



HYBRID IAM

Interoperable VCs for Workforce Identity



DR. MATTIA ZAGO

Solutions Architect

mattia.zago@monokee.com



MATTEO MIDENA

Self-Sovereign Identity Specialist

matteo.midena@monokee.com

HYBRID IAM

Interoperable VCs for Workforce Identity

HYBRID IAM

Interoperable VCs for Workforce Identity

- Central Authority
- Central Control
- Implicit Trust
- Persistent

HYBRID IAM

Interoperable VCs for Workforce Identity

Decentralized
No standard tech
Explicit trust
User-owned

Central Authority
Central Control
Implicit Trust
Persistent

HYBRID IAM

Interoperable VCs for Workforce Identity

Tech-independent?
User-chosen?
Cross-compatible?
Easy integration?

Decentralized
No standard tech
Explicit trust
User-owned

Central Authority
Central Control
Implicit Trust
Persistent

Central Authority
Central Control
Cross-compatible

Easy integration
Explicit Trust
Enterprise-managed but user-owned

HYBRID IAM

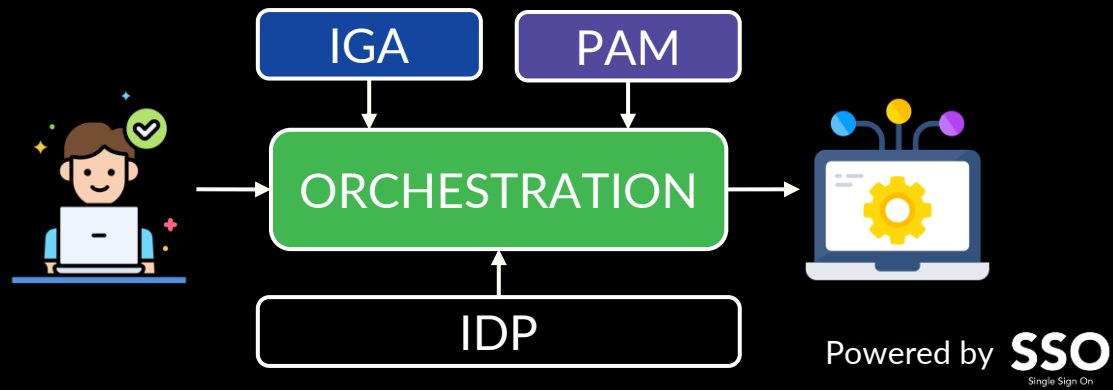
Interoperable VCs for Workforce Identity

Tech-independent?
User-chosen?
Cross-compatible?
Easy integration?

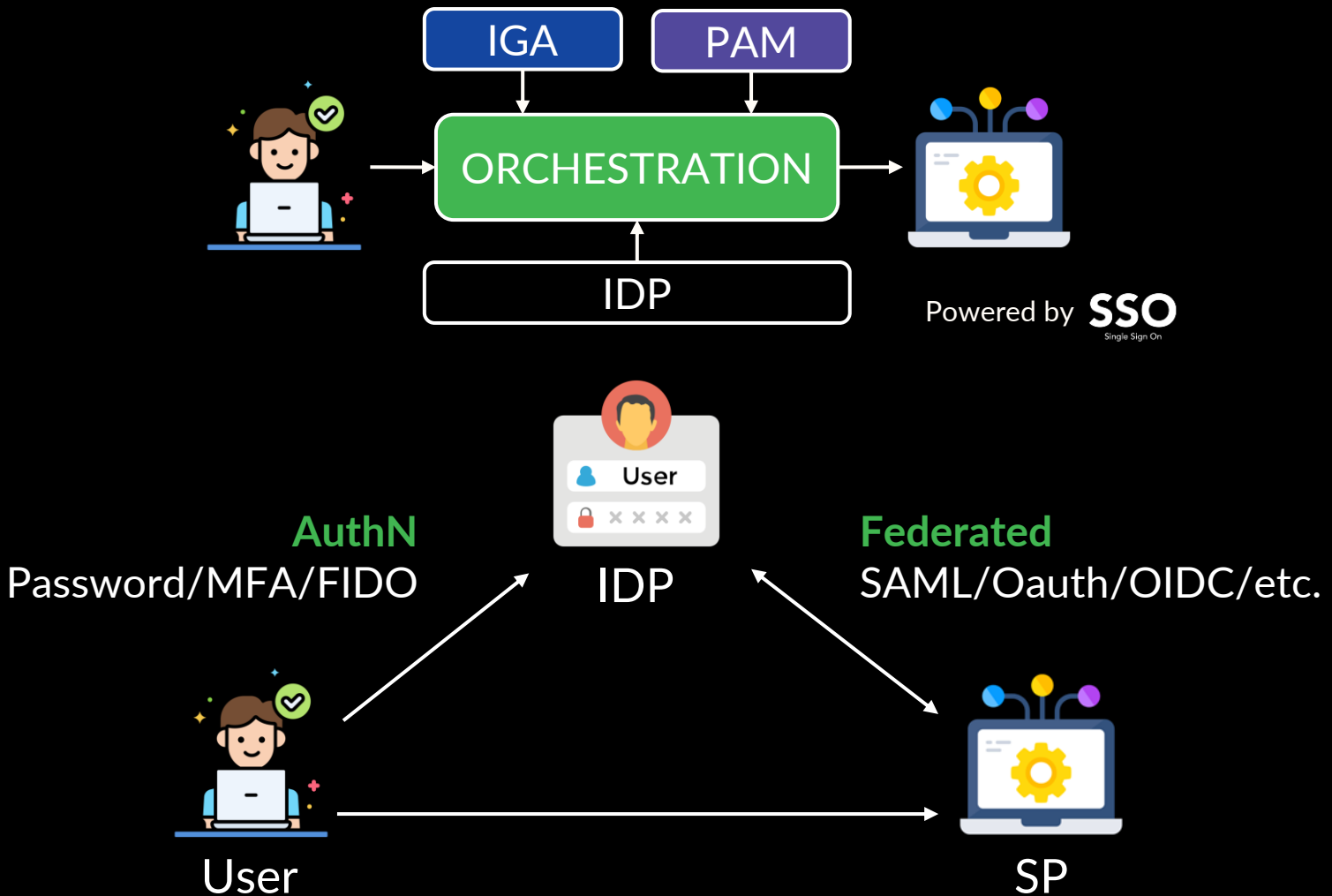
Decentralized
No standard tech
Explicit trust
User-owned

Central Authority
Central Control
Implicit Trust
Persistent

HYBRID IAM



HYBRID IAM



What about **Web 3.0**? What about **SSI**?

On paper, they are wonderful

What about **Web 3.0**? What about **SSI**?

On paper, they are wonderful



Security

Fewer Company Hacks

What about **Web 3.0**? What about **SSI**?

On paper, they are wonderful



Security

Fewer Company Hacks



Data Sovereignty

User is IDP itself

What about **Web 3.0**? What about **SSI**?

On paper, they are wonderful



Security

Fewer Company Hacks



Data Sovereignty

User is IDP itself



Interoperability

Open Standards

What about **Web 3.0**? What about **SSI**?

On paper, they are wonderful



Security

Fewer Company Hacks



Data Sovereignty

User is IDP itself



Interoperability

Open Standards



Transparency

Public blockchain and accountability

What about **Web 3.0**? What about **SSI**?

On paper, they are wonderful



Security

Fewer Company Hacks



Data Sovereignty

User is IDP itself



Interoperability

Open Standards



Transparency

Public blockchain and accountability



Compliant with SSI philosophy

Data ownership

What about **Web 3.0**? What about **SSI**?

