Deploying 2FA To Millions of Users

Emanuele Cesena
ema@pinterest.com
@0x0ece

Emanuele Cesena

Security Engineer

Built 2FA,
focusing on Product & Ads

Co-Founder

Making open source
security keys


v1.2
Solo
@SoloKeysSec

Agenda

1. Intro
2. Design
3. Login
4. Enable
5. Juicy details

Agenda

1. Intro
2. Design
3. Login
4. Enable
5. Juicy details

Definition

Two-Factor Authentication

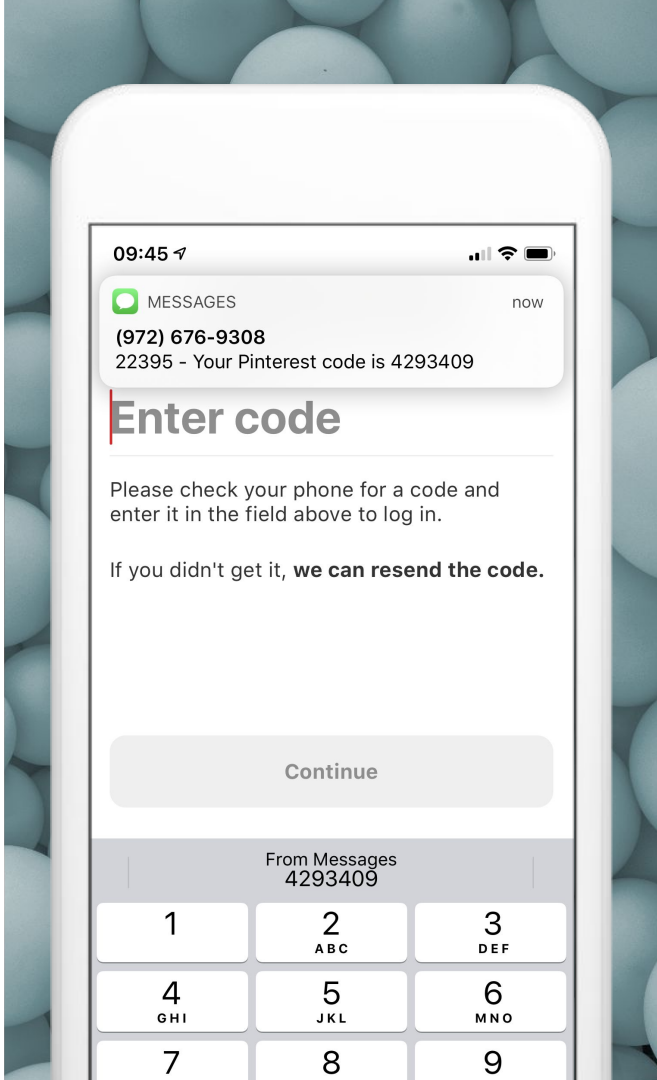
Auth method: a user is granted access after presenting 2+ pieces of evidence

Pros

Protection against ATO, phishing*, …

Cons

Can lock users out (growth, support)



Auth Factors

Something you know

Something you have

Something you are

Auth Factors

First factor

Something you know	Password
Something you have	OAuth Link via Email
Something you are	

Auth Factors

	First factor	Second factor
Something you know	Password	Codes (SMS, TOTP, backup)
Something you have	OAuth Link via Email	Push notifs Security keys
Something you are		

Auth Factors

	First factor	Second factor	Client-only
Something you know	Password	Codes (SMS, TOTP, backup)	
Something you have	OAuth Link via Email	Push notifs Security keys	
Something you are			Fingerprint, Face recogn.

1. Thou shalt have no other gods before me

2. Thou shalt not send biometrics to any server

...

God
Ten Commandments

Agenda

1 Intro

2 **Design**

3 Login

4 Enable

5 Juicy details

How-To Build 2FA

Login *
Enable * (in Settings)

* Owners can be different teams

How-To Build 2FA

	API + Backend(s)
Login *	✓
Enable * (in Settings)	✓

* Owners can be different teams

How-To Build 2FA

	API + Backend(s)	Web	Mobile (x2)
Login *	✓	✓	✓
Enable * (in Settings)	✓	✓	

* Owners can be different teams

How-To Build 2FA

	API + Backend(s)	Web	Mobile (x2)	Design + I18N
Login *	✓	✓	✓	✓
Enable * (in Settings)	✓	✓		✓

