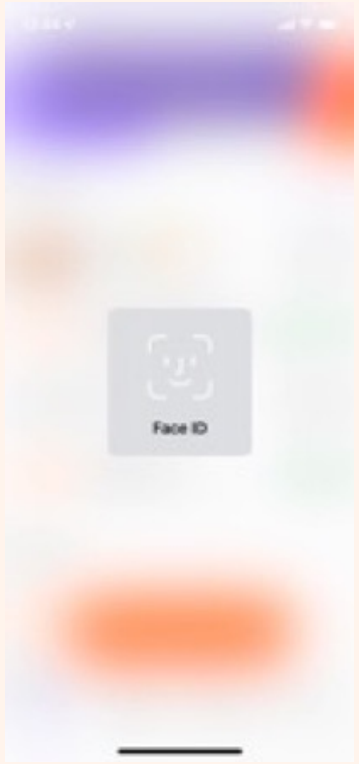
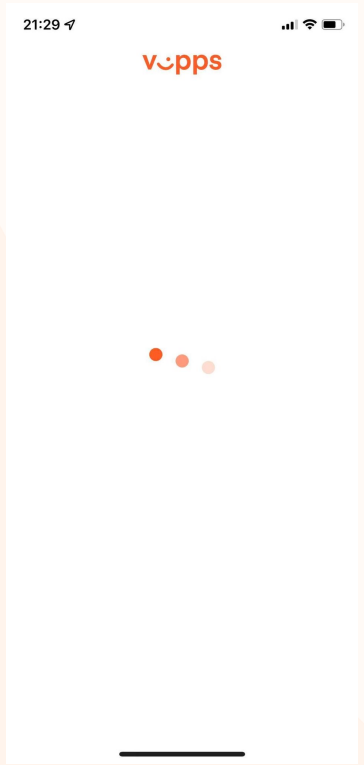
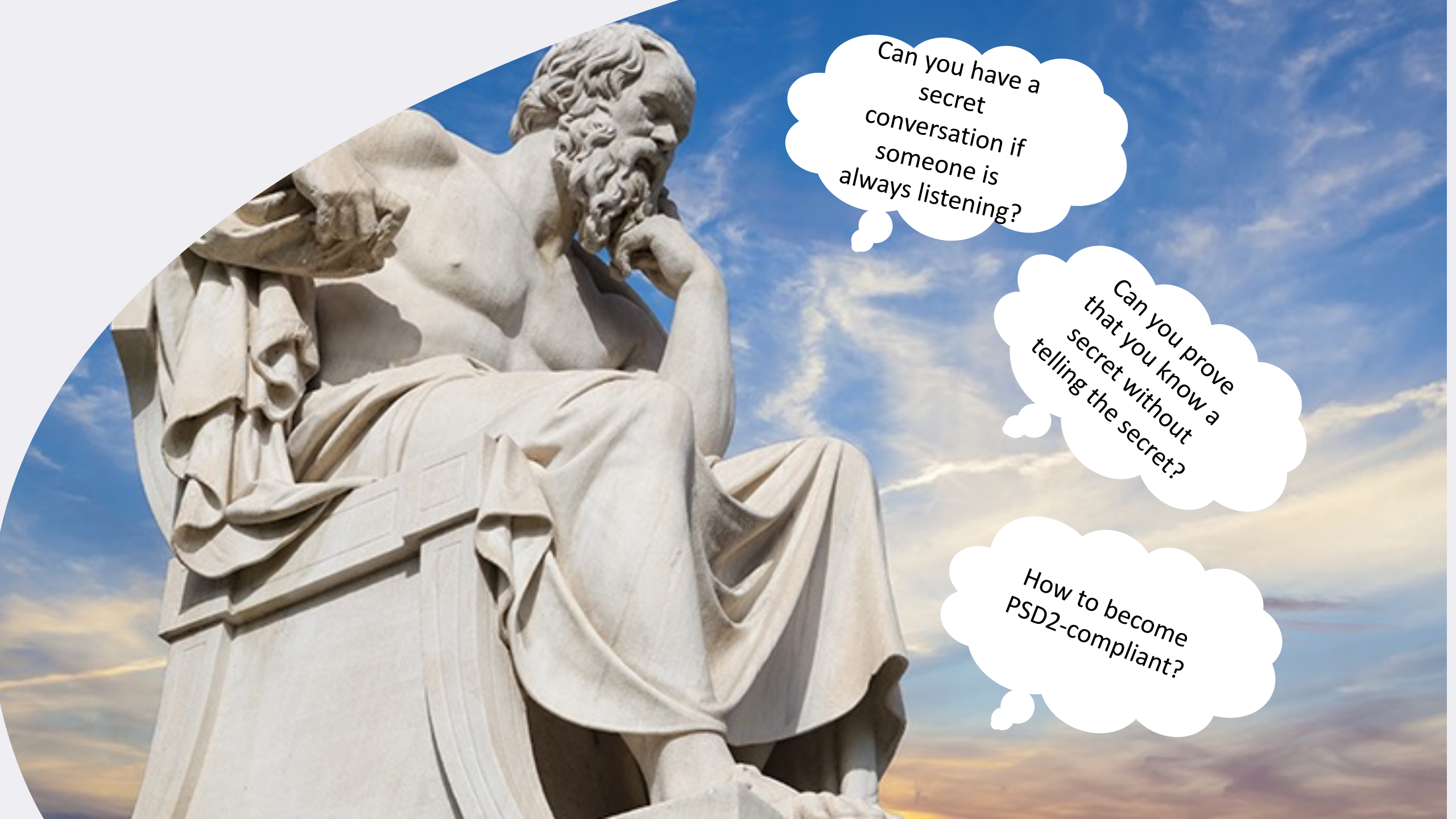
Security at high speeds

- How Vipps secures their APIs


How do I add “pay with Vipps on my website”?
I am not able to remove someone from a settlement
Isn’t the Vipps ap already finished?


