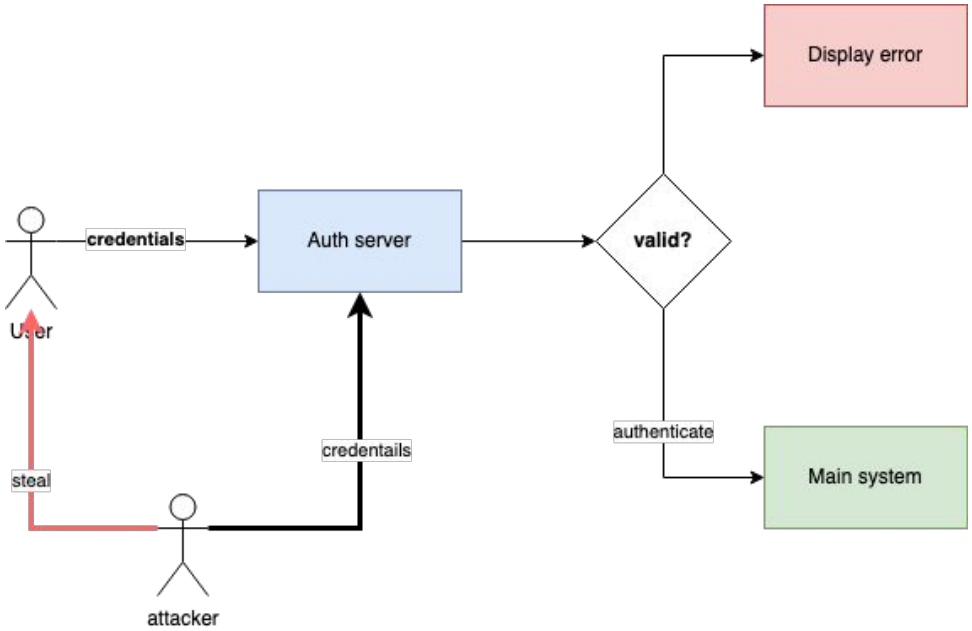
Built using Rails and Hanami



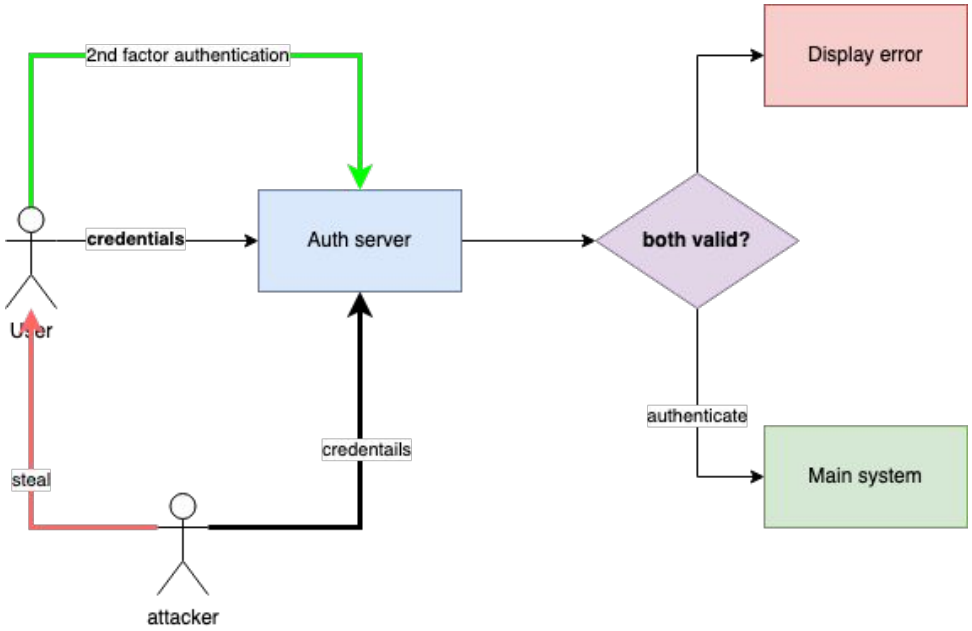
# How do we verify ownership of account?