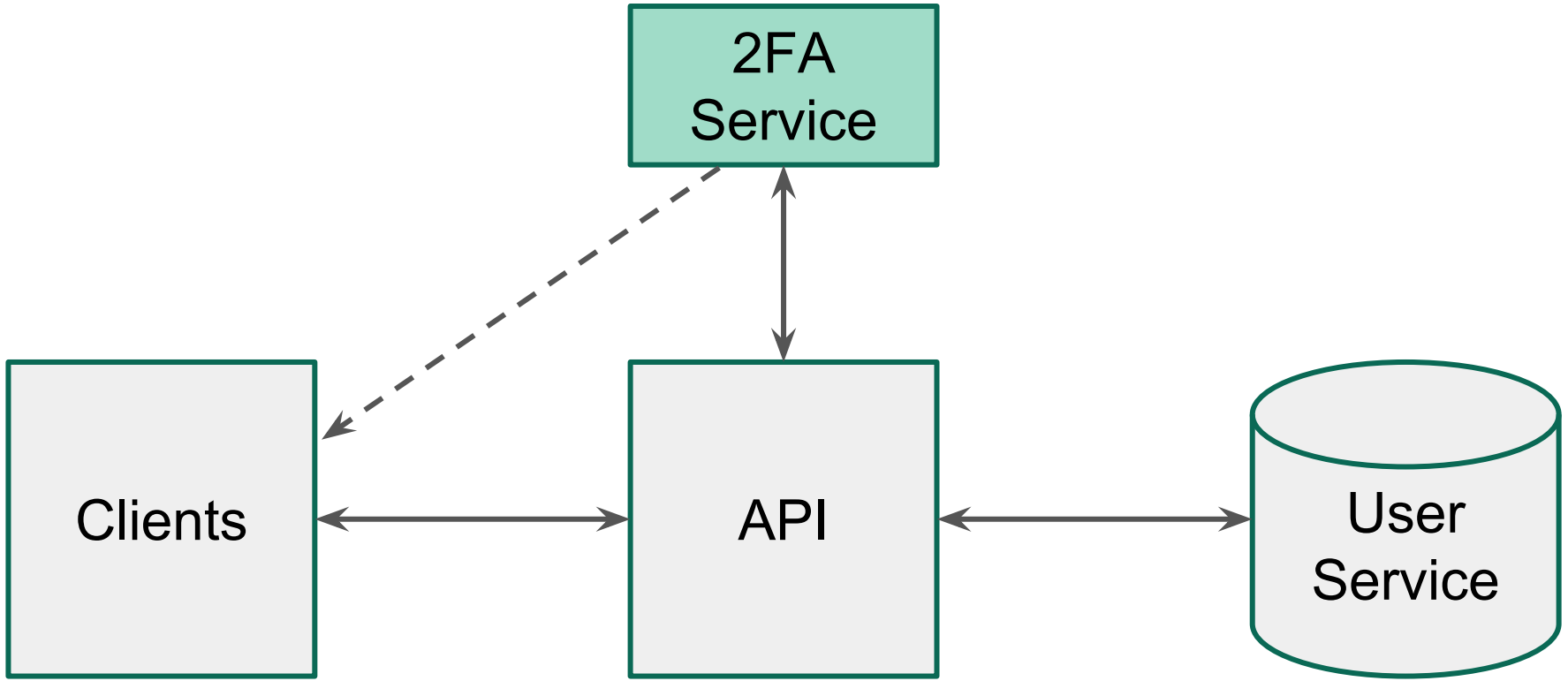
* Owners can be different teams

How-To Build 2FA

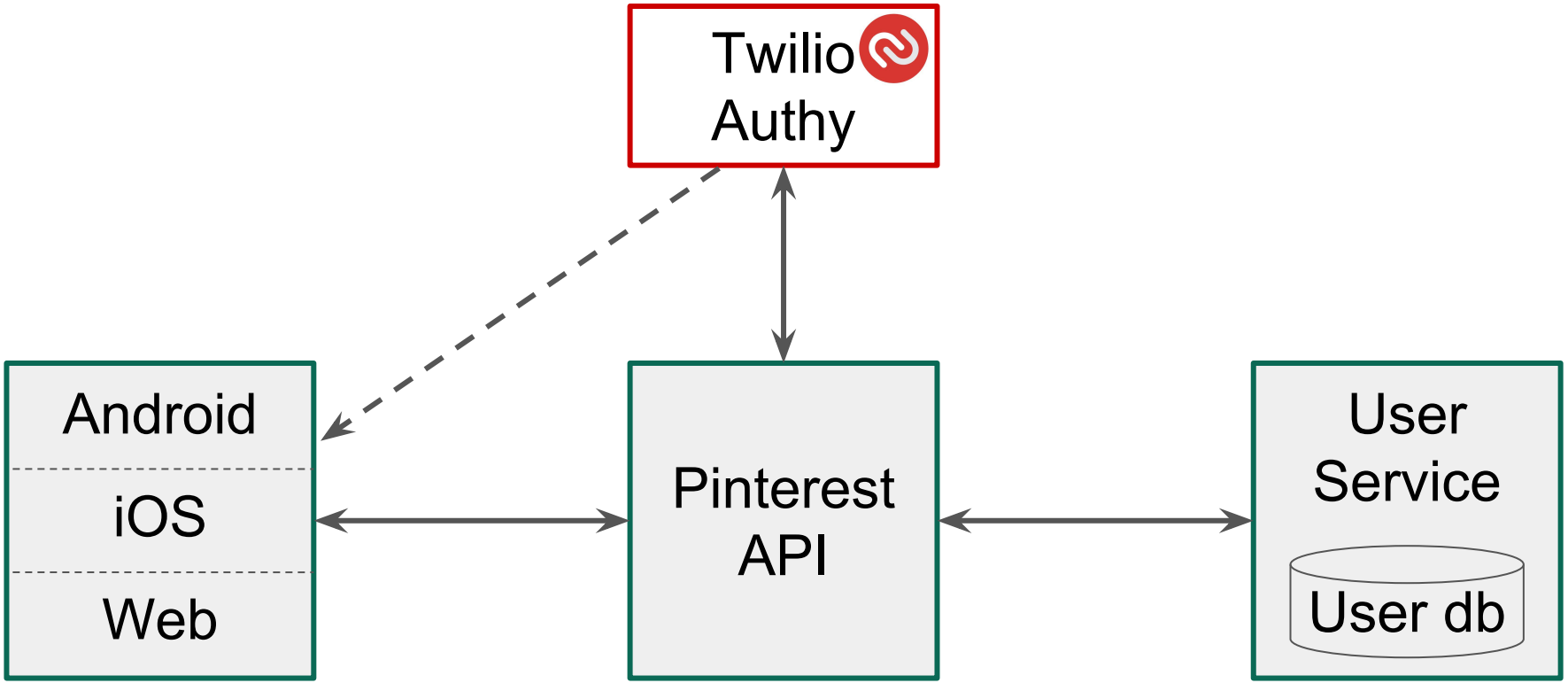
	API + Backend(s)	Web	Mobile (x2)	Design + I18N	Marketing + PR
Login *	✓	✓	✓	✓	✓
Enable * (in Settings)	✓	✓		✓	