Face ID


21:29
vipps


Can you have a secret conversation if someone is always listening?
Can you prove that you know a secret without telling the secret?
How to become PSD2-compliant?

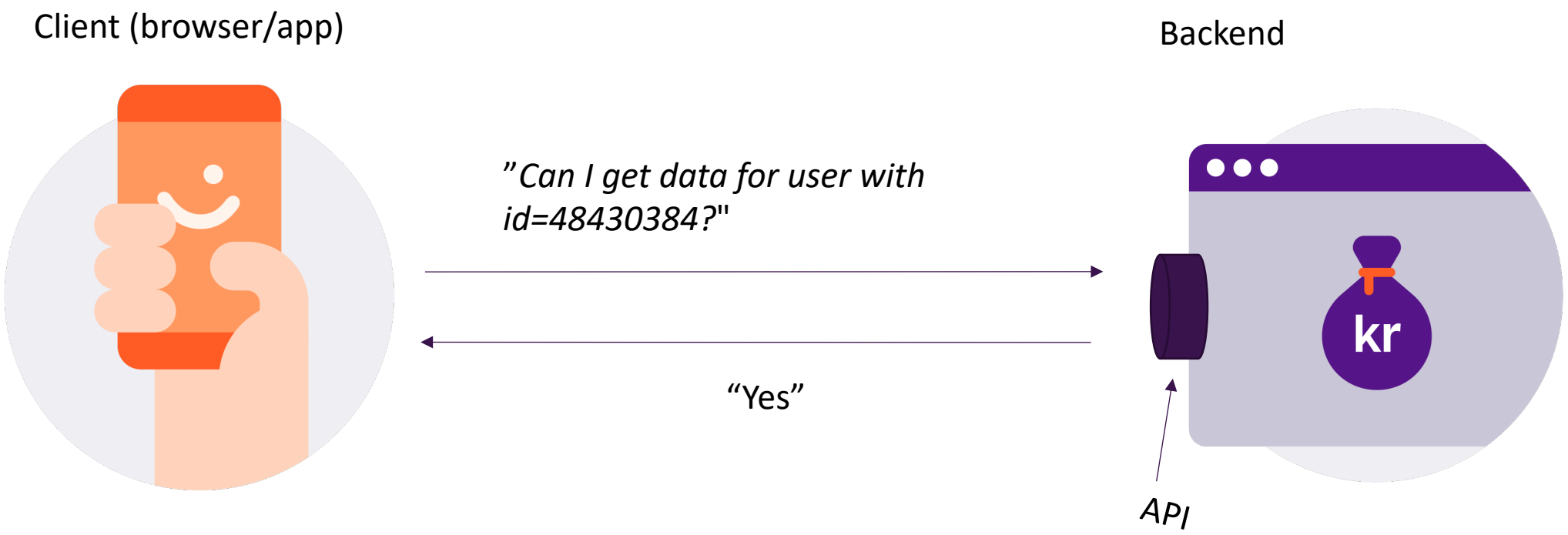
Vinx

- Login-system to the Vipps app
- 1,2 billion authentications per year
- Users have to go through Vinx to do anything
  - System needs to be quick!

Protector of all Vipps APIs

V + Sphinx = Vinx

No authentication



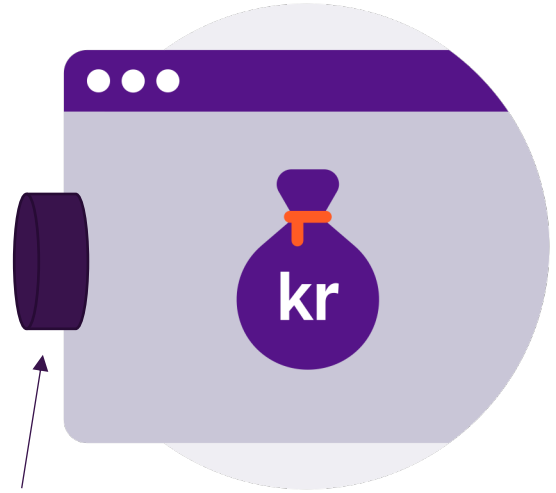
Username and password

Client (browser/app)

”Can I get data fro a user with id=48430384?
Username = admin, password = 123456"

”Only with the correct username and password”

Backend



API

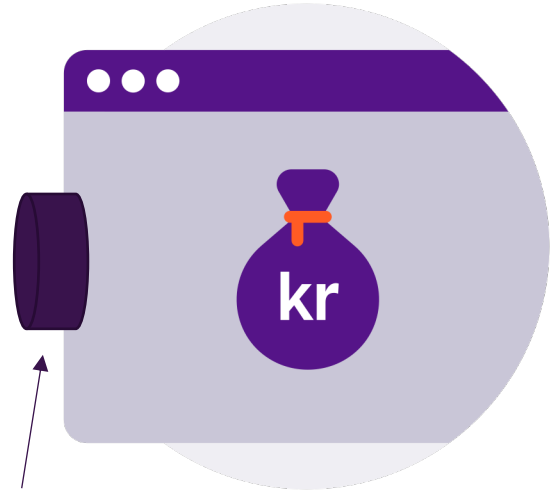
API-key

Client (browser/app)

”Can I get data for a user with id=48430384?
***API-key* = aGVpaGVpam...**"

”As long as you have the correct API-key!”

