An introduction to decentralized identity

Stefan van der Wiele
Senior Product Manager – Microsoft
@wiele / @wiele@infosec.exchange

Stefan van der Wiele

Senior Product Manager
Microsoft Entra

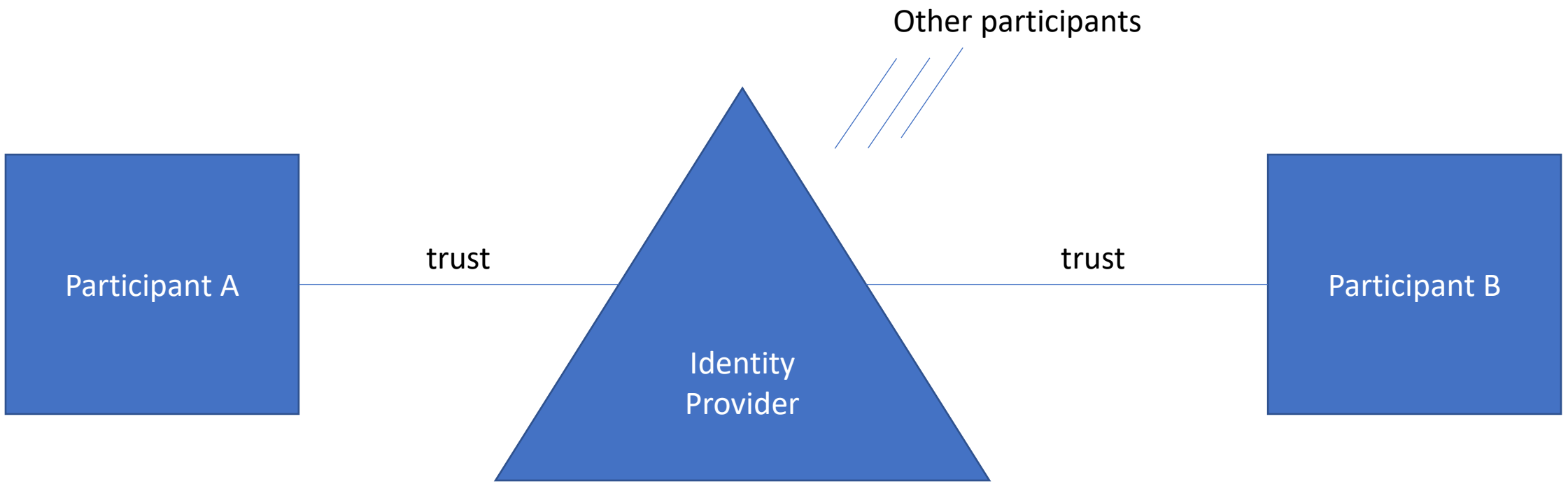