* Owners can be different teams

Architecture



Architecture - Pinterest



Agenda

1 Intro

2 Design

3 **Login**

4 Enable

5 Juicy details

Login with 2FA

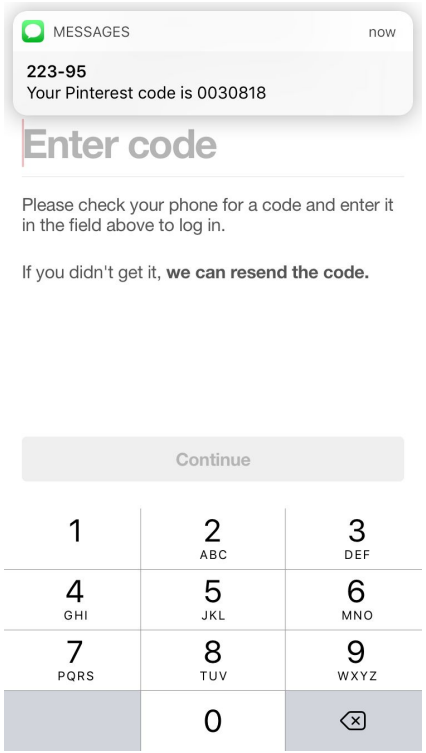
TIP: build login first

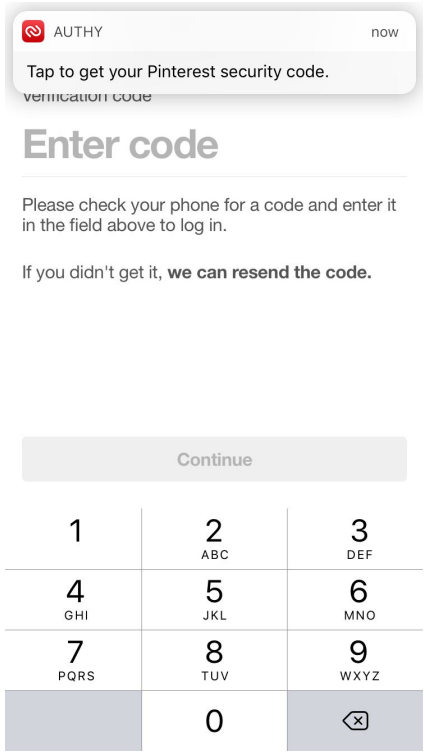
Multiple platforms, slow deployment

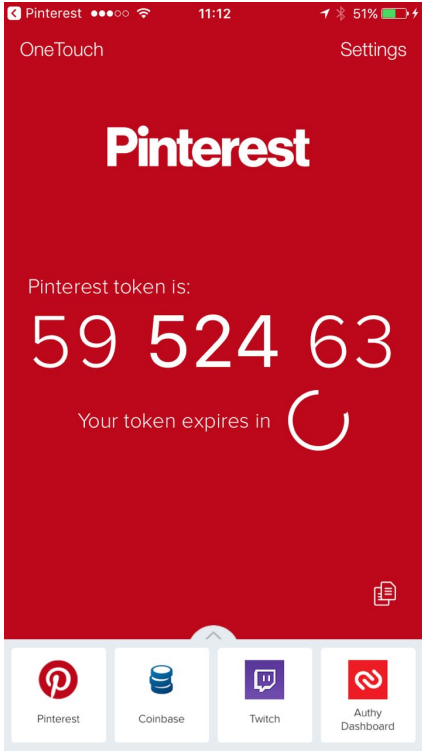