Backend



API

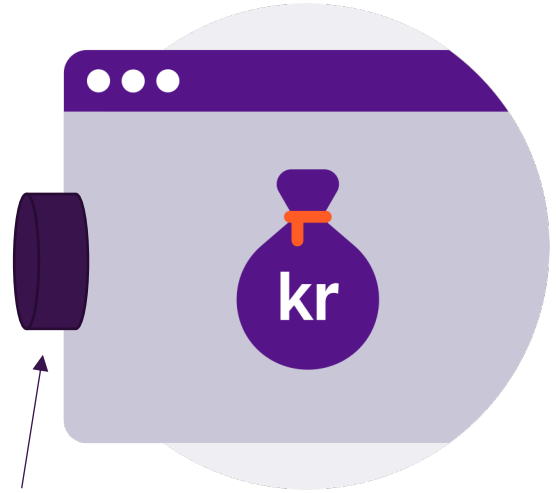
Access Token

Klient (nettleser/app)

”Can I get a data fro a user with id=48430384?
Authorization Bearer djf4r9fuhf..."

”As long as you have an Authorization-token!"

Backend



API

Access Tokens

Encoded token

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JpZCI6IjEyMzQ1Njc4OTAiLCJuYW1lIjoiTm9yY
SIsImlhdCI6MTUxNjIzOTAyMn0.hunZAgTOj5lh
BzmyiGwkXm2z7RJ-viqUsBZ7Xjsojm0
```

Decoded token

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

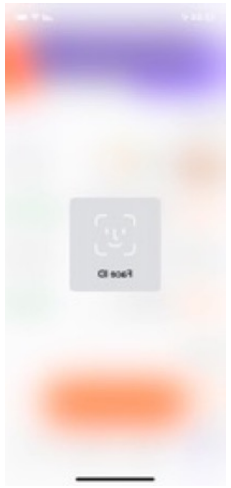
PAYLOAD: DATA