Microsoft

Owner of a radio station
hotdanceradio.com

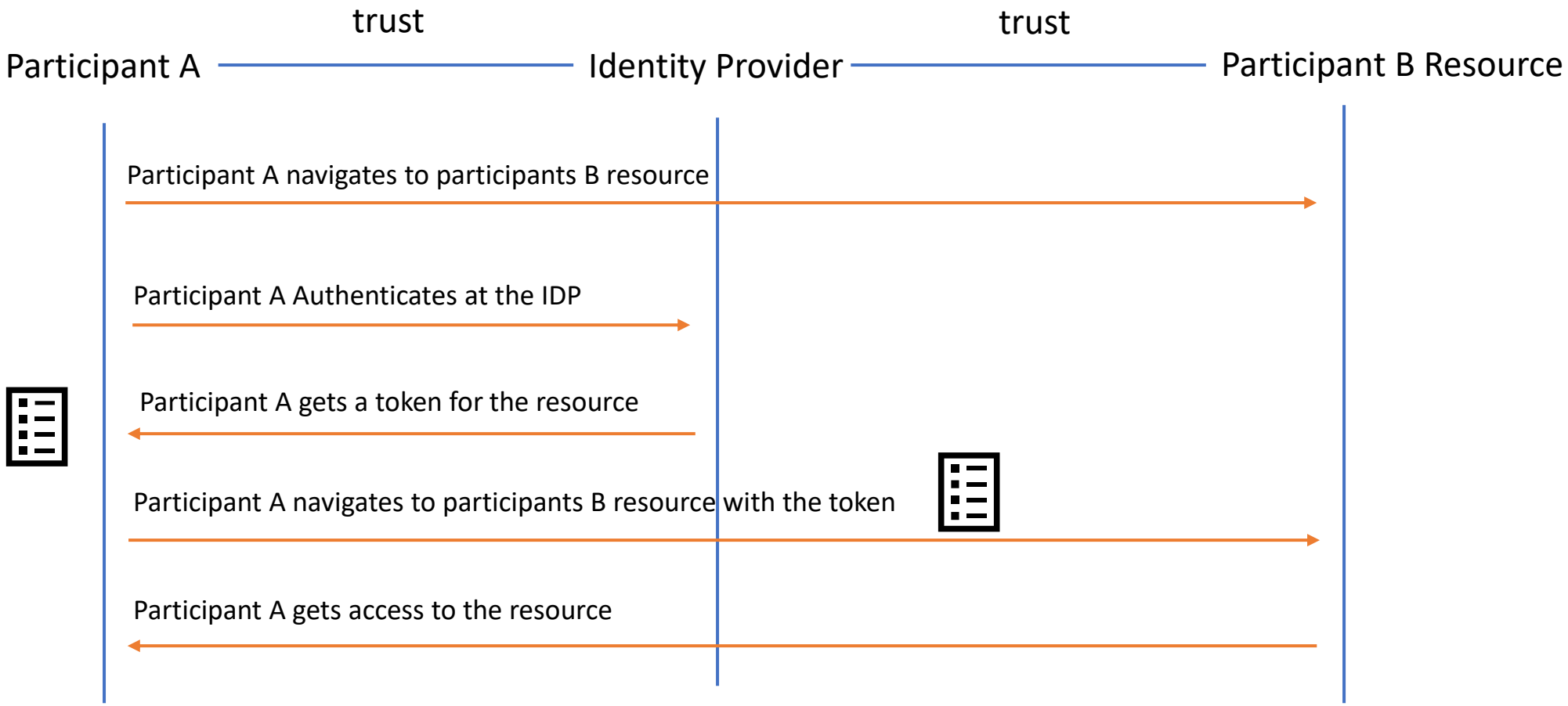
hotdanceradio
hits with a beat

Who can explain the difference between centralized and decentralized identity?