On paper, they are wonderful



Security

Fewer Company Hacks



Data Sovereignty

User is IDP itself



Interoperability

Open Standards



Transparency

Public blockchain and accountability



Compliant with SSI philosophy

Data ownership

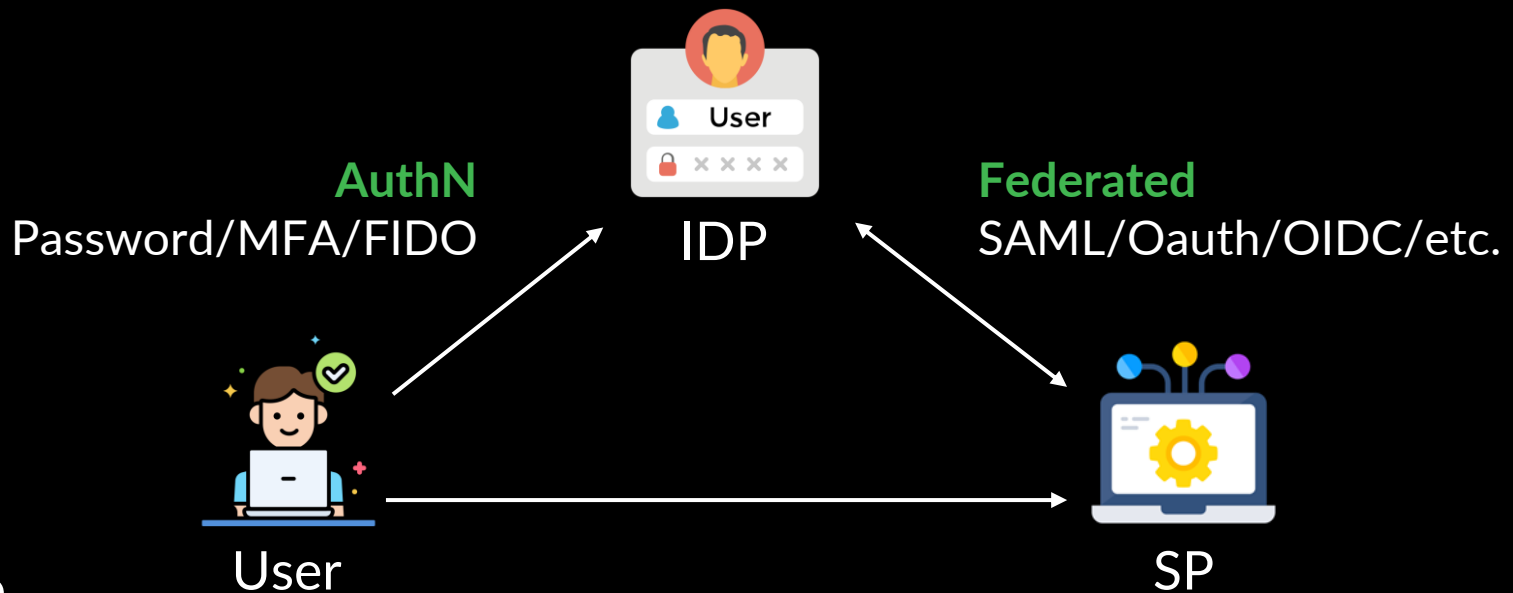


Truly Decentralized

No more central authority

HYBRID IAM

Where would **VCs/VPs** fit?

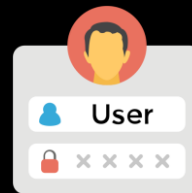


HYBRID IAM

Where would VCs/VPs fit?

✗ M2M SSO Protocol

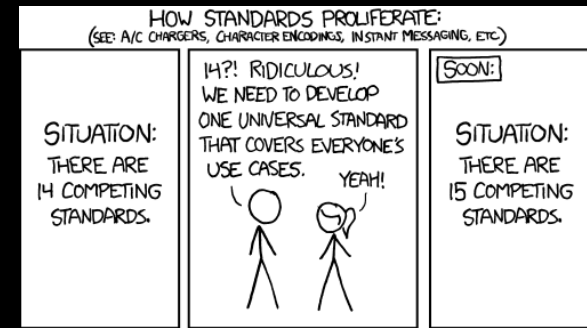
AuthN
Password/MFA/FIDO



IDP



User



Federated
SAML/Oauth/OIDC/etc.



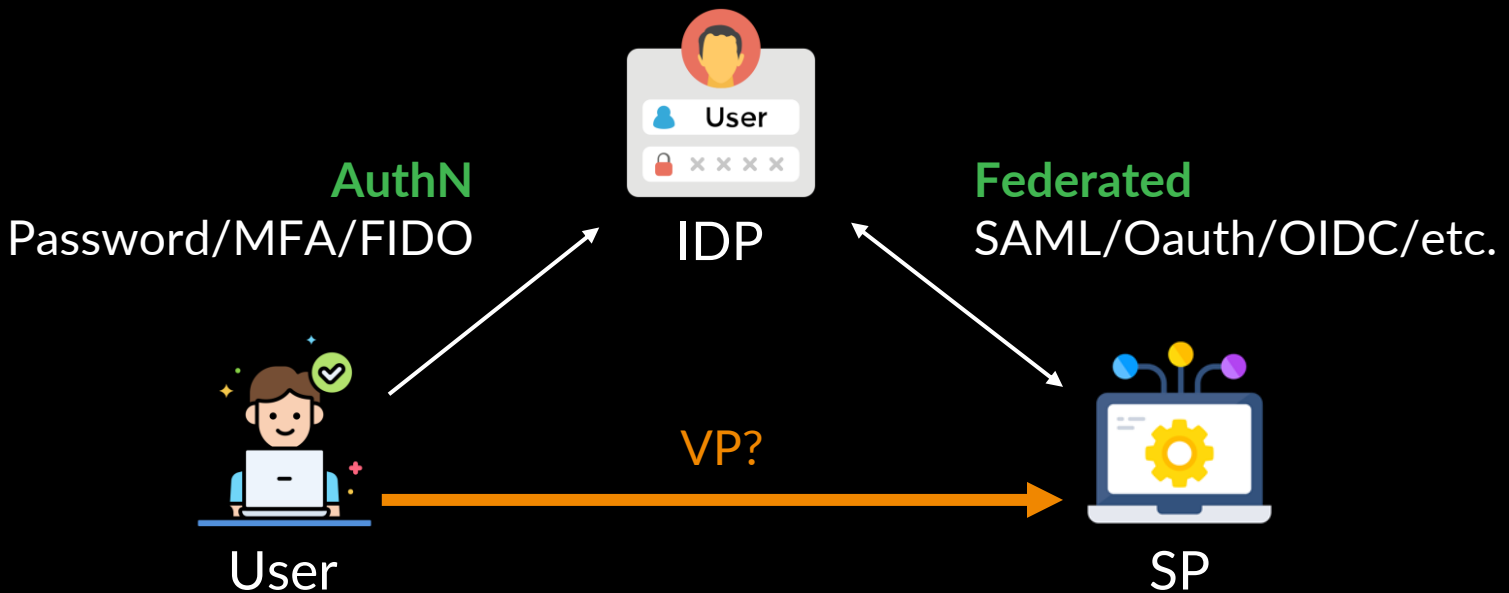
SP



HYBRID IAM

Where would **VCs/VPs** fit?