# Compromised credentials?



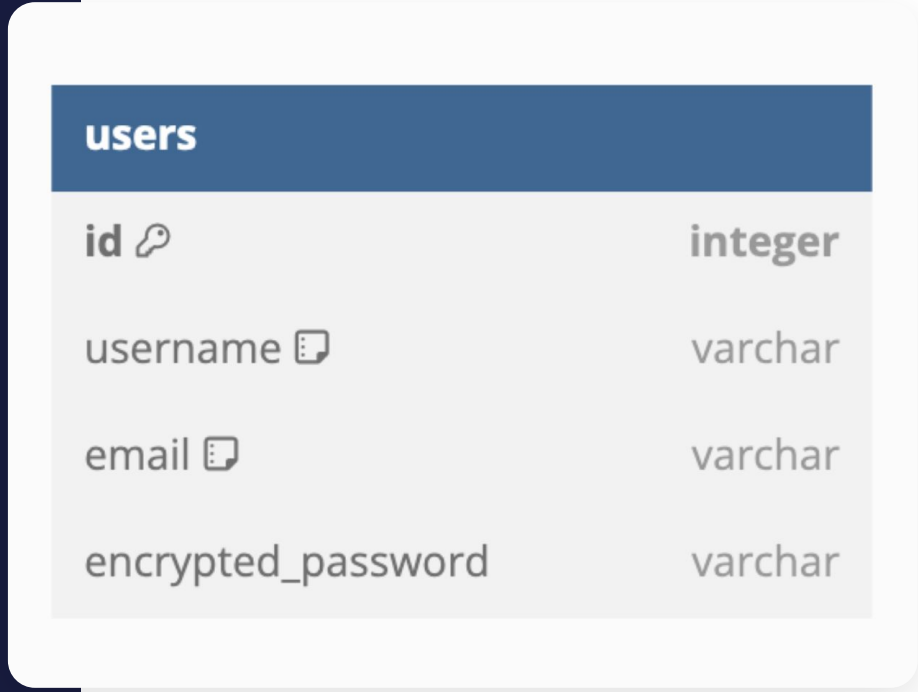
# Multi-factor authentication



# Traditional approach

1st factor authentication →

2nd factor authentication →

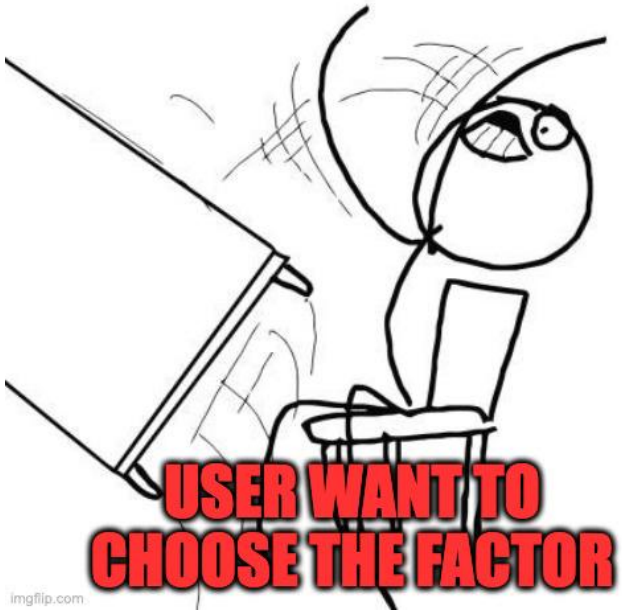


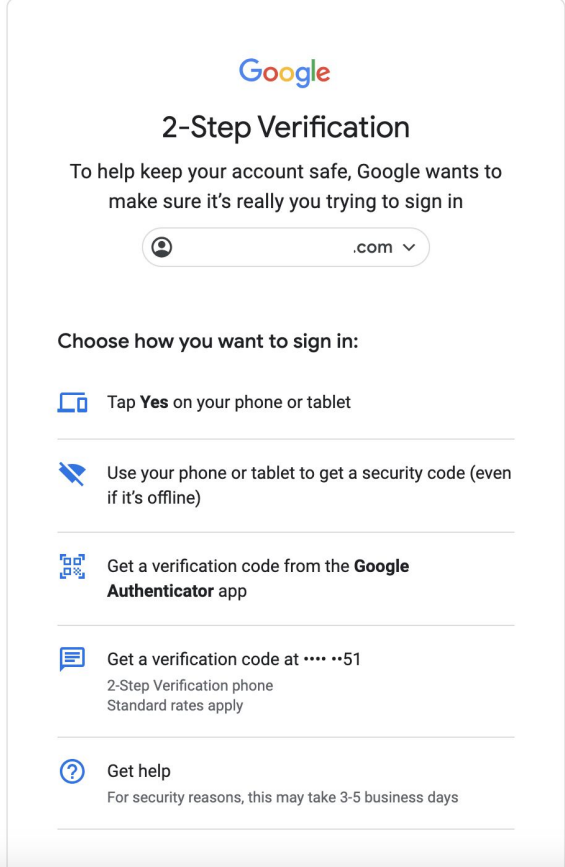
# Traditional approach

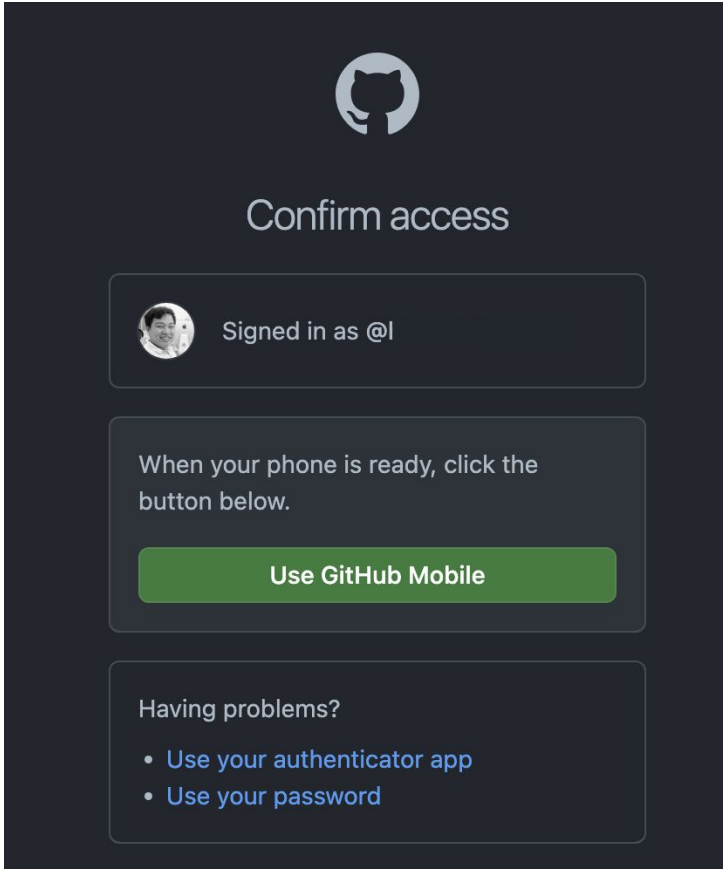
```
if user = authenticate(username, password)
  if require_mfa?(user)
    trigger_mfa(user.email)
  end
else
  # render error
end
```

# Drawbacks


NEED TO ADD NEW
AUTHENTICATION FACTOR
imgflip.com

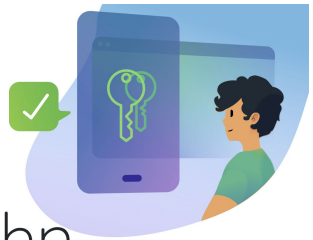

USER WANT TO
CHOOSE THE FACTOR
imgflip.com


Google
2-Step Verification
To help keep your account safe, Google wants to make sure it's really you trying to sign in
.com
Choose how you want to sign in:
Tap Yes on your phone or tablet
Use your phone or tablet to get a security code (even if it's offline)
Get a verification code from the Google Authenticator app
Get a verification code at •••• ••51
2-Step Verification phone
Standard rates apply
Get help
For security reasons, this may take 3-5 business days