Centralized vs. Decentralized

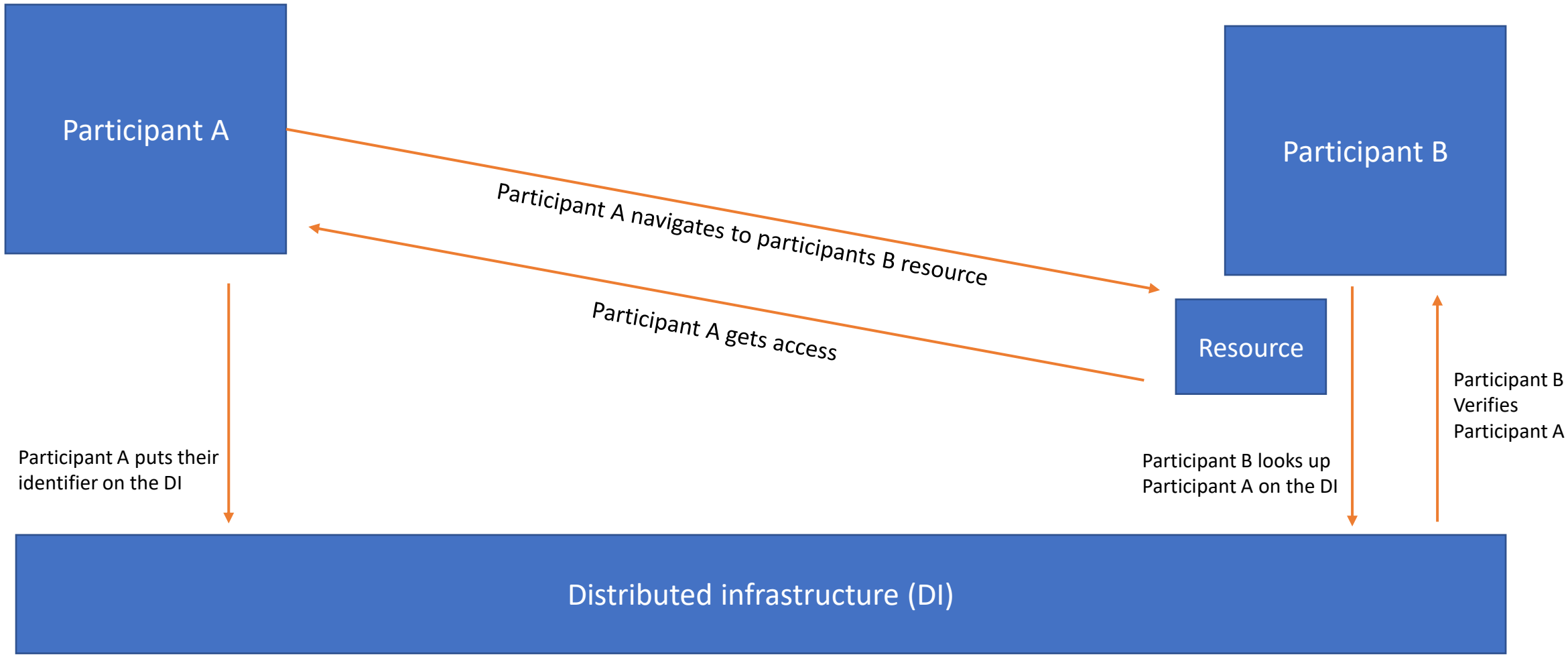


Examples: OpenIDConnect, SAML, WS-Fed


trust
trust
Participant A
Identity Provider
Participant B Resource
Participant A navigates to participants B resource
Participant A Authenticates at the IDP
Participant A gets a token for the resource
Participant A navigates to participants B resource with the token
Participant A gets access to the resource

Centralized vs. Decentralized

Centralized vs. Decentralized

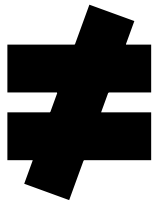


Over a million are owed money by failed crypto exchange

1 day ago · Comments

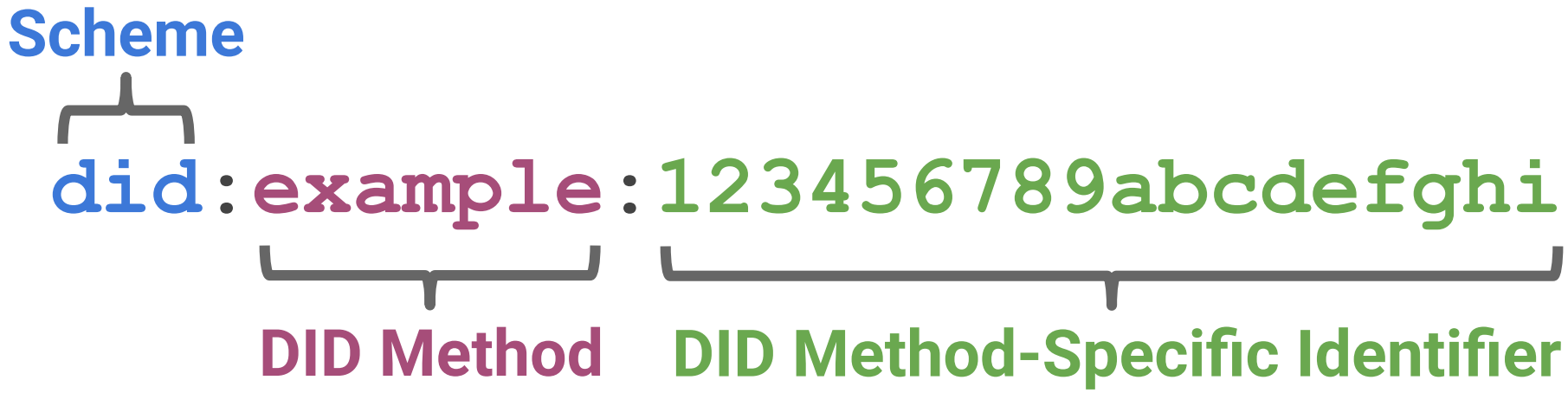
GETTY IMAGES

Decentralized Identity



Blockchain

Decentralized Identifiers



Decentralized Identifiers Methods

- Over 80 different methods
- Defines the trusted infrastructure
- How to read and write identifiers to the infrastructure