```
{
  "id": "1234567890",
  "navn": "Per Dhal",
  "exp": "10min"
}
```

10hours

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

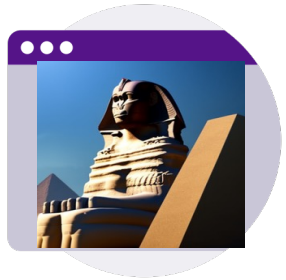


App

1. User proves identity
(? Mystery algorithm ?)

2. App gets Vinx-token
(signed by Vinx)

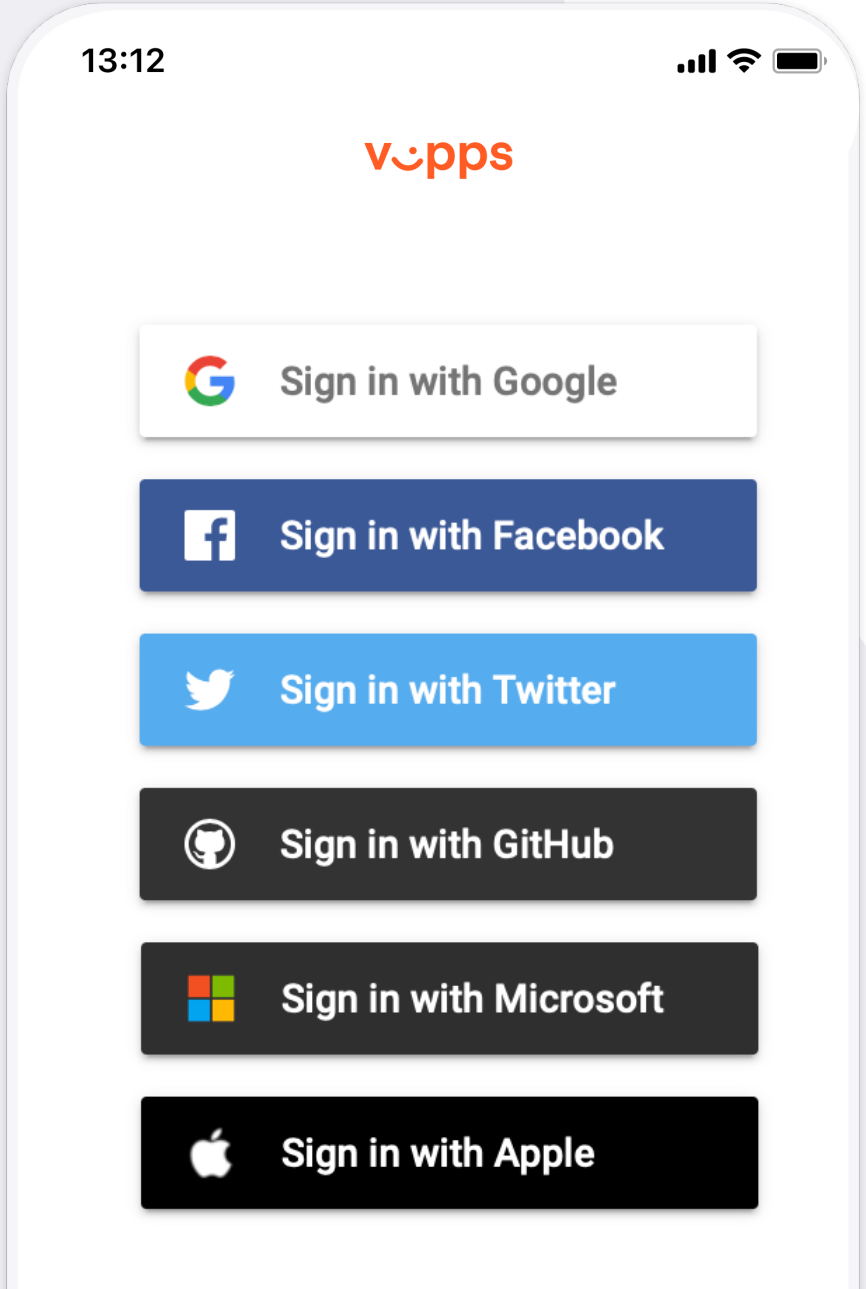
3. *Uses Vinx-token to get access to other Vipps APIs*



Vinx

Checks that token is from Vinx

Vipps Payment API


13:12
vopps
Sign in with Google
Sign in with Facebook
Sign in with Twitter
Sign in with GitHub
Sign in with Microsoft
Sign in with Apple