- ✗ M2M SSO Protocol
 - User → SP



WHY **NOT** WEB 3.0 SOLUTIONS? ❌



More conscious users

True data ownership
implies awareness

WHY **NOT** WEB 3.0 SOLUTIONS? ❌



More conscious users

True data ownership
implies awareness



Users left alone

True self custody implies
no recovery options

WHY **NOT** WEB 3.0 SOLUTIONS? ❌



More conscious users

True data ownership
implies awareness



No central authority

No one makes decisions
or resolves disputes



Users left alone

True self custody implies
no recovery options

WHY **NOT** WEB 3.0 SOLUTIONS? ❌



More conscious users

True data ownership
implies awareness



No central authority

No one makes decisions
or resolves disputes



Users left alone

True self custody implies
no recovery options



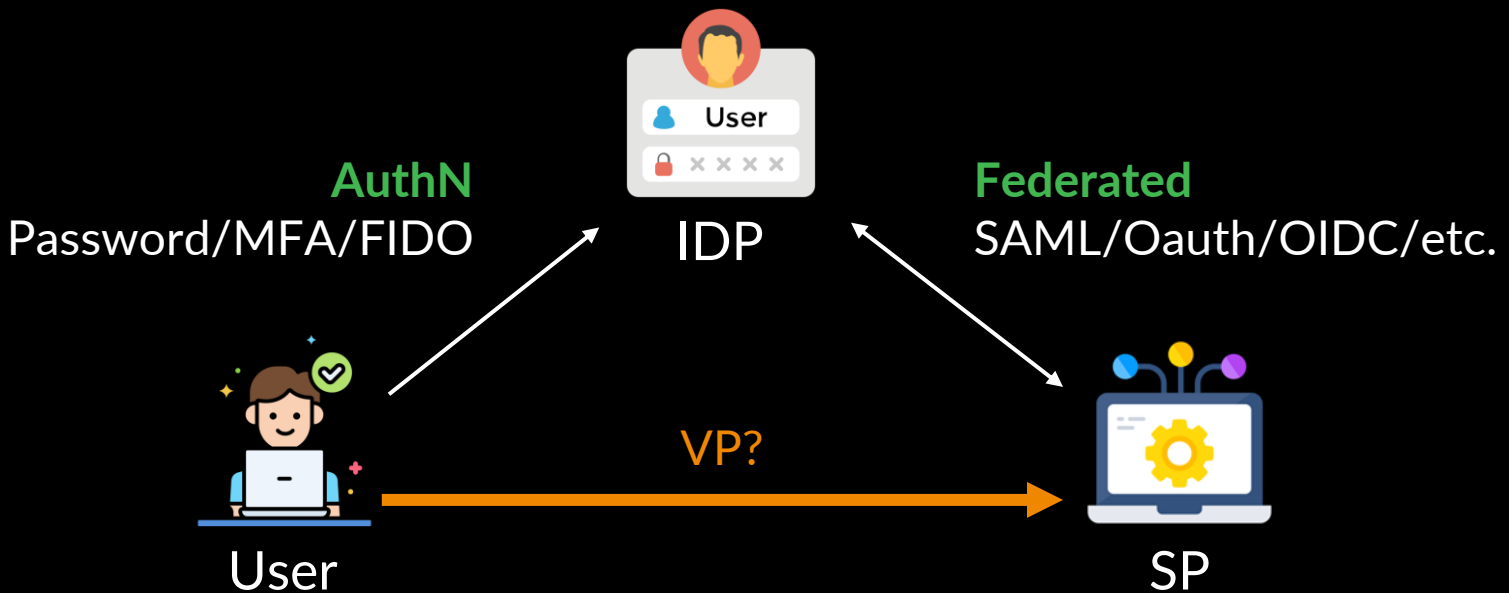
Expensive integrations

The architecture changes and
so will your tech

HYBRID IAM

Where would VCs/VPs fit?

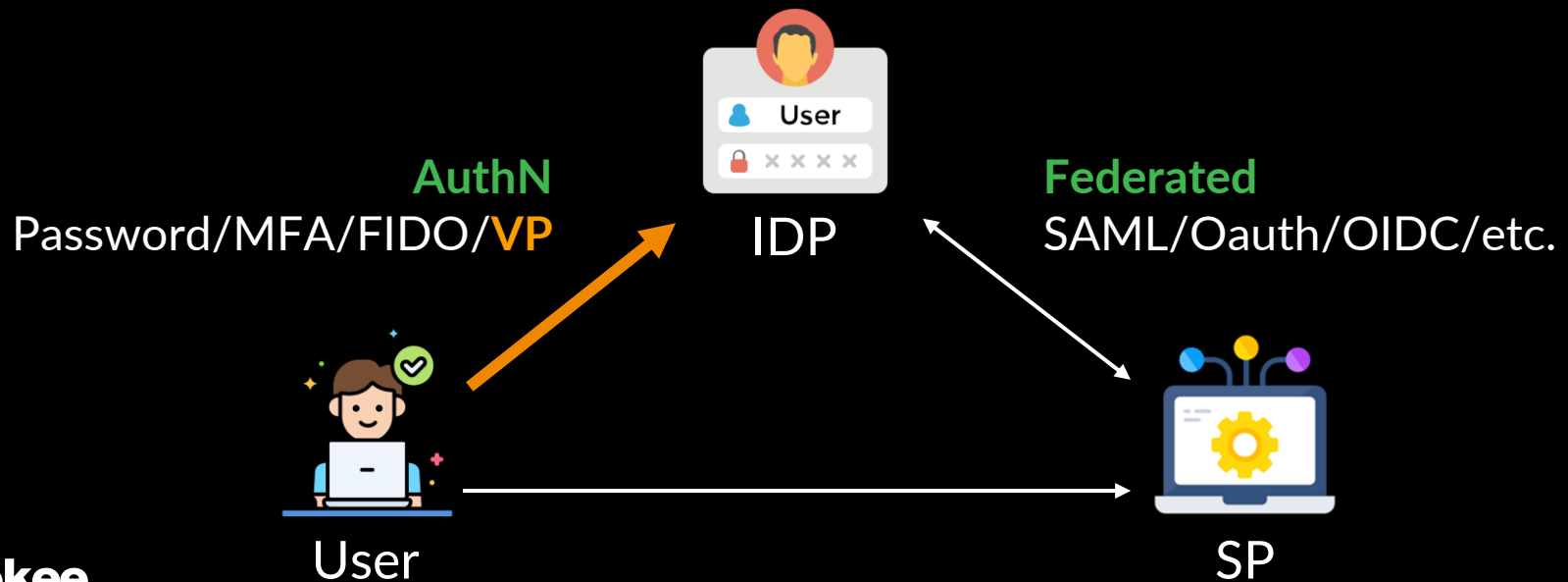
- ✗ M2M SSO Protocol
- ✗ User → SP – maybe in due time



HYBRID IAM

Where would VCs/VPs fit?

- ✗ M2M SSO Protocol
- ✗ User → SP – maybe in due time
- ✓ VP as Authentication Factor



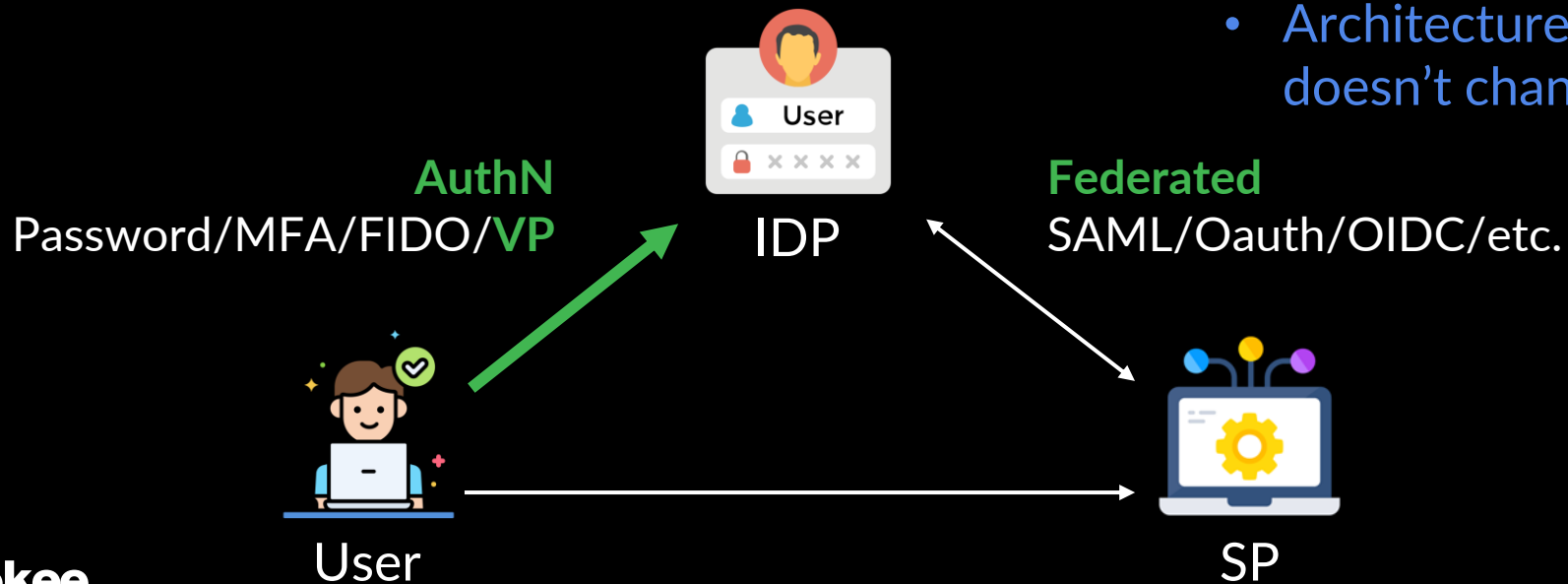
HYBRID IAM

Where would VCs/VPs fit?