Choice: build codes only

One single login screen

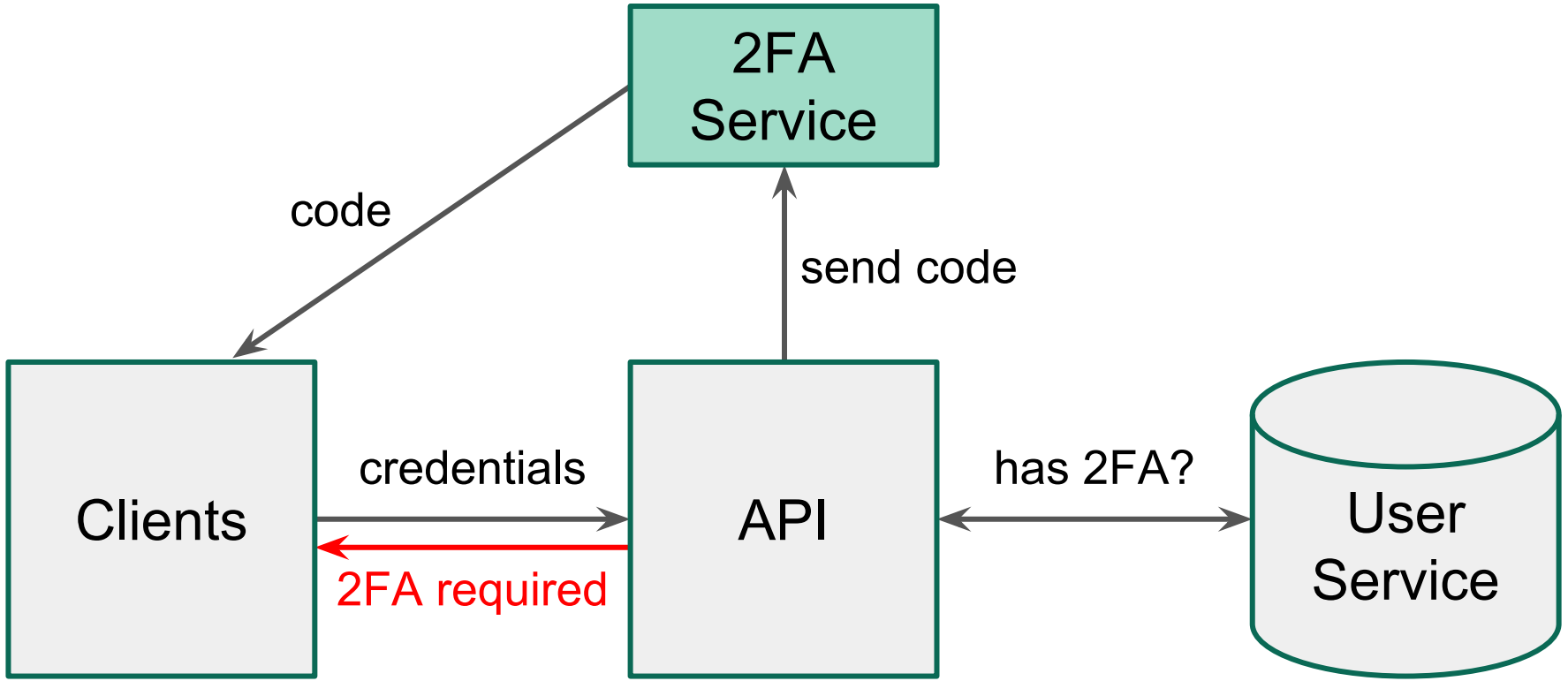
Login with 2FA: Goal



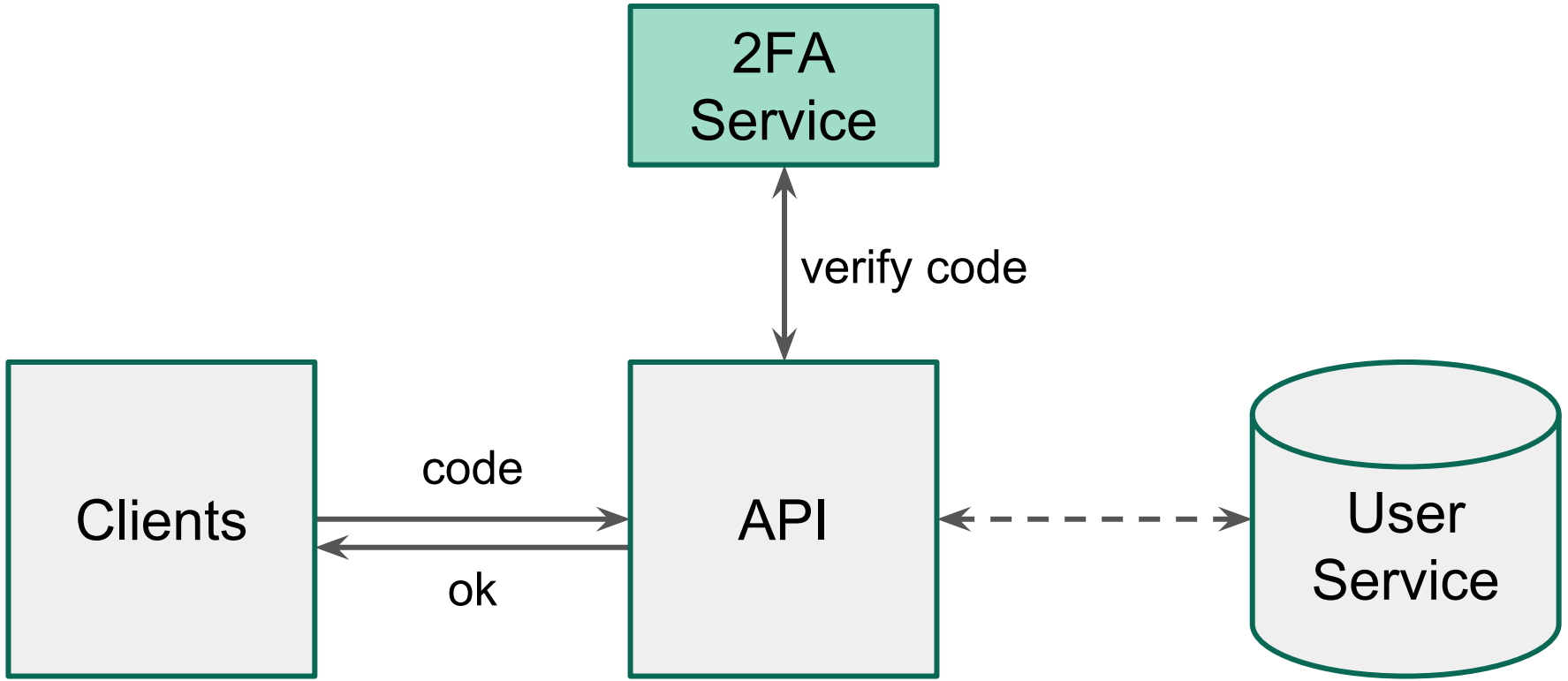




Login: Existing Endpoint



Login: New Endpoint



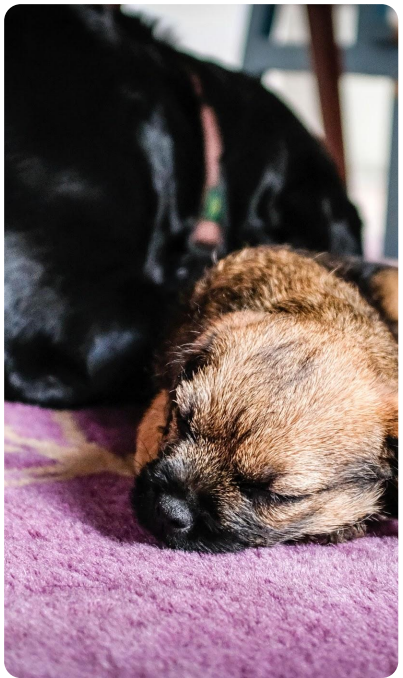
Login: BE vs FE

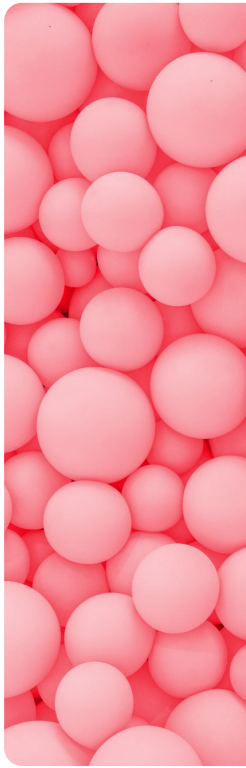
Backend - smooth

- Current login endpoints throw exception (send code)
- New login endpoint verify 2FA challenge

Frontend - expect issues

- Catch exception, show 2FA screen
- Deep in the network stack, can be hard

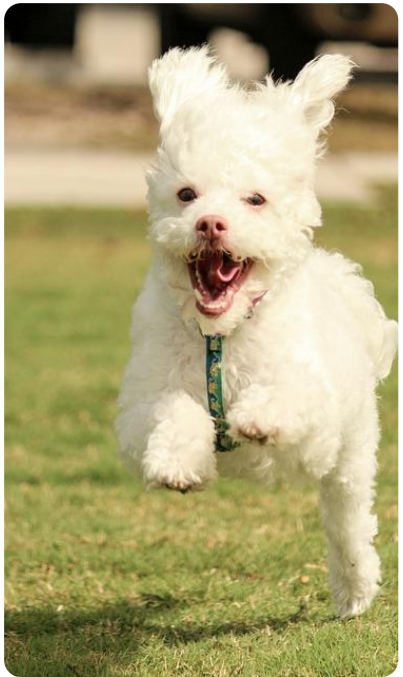




Login with 2FA

Rollout

- Gate new code before release!
- Deploy to employees
- Check for unexpected regressions