Confirm access
Signed in as @l
When your phone is ready, click the button below.
Use GitHub Mobile
Having problems?
Use your authenticator app
Use your password

# Existing solution

## Devise-Two-Factor Authentication



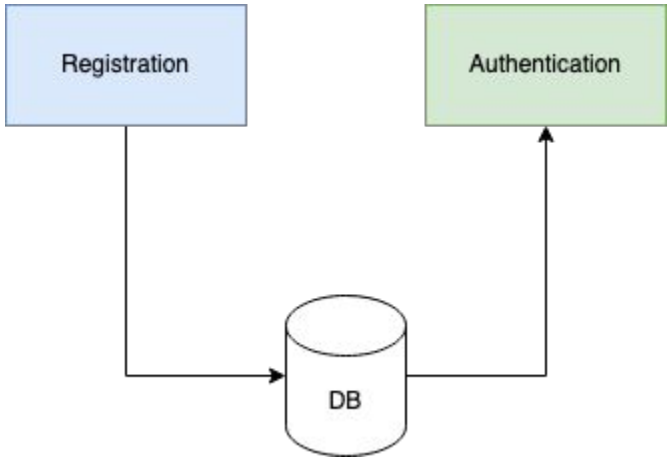
WebAuthn

## The Ruby One Time Password Library

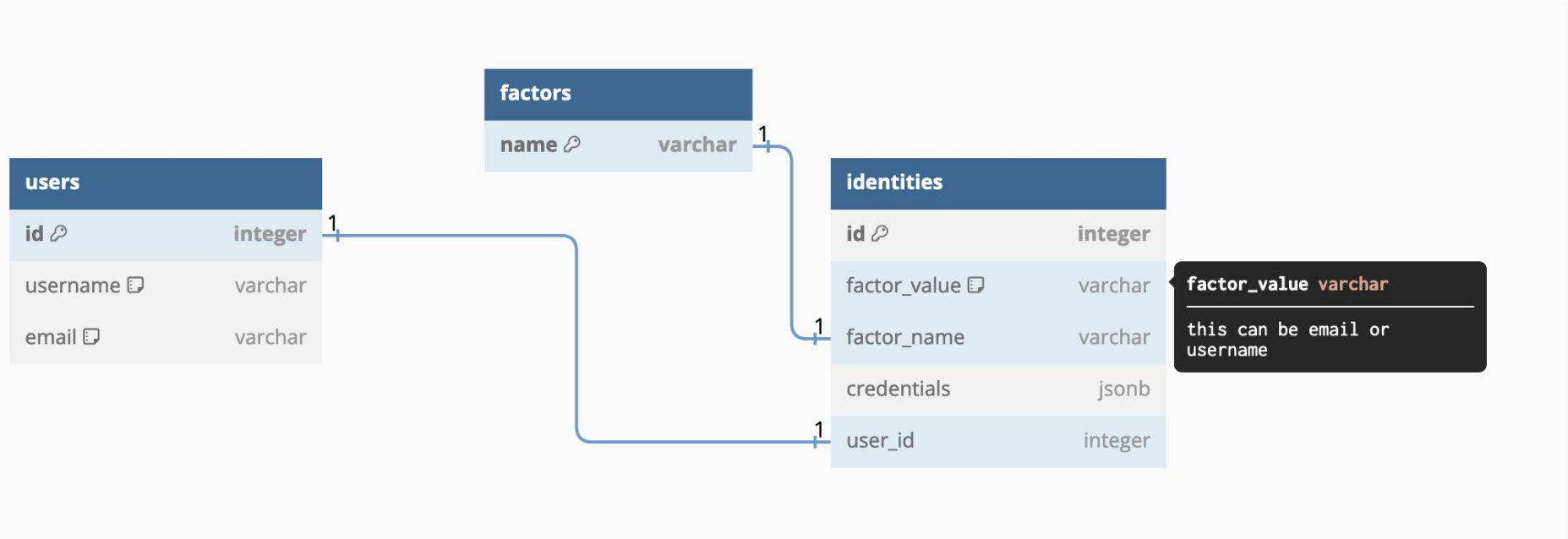
Tests passing | gem version 6.2.2 | docs rdoc.info | license MIT