did:ion:	PROVISIONAL	Bitcoin	Various DIF contributors	ION DID Method
did:iota:	PROVISIONAL	IOTA	IOTA Foundation	IOTA DID Method
did:ipid:	PROVISIONAL	IPFS	TranSendX	IPID DID method
did:is:	PROVISIONAL	Blockcore	Blockcore	Blockcore DID Method
did:iwt:	PROVISIONAL	InfoWallet	Raonsecure	InfoWallet DID Method
did:jlinc:	PROVISIONAL	JLINC Protocol	Victor Grey	JLINC Protocol DID Method
did:jnctn:	PROVISIONAL	Jnctn Network	Jnctn Limited	JNCTN DID Method
did:jolo:	PROVISIONAL	Ethereum	Jolocom	Jolocom DID Method
did:keri:	PROVISIONAL	Ledger agnostic	Dr. Sam Smith, Charles Cunningham, Phil Feairheller	KERI DID Method

SIONAL	Zilliqa	Julio Cabrapan Duarte	tyronZIL DID-Method
SIONAL	DID Specification	Chainyard	TYS DID Method
SIONAL	Tezos	Spruce Systems, Inc.	Tezos DID Method
SIONAL	uns.network	Space Elephant SAS	UNIK DID Method
SIONAL	Bitcoin SV	UNISOT AS	UNISOT DID Method
SIONAL	uns.network	Space Elephant SAS	UNS DID Method