- ✗ M2M SSO Protocol
- ✗ User → SP – maybe in due time
- ✓ VP as Authentication Factor

It does make sense

- Passwordless
- Distributed
- Flexible
- Choice-based
- Architecture doesn't change



HYBRID IAM: THERE ARE ALREADY EXAMPLES

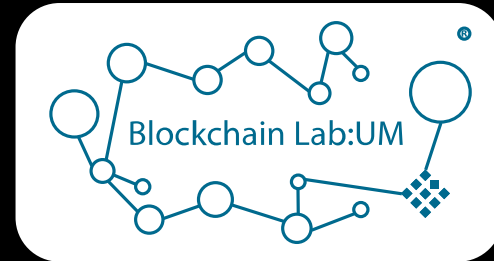
Spoiler: not only Sovrin and Hyperledger Indy

HYBRID IAM: THERE ARE ALREADY EXAMPLES

Spoiler: not only Sovrin and Hyperledger Indy



Metamask Flask



SSI Snap

Save Verifiable Credentials within Metamask Wallet
and use them on-chain and off-chain

HYBRID IAM: THERE ARE ALREADY EXAMPLES

Spoiler: not only Sovrin and Hyperledger Indy



Polygon



IDEN 3



Polygon Identity

Self-Sovereign Identity infrastructure which use ZKPs for on-chain and off-chain verification

HYBRID IAM: WE HAVE TESTED IT. IT WORKS!

We have W3C Data Model standard...

W3C[®]



HYBRID IAM: WE HAVE TESTED IT. IT WORKS!

... we have a Web3 wallet ...



HYBRID IAM: WE HAVE TESTED IT. IT WORKS!

... we have trusted and verifiable
authentication method



WHAT? HOW DOES IT WORK?

W3C

Credentials

They're simply a JSON object

WHAT? HOW DOES IT WORK?

W3C Verifiable Credentials

They're simply a JSON object but...

with a **proof**



WHAT? HOW DOES IT WORK?

W3C Verifiable Credentials

They're simply a JSON object but...