# Multi-factor Authentication

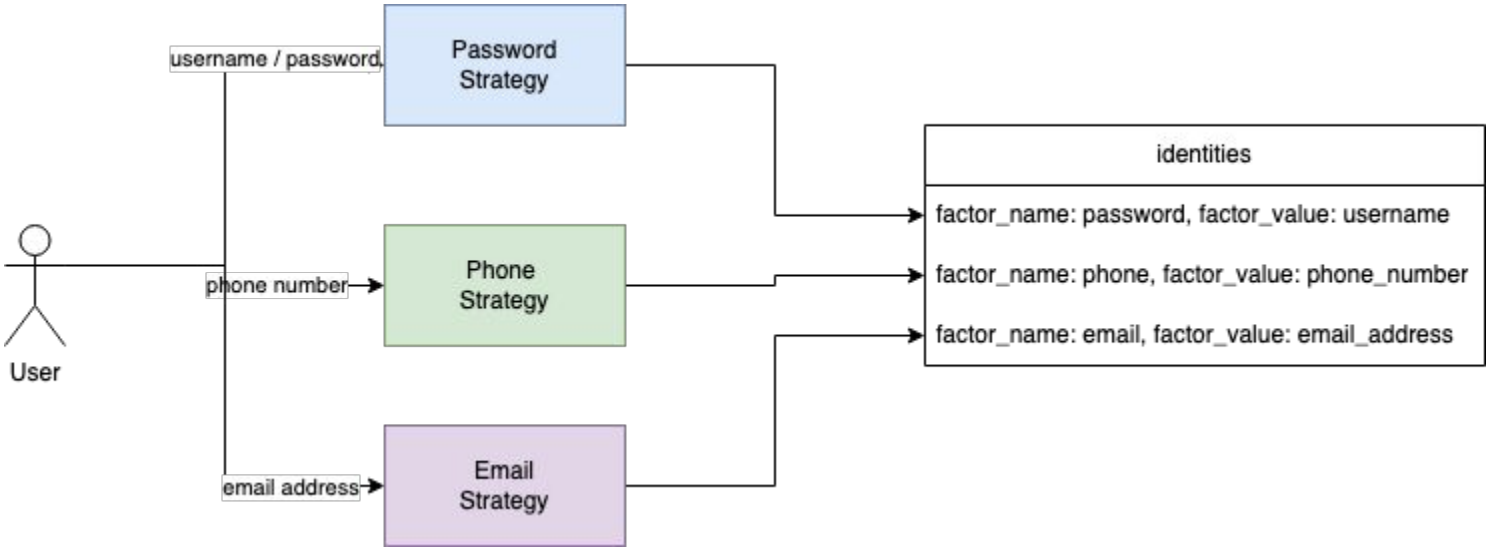
# Main flow



# Database schema



# Registration



# Why identity?

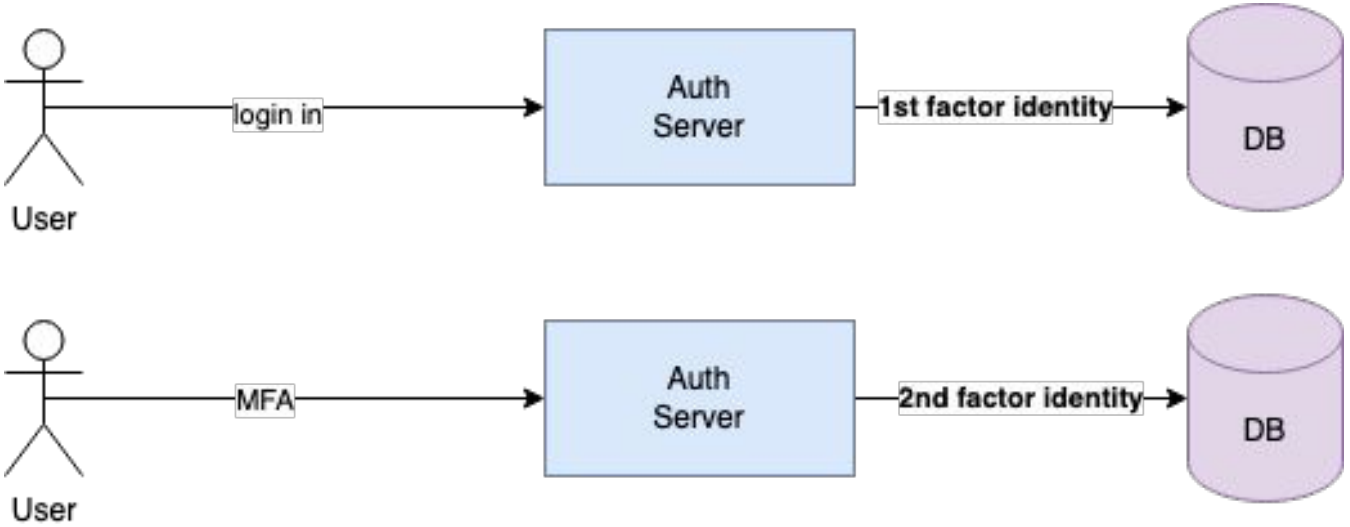