Agenda

1 Intro

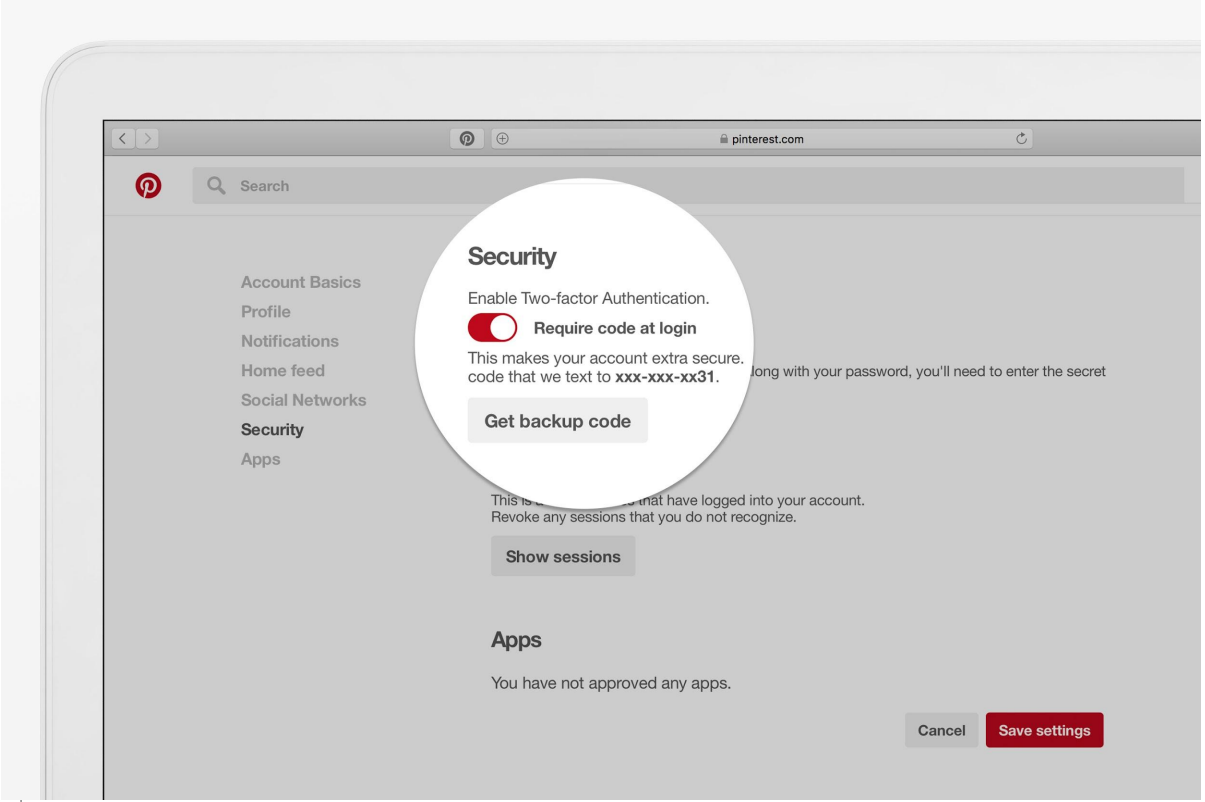
2 Design

3 Login

4 **Enable**

5 Juicy details

Enable 2FA: Goal



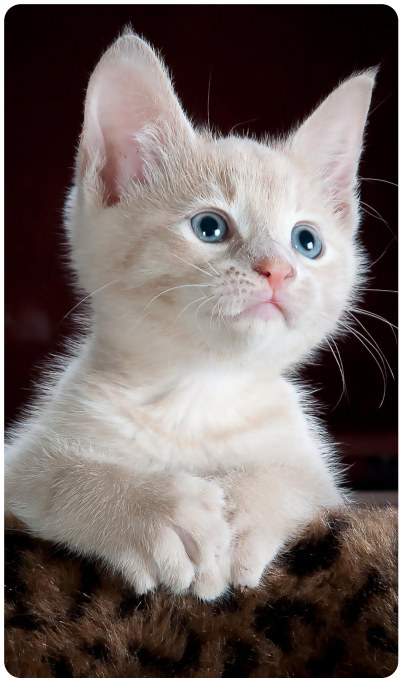
Enable 2FA

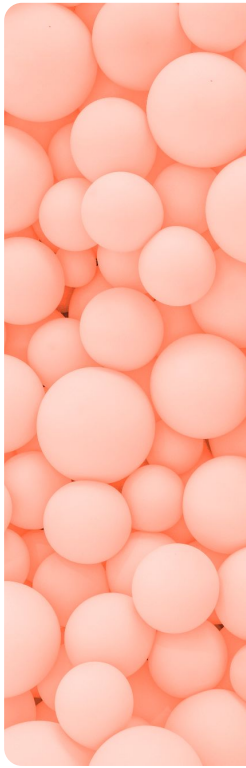
TIP: don't waste time on details

E.g., phone number formatting, country codes...

Choice: build web only

Control rollout from a single platform





Enable: Flows

Enable

- Verify password!
- Input + verify phone
- Fallback! (generated backup codes)

Disable

- Verify password! (usually not 2FA)
- No override, slow process to force disable

Enable 2FA