with a **proof**

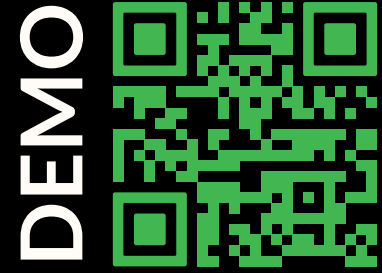


signed JWT



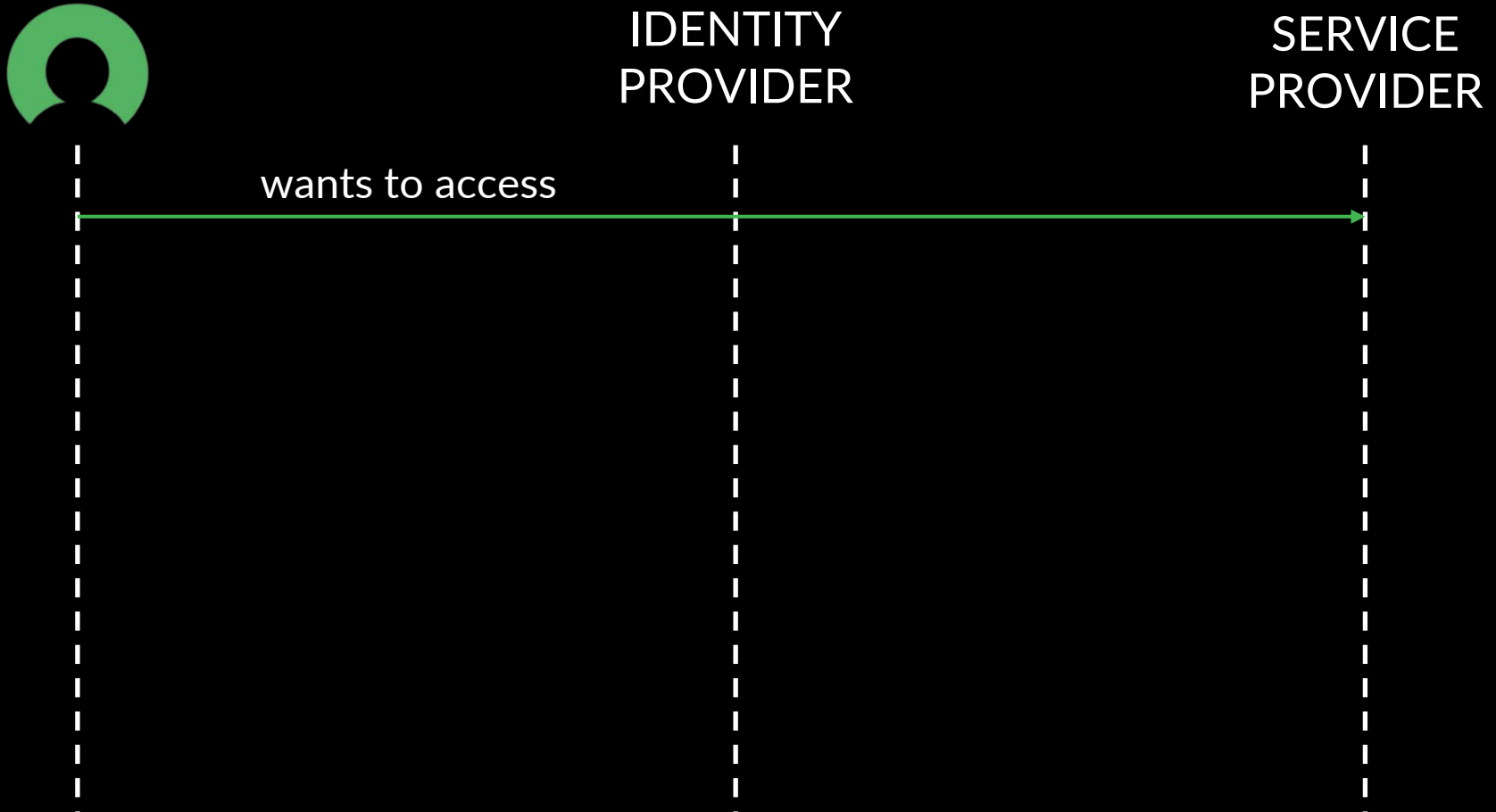
Wallet Signature

Using Ethereum keypair and
DIDs derived from user
address



LET'S SEE IT IN DEPTH

Giving you an example of what this could mean



DEMO



LET'S SEE IT IN DEPTH

Giving you an example of what this could mean

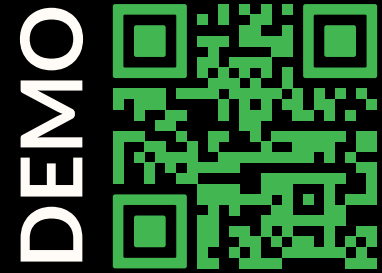


IDENTITY
PROVIDER

SERVICE
PROVIDER

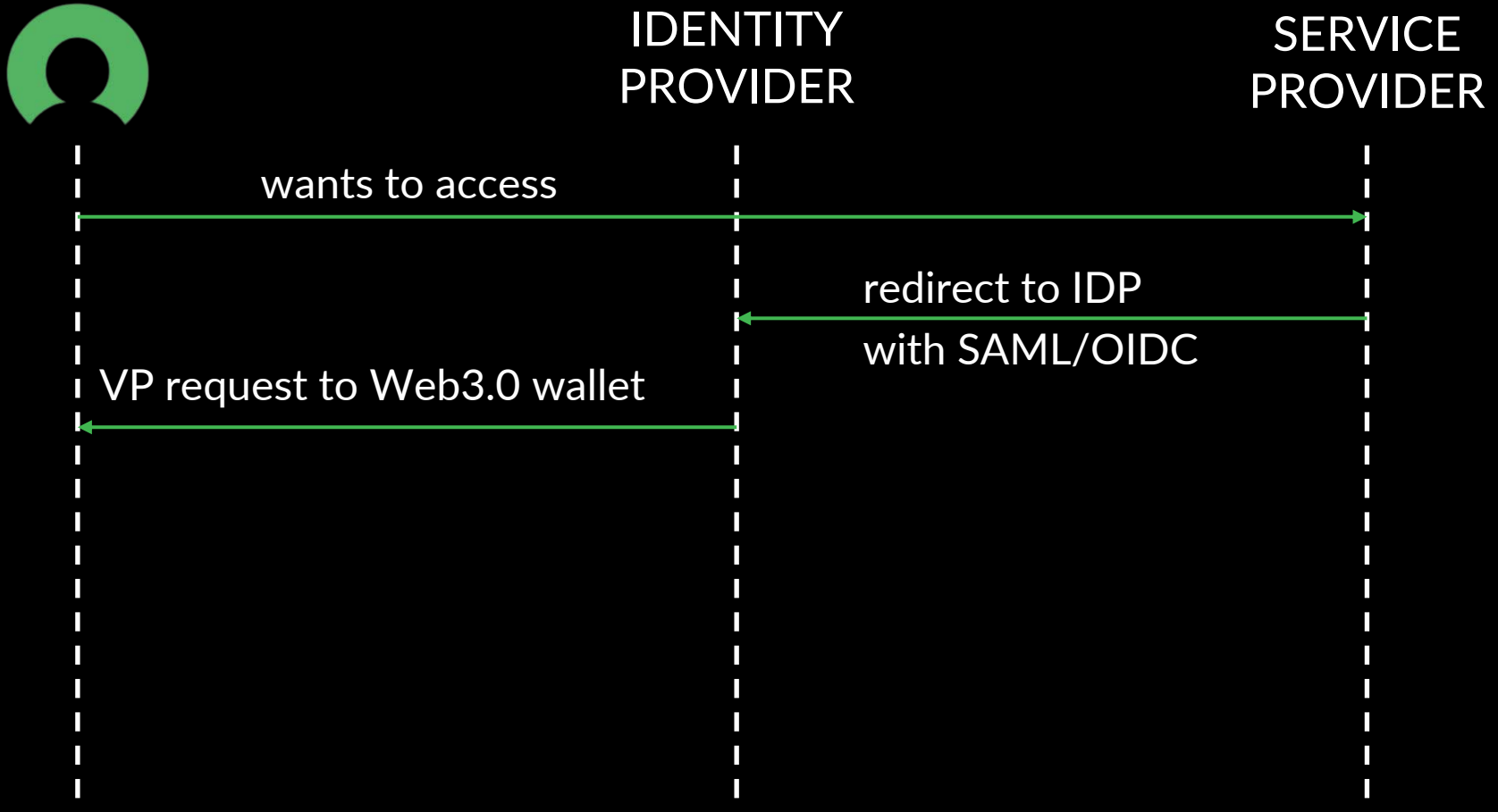
wants to access

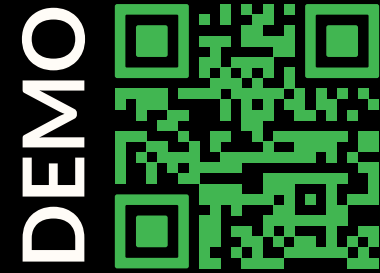
redirect to IDP
with SAML/OIDC



LET'S SEE IT IN DEPTH

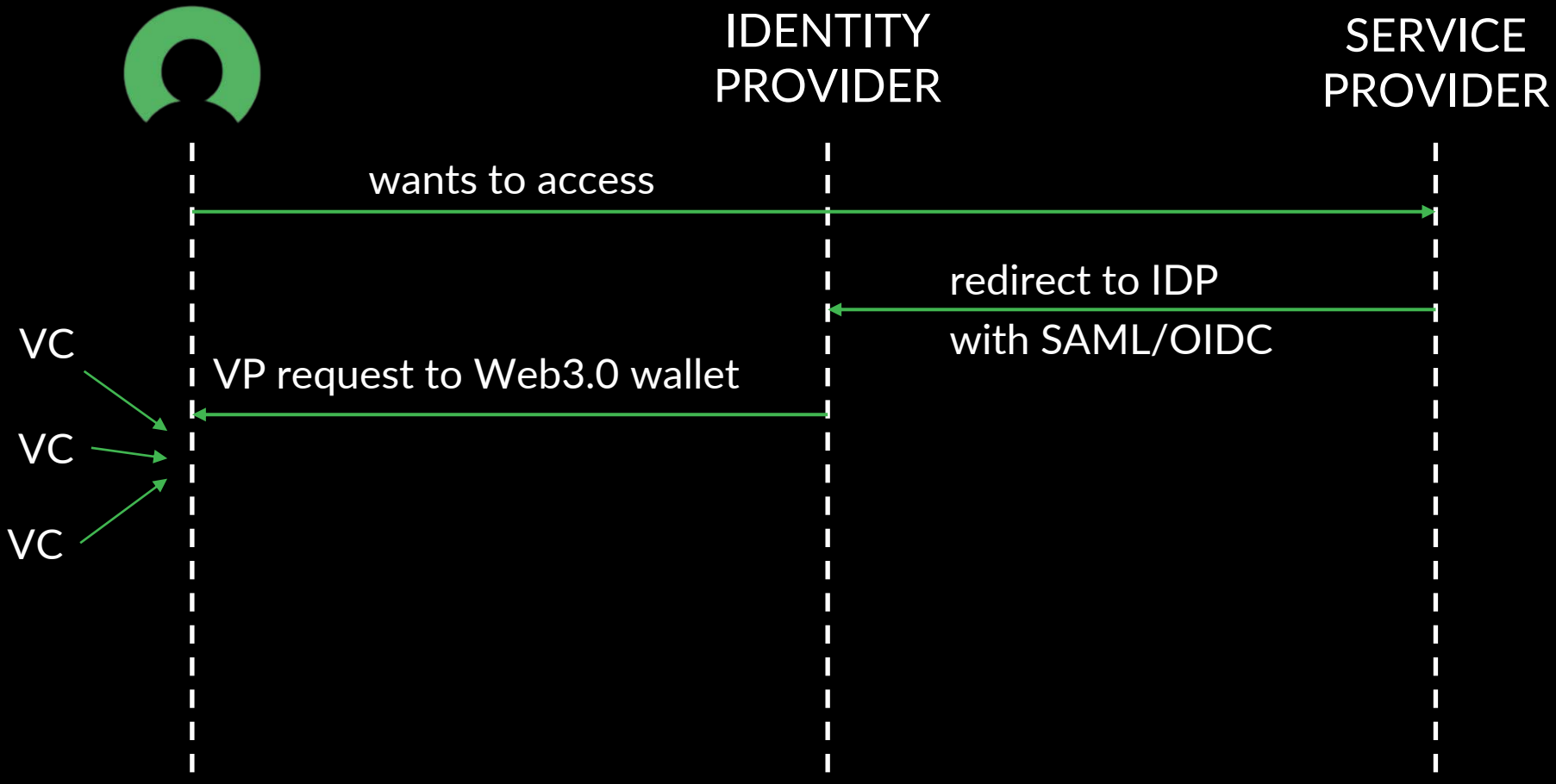
Giving you an example of what this could mean