ECATED	Ethereum	uPort	
SIONAL	Veres One	Digital Bazaar	Veres One DID Method
SIONAL	bif	China Academy of Information and Communications Technology (CAICT)	VAA Method
SIONAL	Ethereum	Vaultie Inc.	Vaultie DID Method
SIONAL	VP	VP Inc.	VP DID Method
SIONAL	NEO2, NEO3, Zilliqa	Vivid	Vivid DID Method
SIONAL	Vivvo	Vivvo Application Studios	Vivvo DID Method
SIONAL	Web	Oliver Terbu, Mike Xu, Dmitri Zagidulin, Amy Guy	Web DID Method
SIONAL	Weelink Network	Weelink	Weelink DID Method
did:work:	PROVISIONAL	Hyperledger Fabric	Workday, Inc.	Workday DID Method

[DID Specification Registries (w3.org)]

Decentralized Identifiers

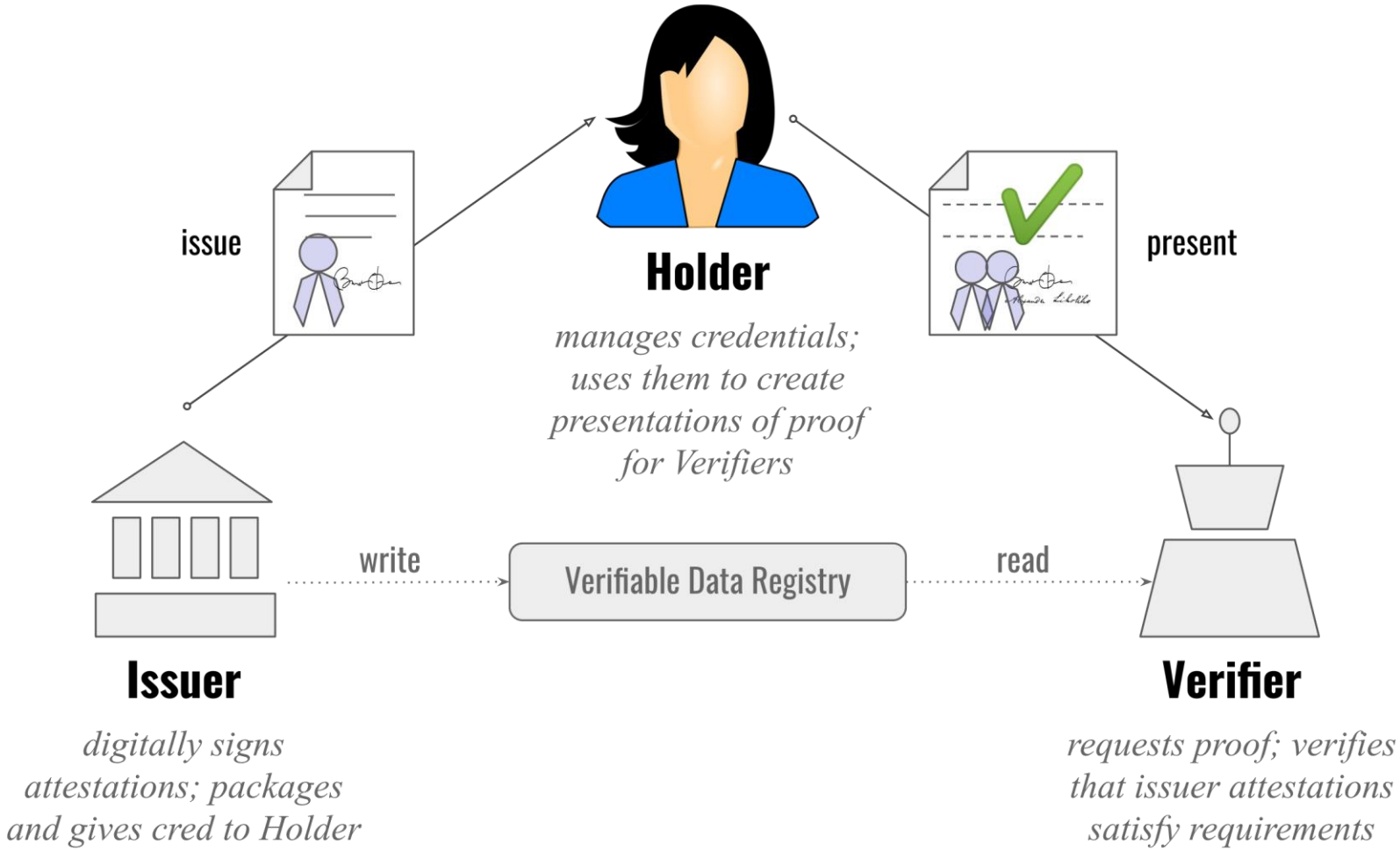
1. **DID** (for self-description)
2. **Set of public keys** (for verification)
3. **Set of auth methods** (for authentication)
4. **Set of service endpoints** (for interaction)
5. **Timestamp** (for audit history)
6. **Signature** (for integrity)