## Flexibility

- More identities per factor
- Separate credentials

## Maintainability

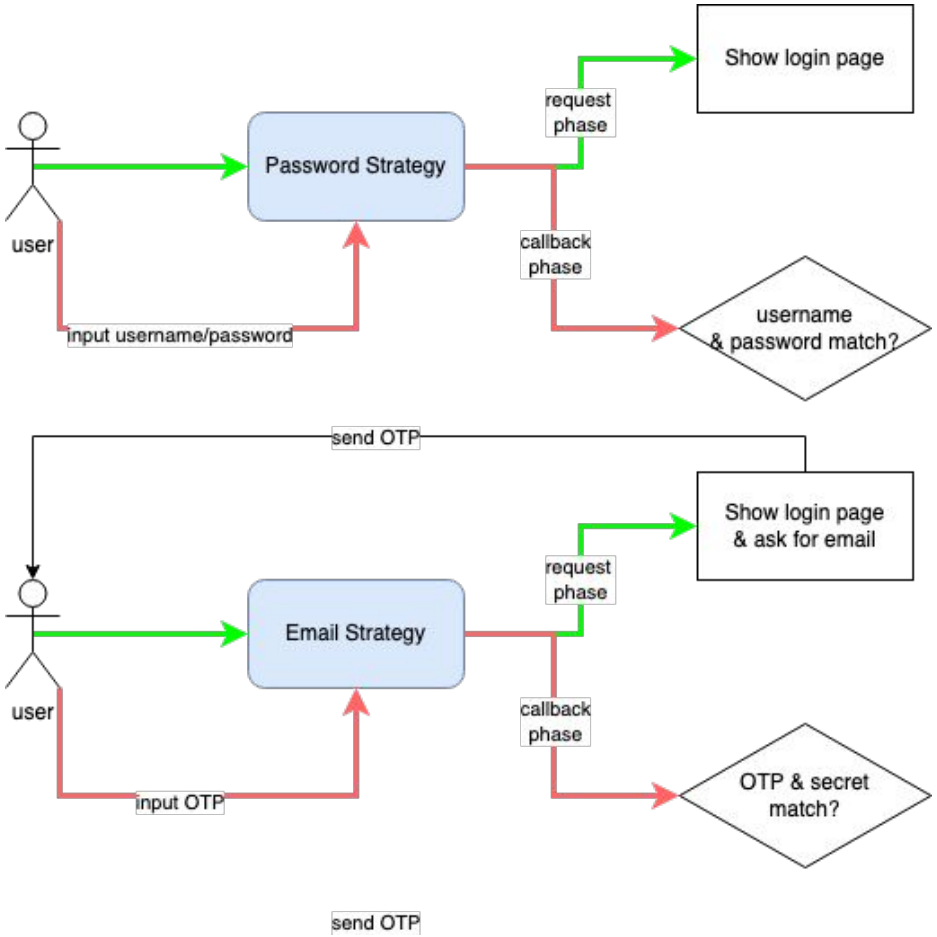
## Unified flow

# Authentication

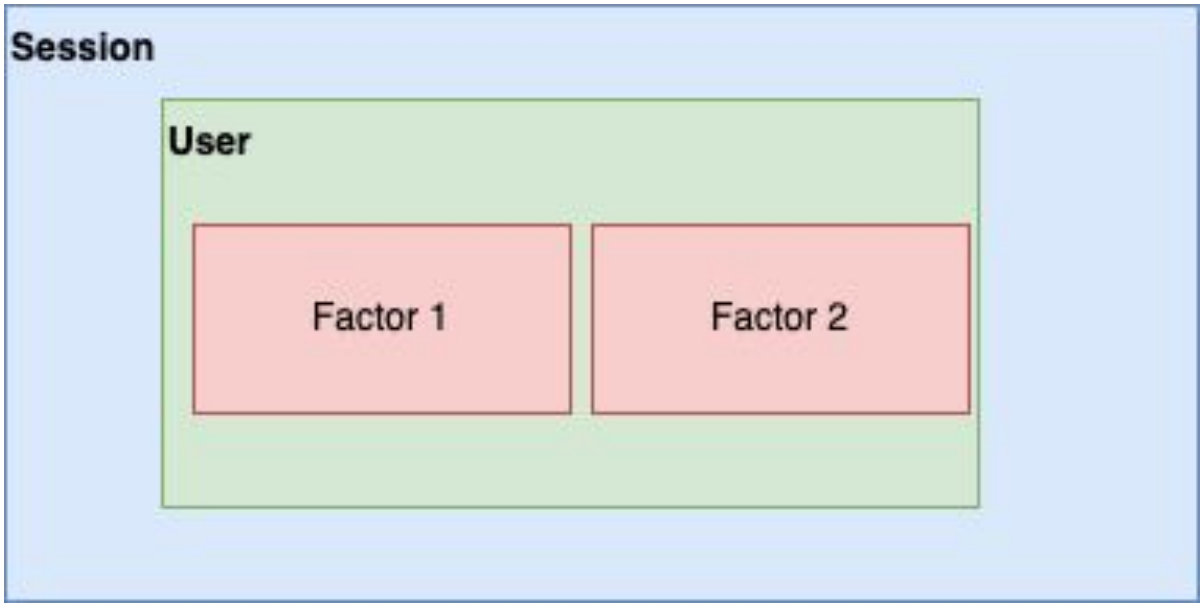


# Authentication

```
if user = authenticate(factor, credentials)
  if require_mfa?(user, session)
    identities = user.remaining_identities(factor)
    trigger_mfa(identities)
  end
else
  # render error
end
```