Nits

- Send security emails
- Unique vs multiple phone numbers?

Rollout

- Test internationally
- Rollout slowly even with big launch

Agenda

1 Intro

2 Design

3 Login

4 Enable

5 **Juicy details**

Other Flows

2FA is a contract with the user

I'll never let you get ATOed again

2FA every new access token

- $ git grep generate_access_token
- password reset, …

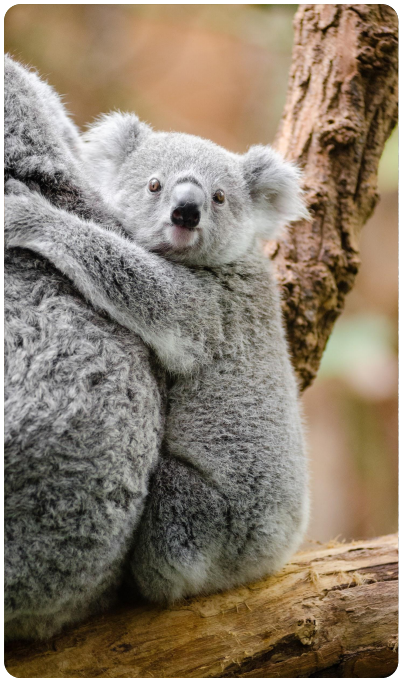
Social Logins

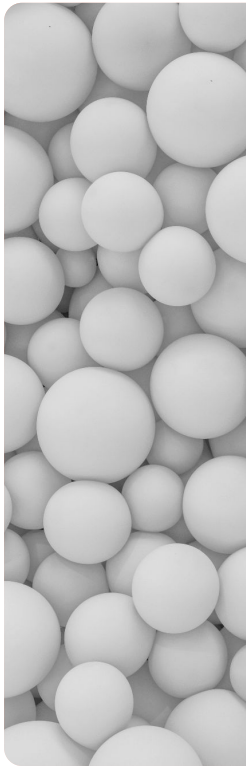
2FA should protect OAuth logins

UX: user enables, then tests… what if she logs in and doesn't see 2FA?