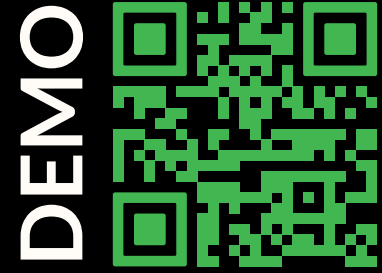




LET'S SEE IT IN DEPTH

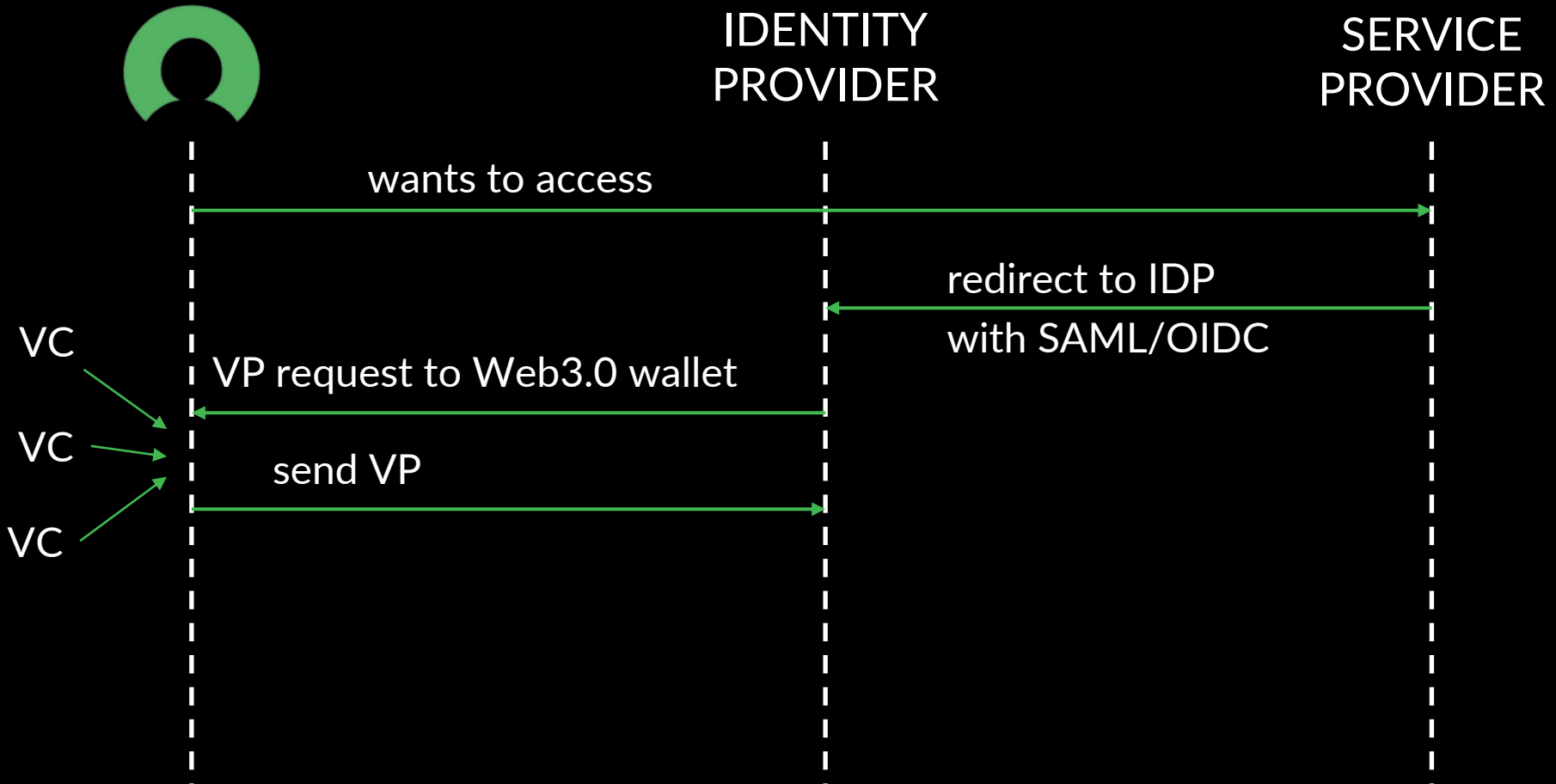
Giving you an example of what this could mean