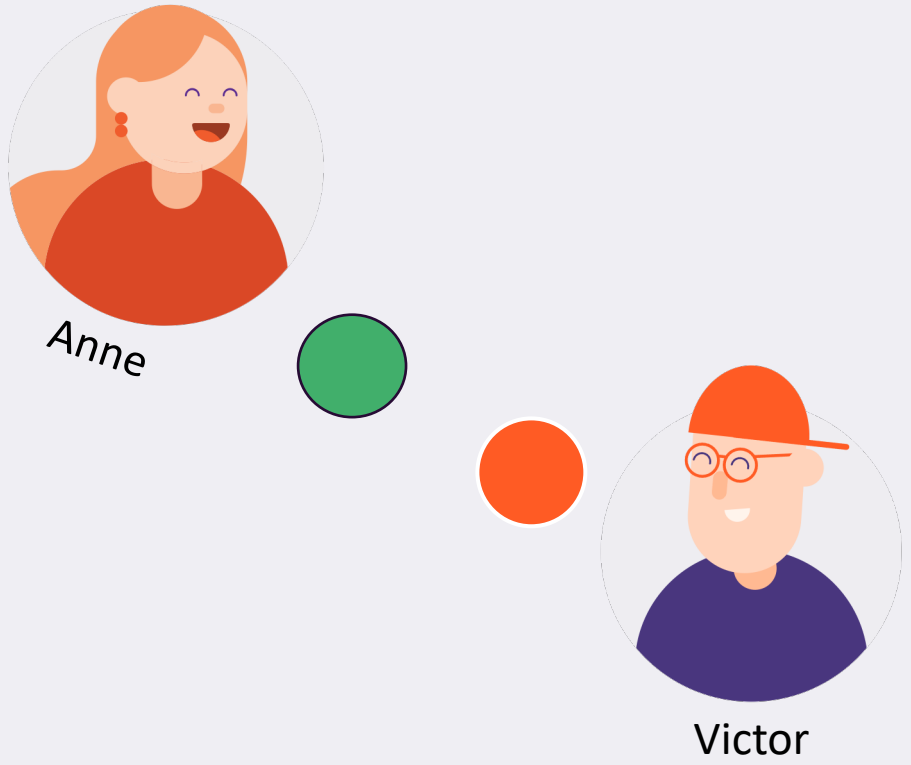
https://www.flickr.com/photos/tiseb/4592786358/

Strong customer authentication

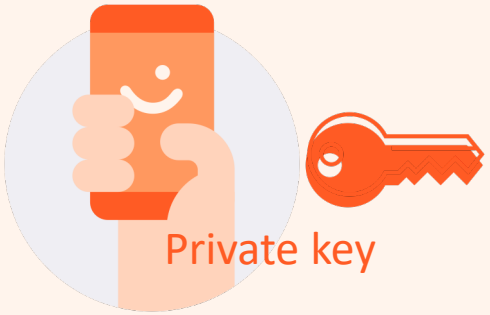
Dynamic linking

SRP Algorithm

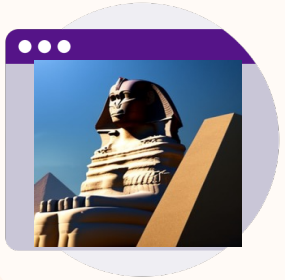
- Zero knowledge proof algorithm
  - Prove that something is true without revealing any reason why
- https://www.youtube.com/watch?v=fOGdb1CTu5c
- https://github.com/secure-remote-password/srp.net



Register new device

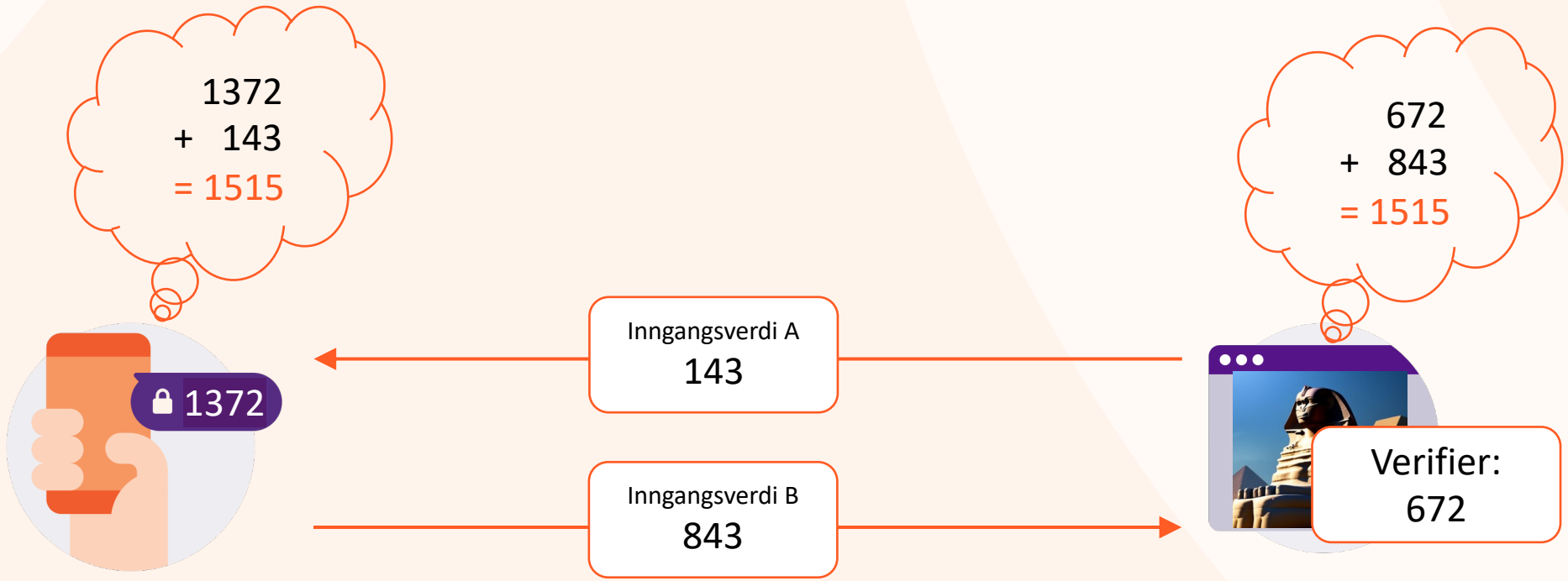


Public key

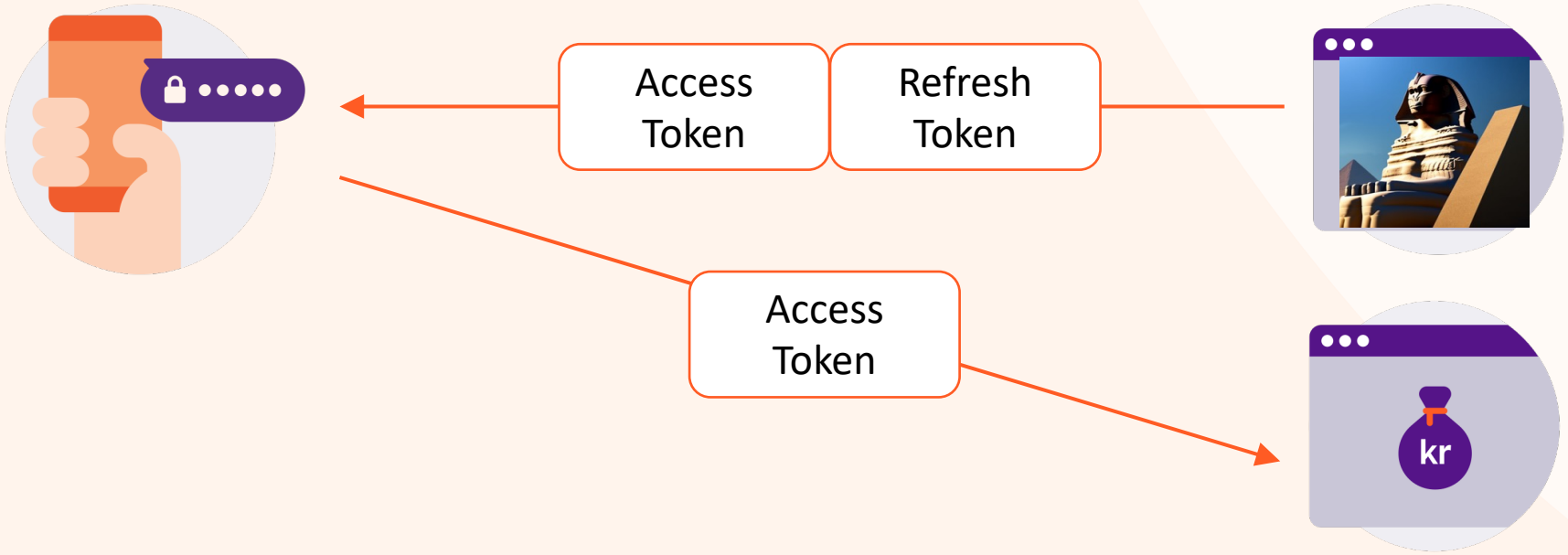


Login