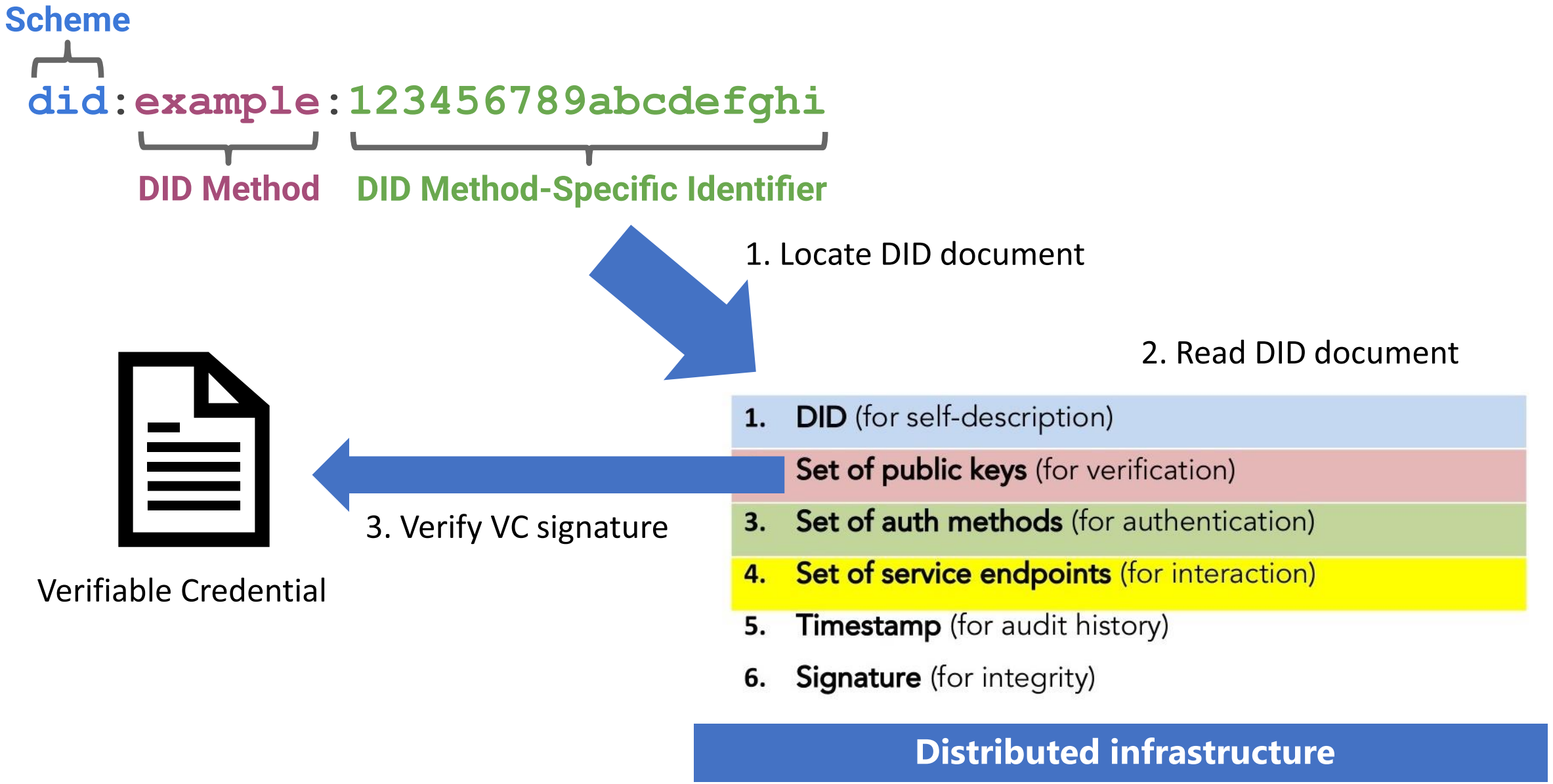
Decentralized Identifiers – Document Example


```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{

    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

W3C Verifiable Credentials




Scheme
did:example:123456789abcdefghi
DID Method
DID Method-Specific Identifier
1. Locate DID document
2. Read DID document
1. DID (for self-description)
Set of public keys (for verification)
3. Set of auth methods (for authentication)
4. Set of service endpoints (for interaction)
5. Timestamp (for audit history)