LET'S SEE IT IN DEPTH

Giving you an example of what this could mean

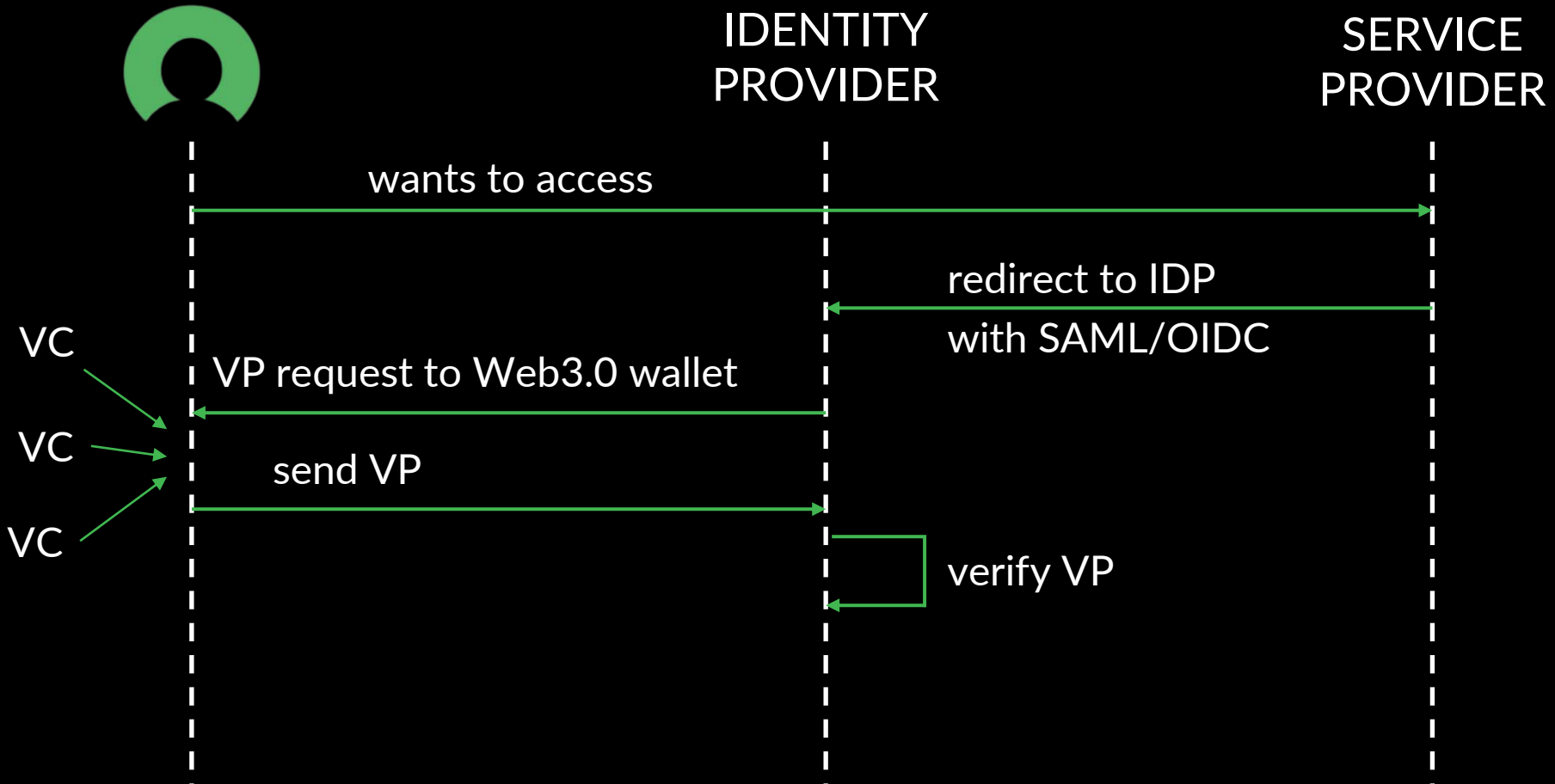


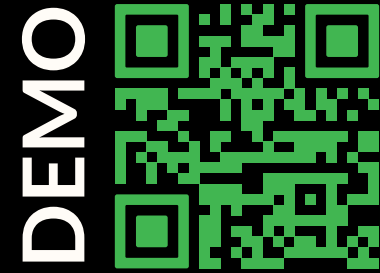
DEMO



LET'S SEE IT IN DEPTH

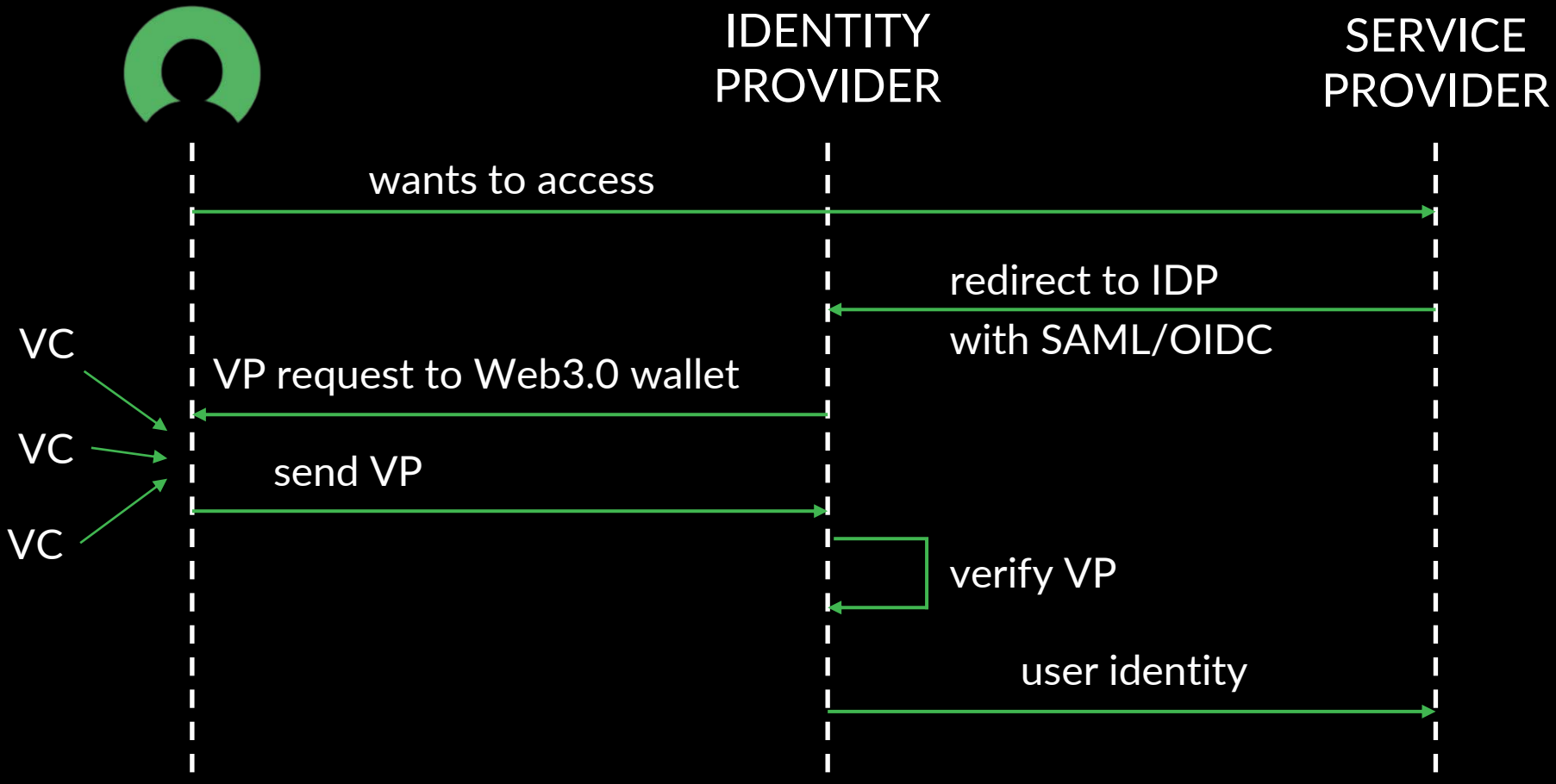
Giving you an example of what this could mean

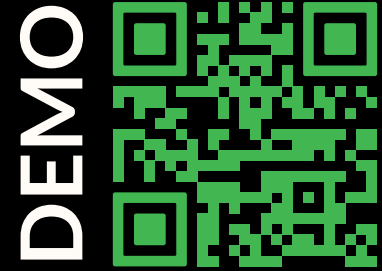




LET'S SEE IT IN DEPTH

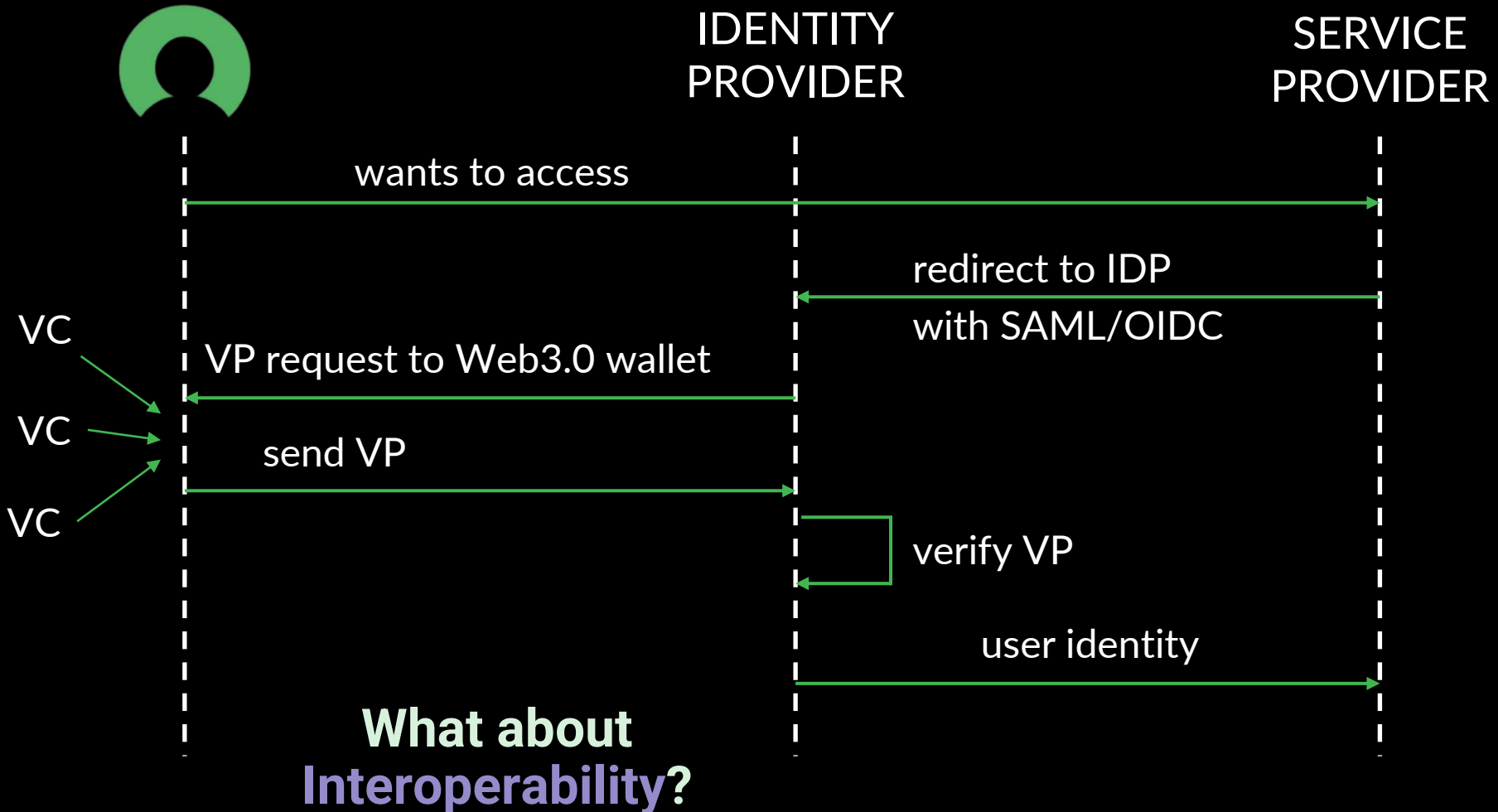
Giving you an example of what this could mean





LET'S SEE IT IN DEPTH

Giving you an example of what this could mean



What about Interoperability?

Tech-independent

User-chosen

Cross-compatible

Easy integration

What about Interoperability?



Tech-independent

User-chosen

Cross-compatible

Easy integration

What about Interoperability?



Tech-independent



User-chosen

Cross-compatible

Easy integration

What about Interoperability?



Tech-independent



User-chosen



Cross-compatible

Easy integration

What about Interoperability?



Tech-independent



User-chosen



Cross-compatible



Easy integration

What about Interoperability?