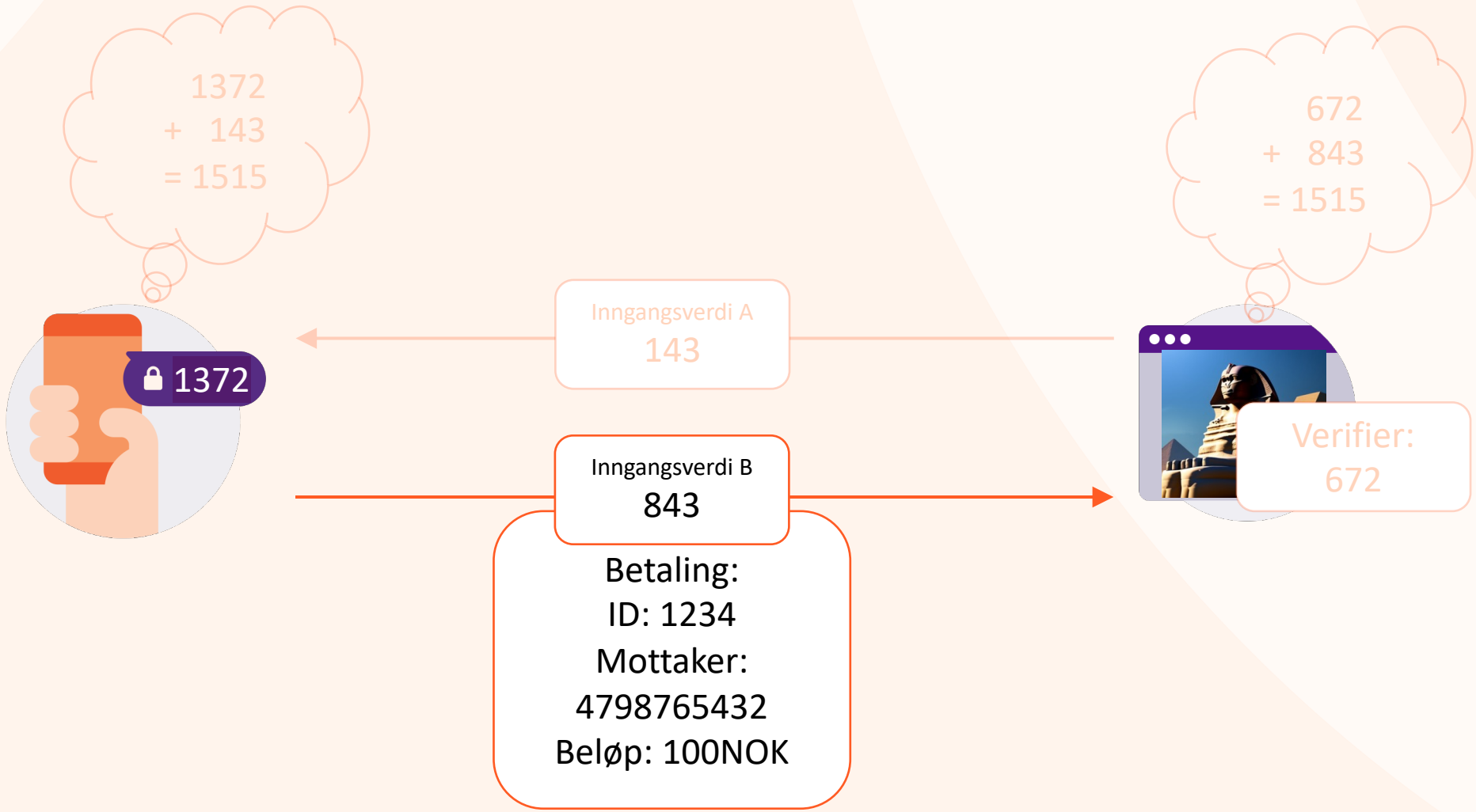
Login


1372
+ 143
= 1515
1372
Inngangsverdi A
143
Inngangsverdi B
843
672
+ 843
= 1515
Verifier:
672

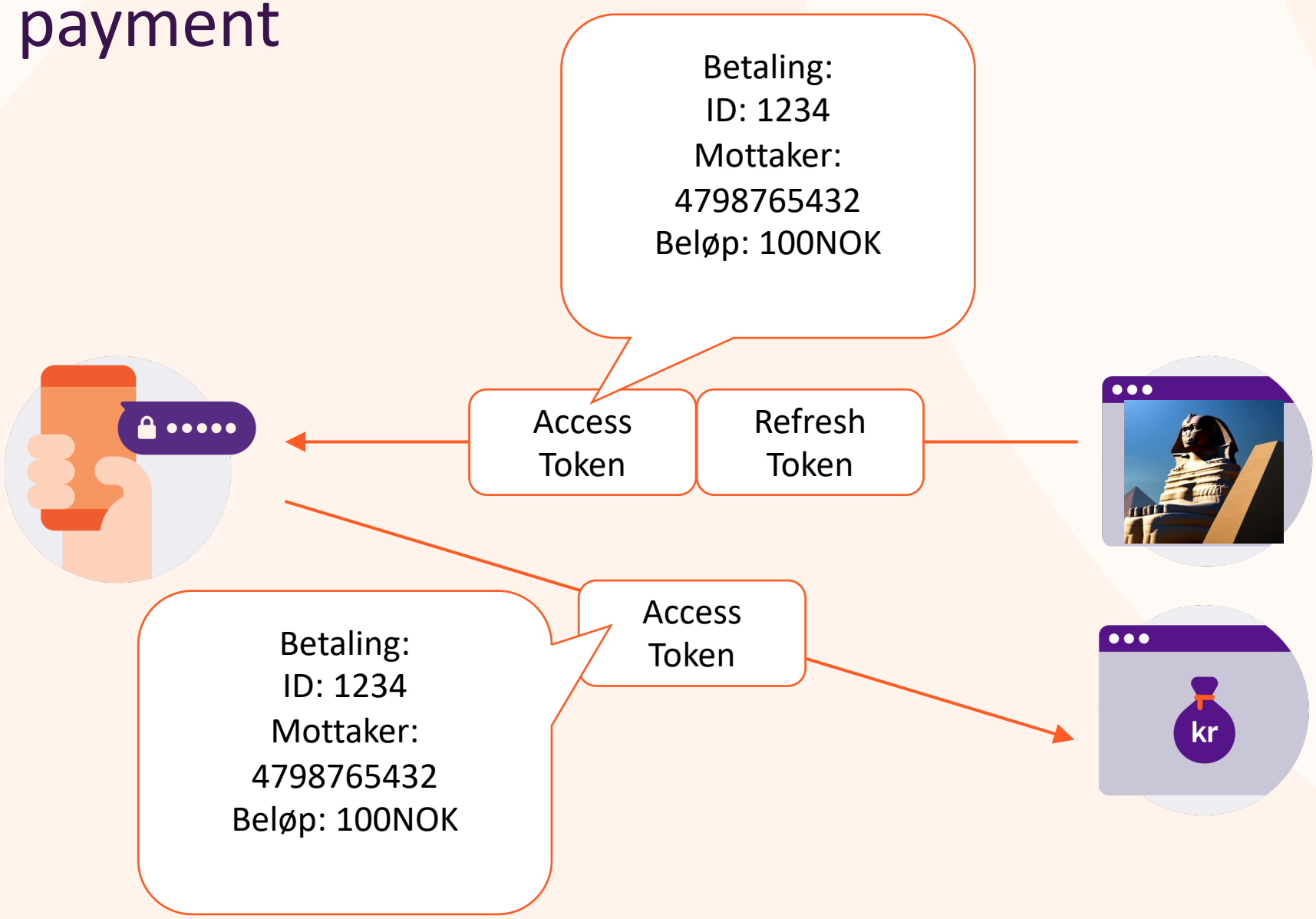
Tokens



Payment


1372
+ 143
= 1515
1372
Inngangsverdi A
143
Inngangsverdi B
843
Betaling:
ID: 1234
Mottaker:
4798765432
Beløp: 100NOK
672
+ 843
= 1515
Verifier:
672

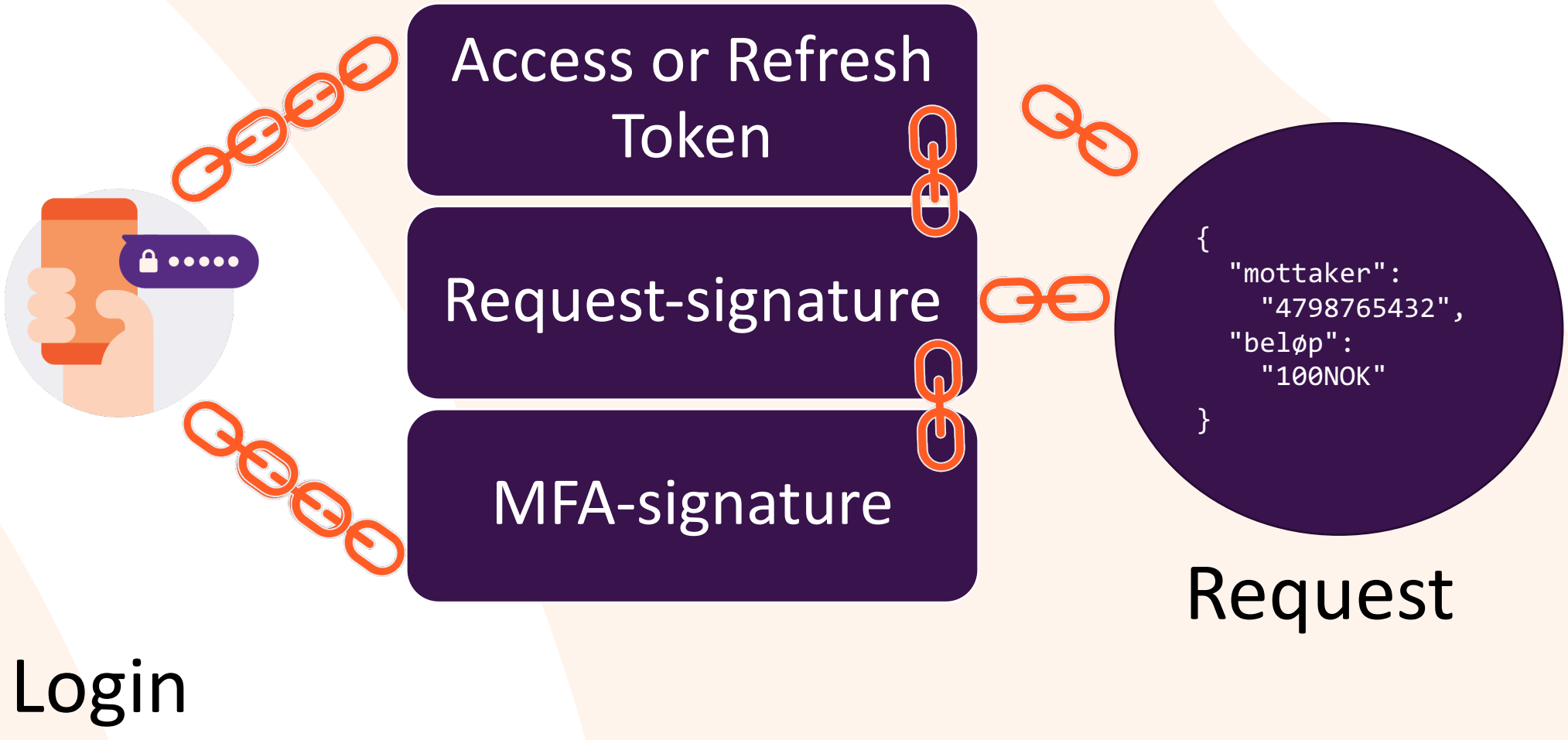
Confirm payment



Security mechanisms in Vinx

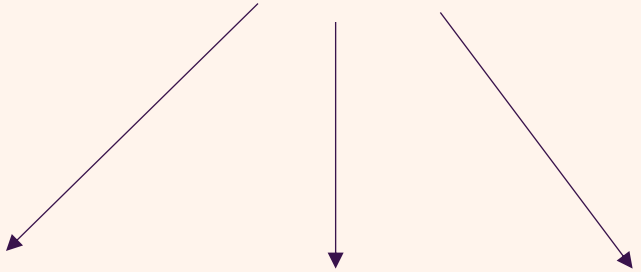
```
POST /payments/5ffc30e9-11e9-43ea-a526-0d3f4b4b26fd HTTP/1.1
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJkZXZpY2UxMjM0IiwiaWF0IjoxN
  TE2MjM5MDIyfQ.y877NTLNZvpXRsAOXAYomfreE1vkFmILbP7163TtHmE
Request-Signature: eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJkZXZpY2UxMjM0IiwiZGlnZXN0Ijoi
  MDI0N2FhZWMwMjljOWU1NGMzNjI0OTg0ZjFiZWQ2ZDQiLCJpYXQiOjE1MTYyMzkwMjJ9.b2T2ZBEkB
  wp_YP2O5DjsQc62JpxWUrabgsfZD4n30ZU
MFA-Signature: eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJkZXZpY2UxMjM0IiwidG9rZW4tZGlnZXN0
  IjoiZWEwNjhhMTExMTYwY2I0ZDFhODVjMDg3MjFjMTIzODciLCJpYXQiOjE1MTYyMzkwMjJ9.MJp2N
  FMDbbxPk4cXCl5jzE_SQfO4QVRe84lvKahI92Y