Nice: know if user has 2FA on Social

Google/Facebook if you read this… <3





Security Keys

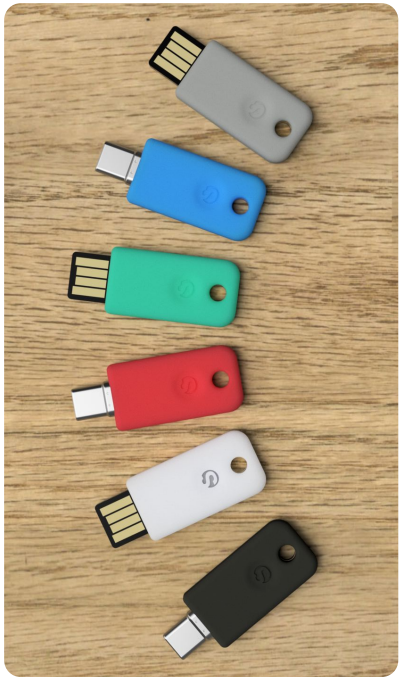
FIDO2 protects against phishing!

Open source security keys exist :)

Pros: WebAuthn

Cons: mobile and especially iOS

Apple, if you read this… <3



Security Keys (2)

Login

- New screen to "change 2FA method"
- Mobile? (skip…)

Enable

- Support multiple security keys per user
- Force a fallback method

Future Bugs

Login

- Login changes, 2FA may be forgotten
- Easy: enforce 2FA blocks
- Hard: make sure 2FA screen is shown

Enable

- n/a

Marketing & PR

Market Internally

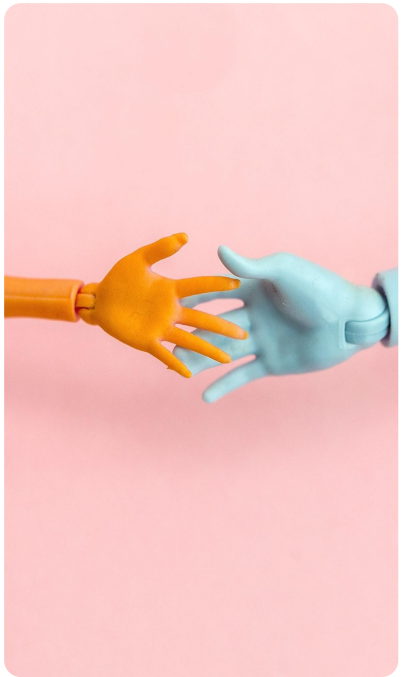
- Showcase
- Employees should enable 2FA

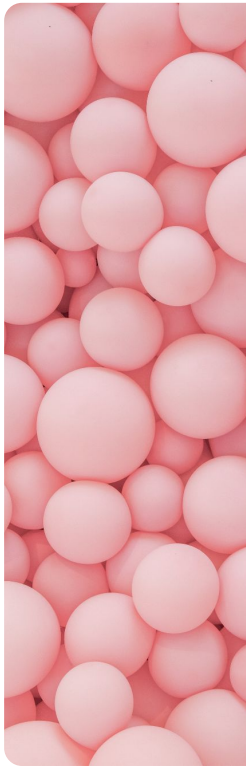
Market Externally

- Tech blog post
- Company blog (internationalized?)
- PR (combine with other security features?)

Thanks

Amanda, Amine, Authy, Chris, Devin, Eric, Evelyn, Flavius, Francesca, Garret, Grey, Hania, Harry, Helen, Henry, Indy, Jamie, Jason, Jean, Jeff, Jerry, Joey, Jon, Juan, Julia, Karan, Kassandra, Kathy, Kelsey, Ken, Kevin, Lang, Madeline, Maggie, Mara, Matt, Megan, Michelle, Nelson, Nestor, Nicole, Purajit, Qi, Rodrigo, Ryan, Sarah, Shira, Tom, Vamsi, Vincent, Vivian, William, Xin, Yuan, Zack





Conclusion

1. Intro
2. Design
3. Login
4. Enable
5. Juicy details

2FA is great,
= big project
= headaches
= smooth
Go build it!

Thank You!

Emanuele Cesena
ema@pinterest.com
@0x0ece

Thank You!

https://solokeys.com
Get 15% off: BSIDES15

Emanuele Cesena
ema@pinterest.com
@0x0ece