Tech-independent



User-chosen



Cross-compatible

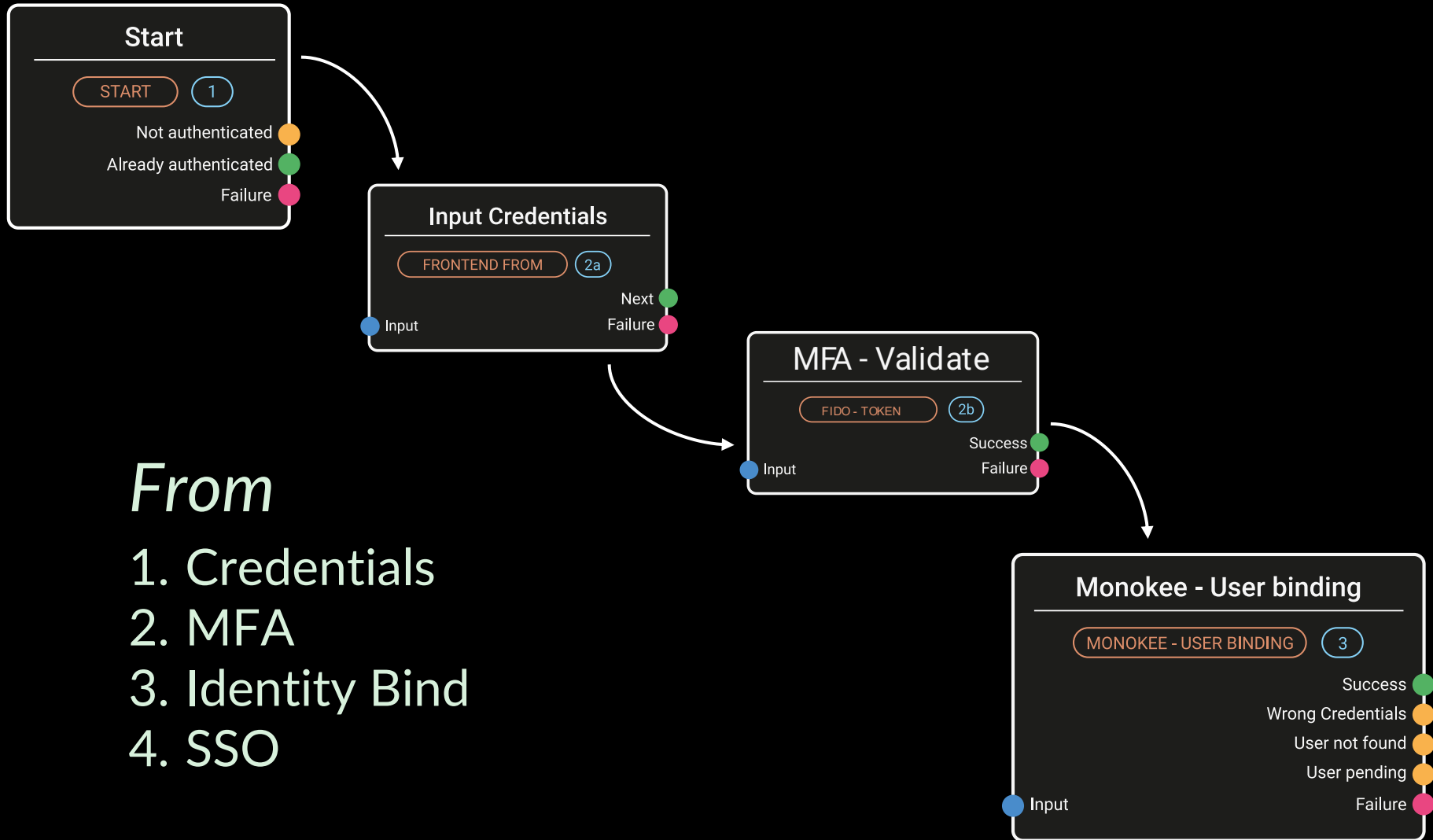


Easy integration

The key is ...

IDENTITY ORCHESTRATION

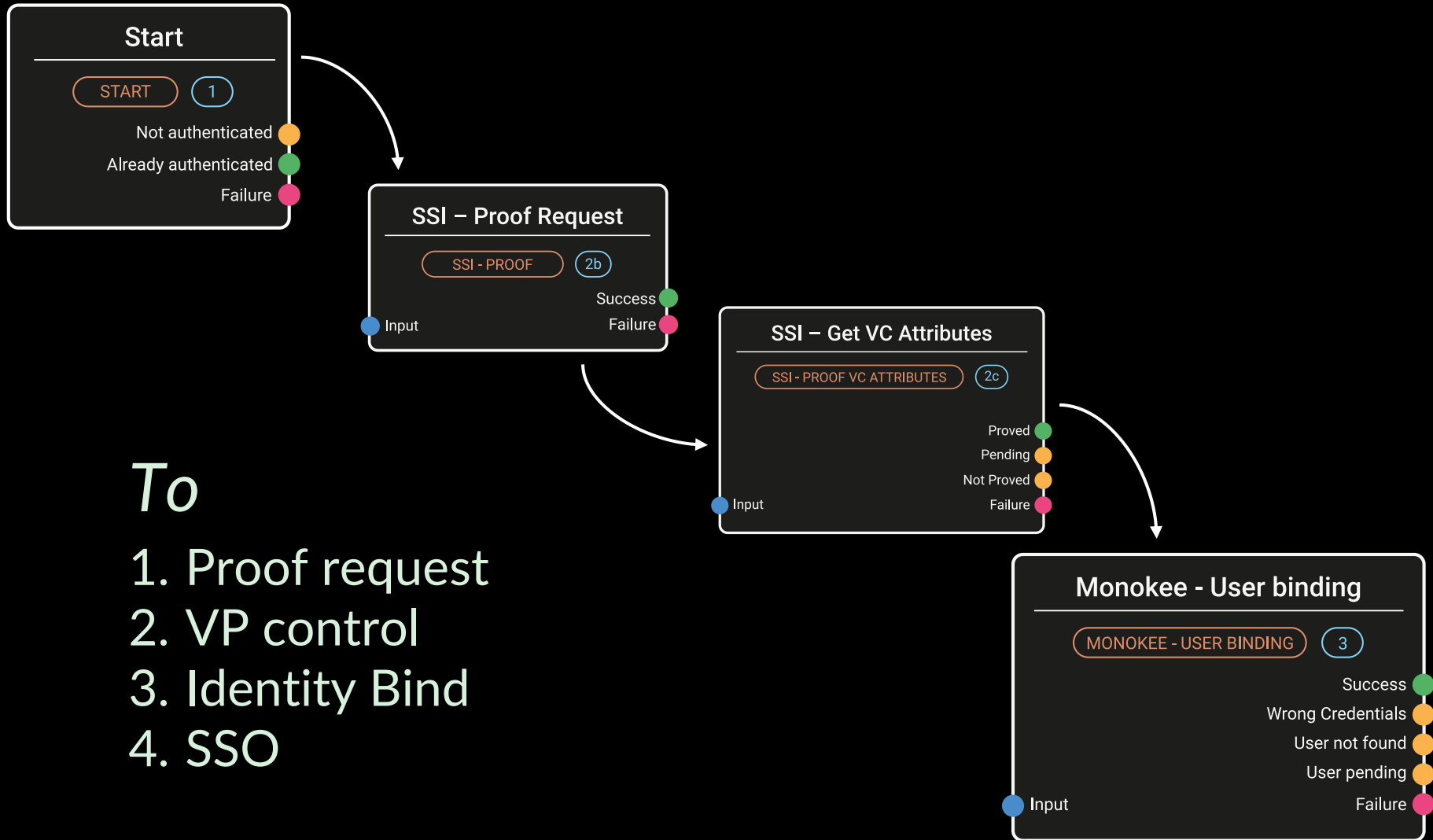
HYBRID IAM: IDENTITY ORCHESTRATION



From

1. Credentials
2. MFA
3. Identity Bind
4. SSO

HYBRID IAM: IDENTITY ORCHESTRATION



To

1. Proof request
2. VP control
3. Identity Bind
4. SSO



Thank you!

HYBRID IAM

Interoperable VCs for Workforce Identity



DR. MATTIA ZAGO

Solutions Architect

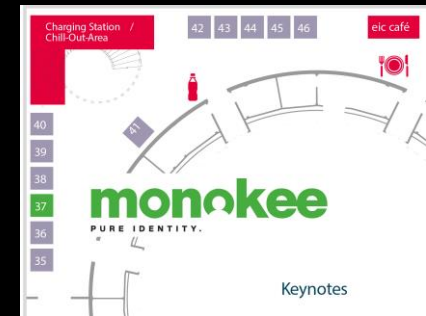
mattia.zago@monokee.com



MATTEO MIDENA

Self-Sovereign Identity Specialist

matteo.midena@monokee.com



Find us at Booth #37



Play with the demo
eic23.monokee.com