6. Signature (for integrity)
Distributed infrastructure
3. Verify VC signature
Verifiable Credential

Which DID methods do you know?

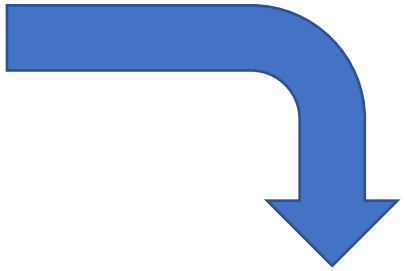
Example DID methods

What is did:web?

- A new DID method that allows participants to bootstrap trust using a web domain's existing reputation.

did:web Method Specification (w3c-ccg.github.io)

did:web:example.com

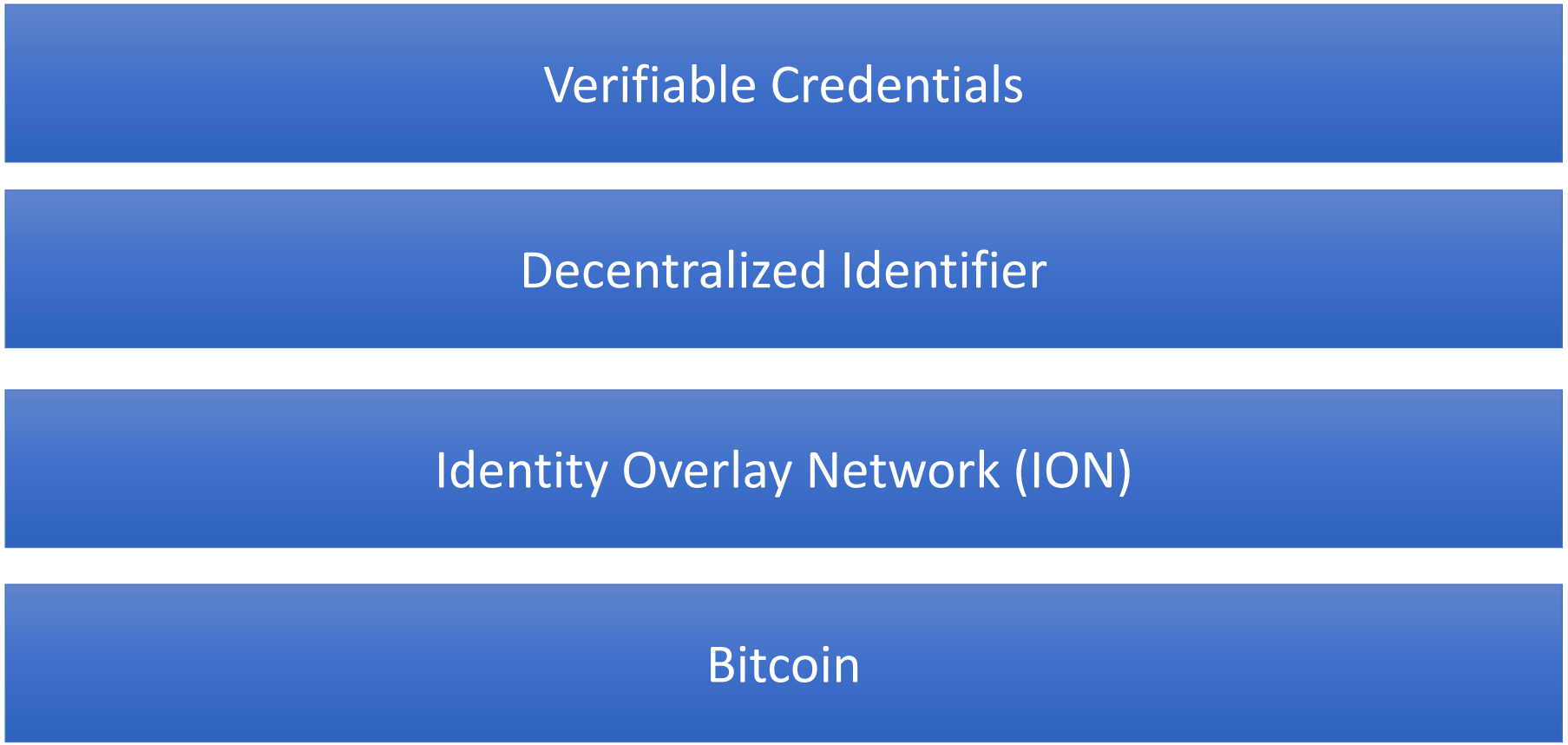


https://example.com/.well-known/did.json

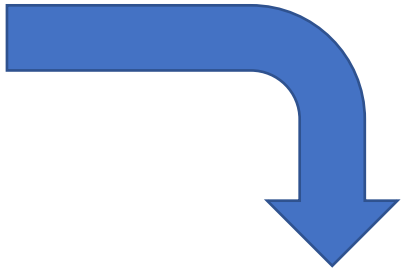
EXAMPLE 1: Example did:web DID document