{
  "recipient": "4798765432",
  "amount": "100",
  "currency": "NOK"
}
```

Security Mechanisms

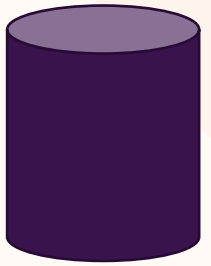


Security and speed

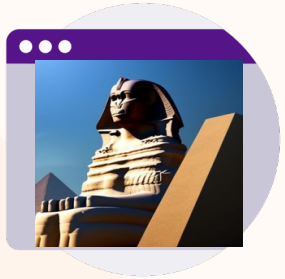
Always listening



No PIN codes in database



Never sends PIN-code



Summary

- Vinx-token
  - User proves identity, gets JWT
- SRP algorithm
  - Device-specific PIN
  - PIN not saved in database
- Payment information in token
  - Cross-referenced by payment backend
  - Proves user saw amount and recipient
- Access token + Request-signature + MFA-signature

Protector of all Vipps APIs

V + Sphinx = Vinx

Things I did not get to cover

- Use of refresh tokens
- Device integrity
- Service-to-service authentication
- Infrastructure security
- Optimization of speed
  - Read/write to database
  - Events

Protector of all Vipps APIs

V + Sphinx = Vinx

Thank you!

Nora Tomas

vopps