# Store factor in session



# Advantages

Can use all factors for login or MFA

Adding new factor verify easily

Can enable/ disable each factor separately

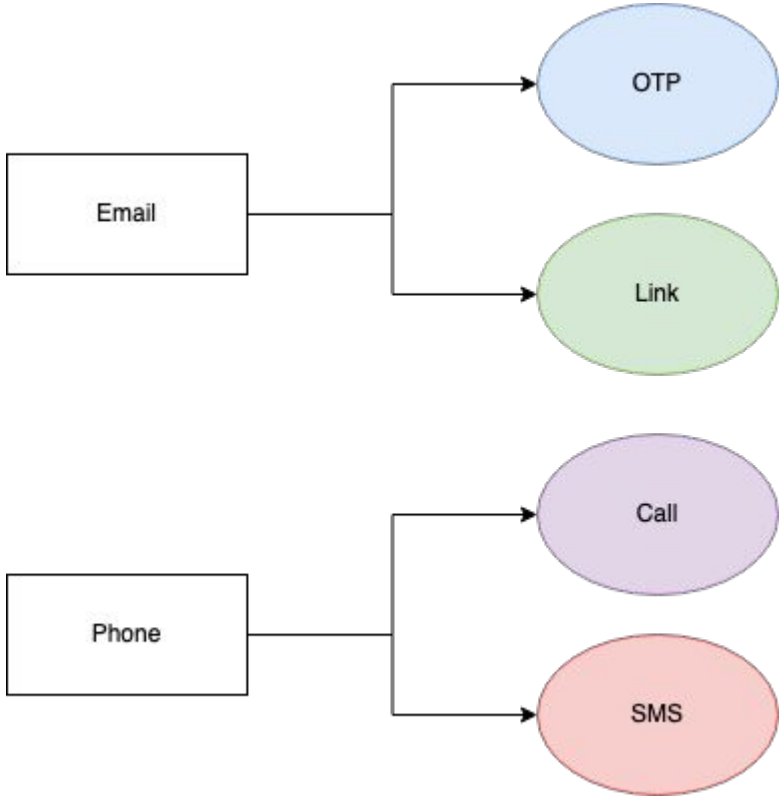
# Drawbacks

More complex (overkill in some scenarios)

Can be harder to implement some factors

# Possible improvements

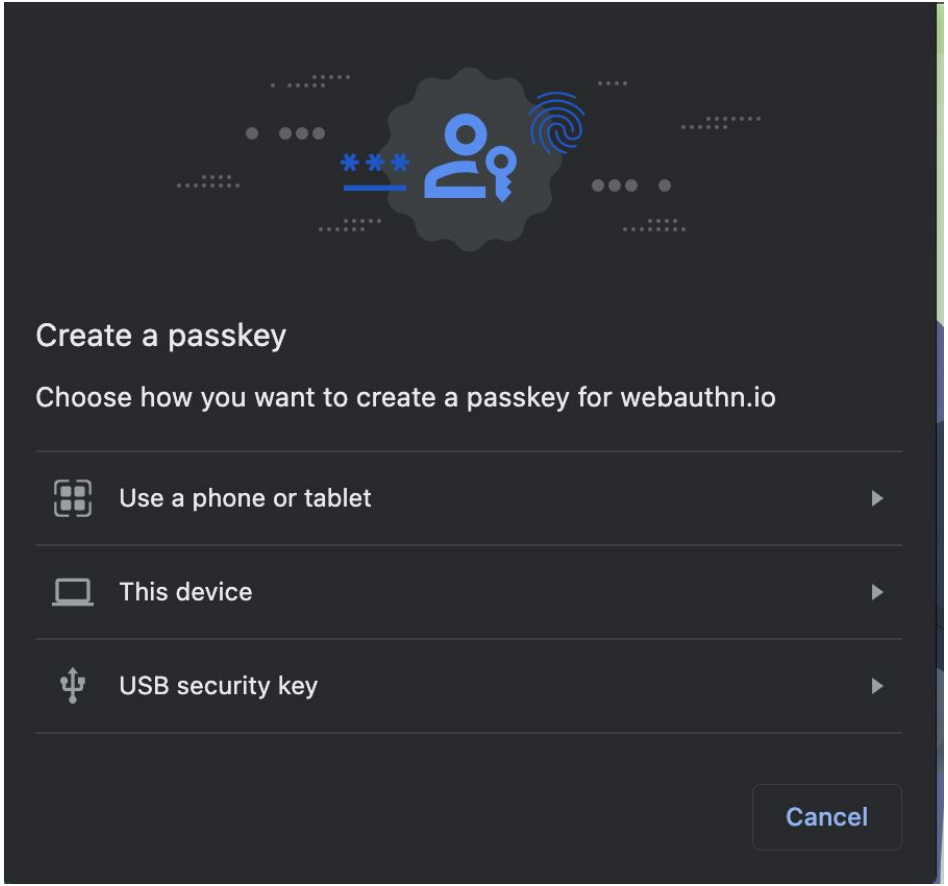
Each factor can have different verification type



# Possible improvements

Non-persisted identities

- Other sessions
- FIDO platform verification



# Take away

1

MFA is **authentication**, first and foremost

2

Storing authentication data as **identities** makes thing more flexible and maintainable

3

Using **strategy** to separate authentication factor implementation from main flow

# Q&A