```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:web:example.com",
  "verificationMethod": [{
     "id": "did:web:example.com#owner",
     "type": "Secp256k1VerificationKey2018",
     "owner": "did:web:example.com",
     "ethereumAddress": "0xb9c5714089478a327f09197987f16f9e5d936e8a"
  }],
  "authentication": [
     "did:web:example.com#owner"
  ]
}
```

What is DID:ION



did:ion:123456678



Lookup on ION network

EXAMPLE 1: Example did:web DID document

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:web:example.com",
  "verificationMethod": [{
     "id": "did:web:example.com#owner",
     "type": "Secp256k1VerificationKey2018",
     "owner": "did:web:example.com",
     "ethereumAddress": "0xb9c5714089478a327f09197987f16f9e5d936e8a"
  }],
  "authentication": [
     "did:web:example.com#owner"
  ]
}
```

What is Microsoft Entra Verified ID

- Provides the backend to issue and verify verifiable credentials
- Provides a wallet (Microsoft Authenticator)
- API for issue and verify
- Support for DID:Web (default) and DID:ION

Use Cases & Demos

Accepts job offer

Visits employer portal to complete pre-onboarding

Identity validated by network partner

Receives verifiable credential with proven identify attributes

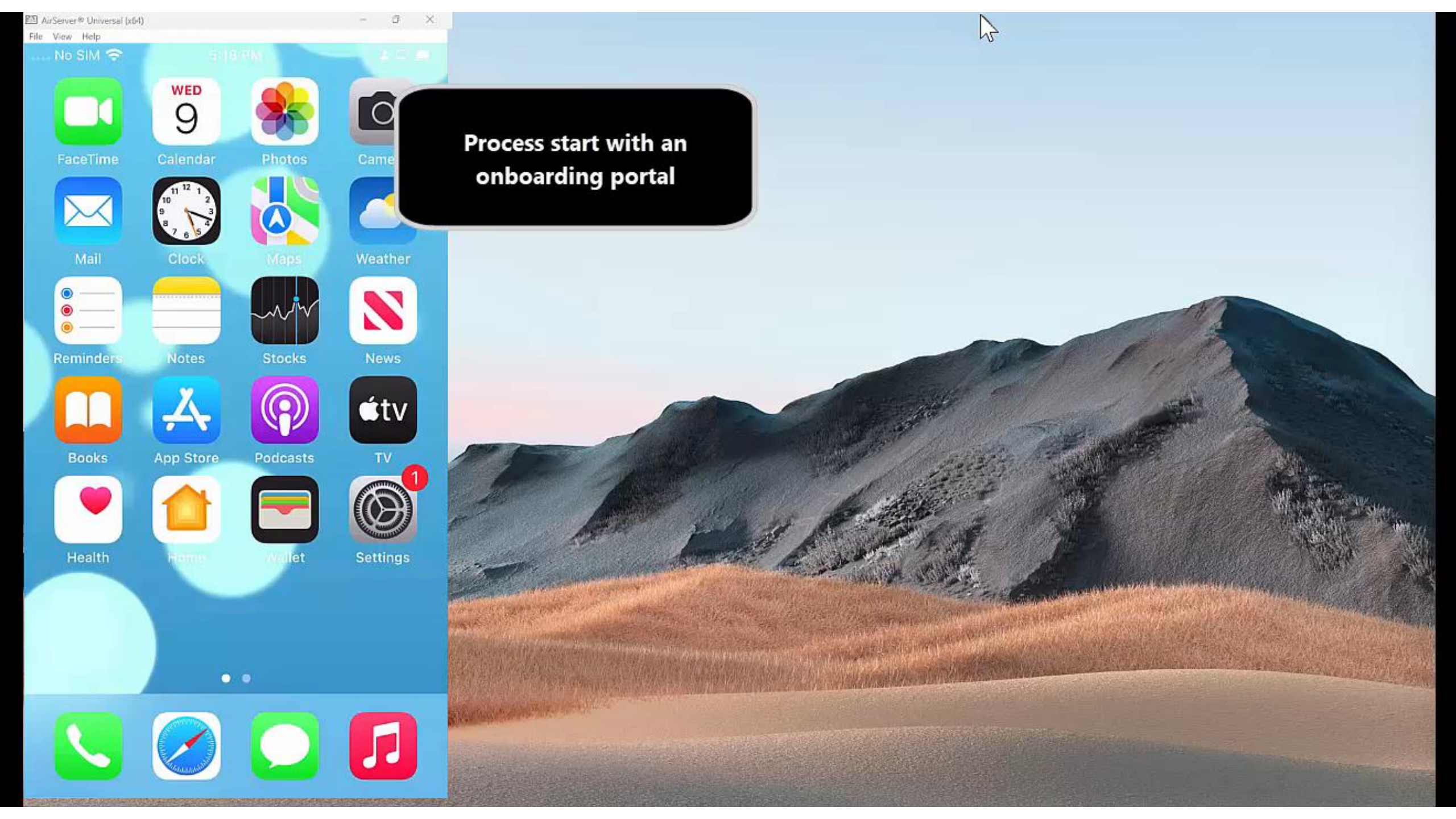
First day of work

Uses verifiable credential to remotely access and set up new account

Receives workplace credential, enabling access & benefits

Completes trainings, attested to workplace credential for compliance and access

Efficient access to employee perks and ongoing life tasks


AirServer® Universal (x64)
File View Help
No SIM
5:18 PM
FaceTime
WED
9
Calendar
Photos
Mail
Clock
Maps
Weather
Reminders
Notes
Stocks
News
Books
App Store
Podcasts
TV
Health
Home
Wallet
Settings
1
Process start with an onboarding portal

Common Use Cases

Fast remote onboarding

Validate identity information for trustworthy self-service enrollment and reduced time-to-hire.

More secure access

Quickly verify an individual's credentials and status to grant least-privilege access with confidence.

Easy account recovery

Replace support calls and security questions with a streamlined self-service process to verify identities.

Custom business solutions

Easily build solutions for a wide range of use cases with our developer kit, APIs, and documentation.

192 countries

6000 identification documents

1000s organizational attributes

Millions individual ID attributes

Decades of experience to go from idea to implementation within hours

Trusted identity verification providers

acuant · AUTHENTIX IDENTITY INTELLIGENCE · CLEAR · Credivera · IDEMIA · jumio · LexisNexis RISK SOLUTIONS · onfido · Socure · VU

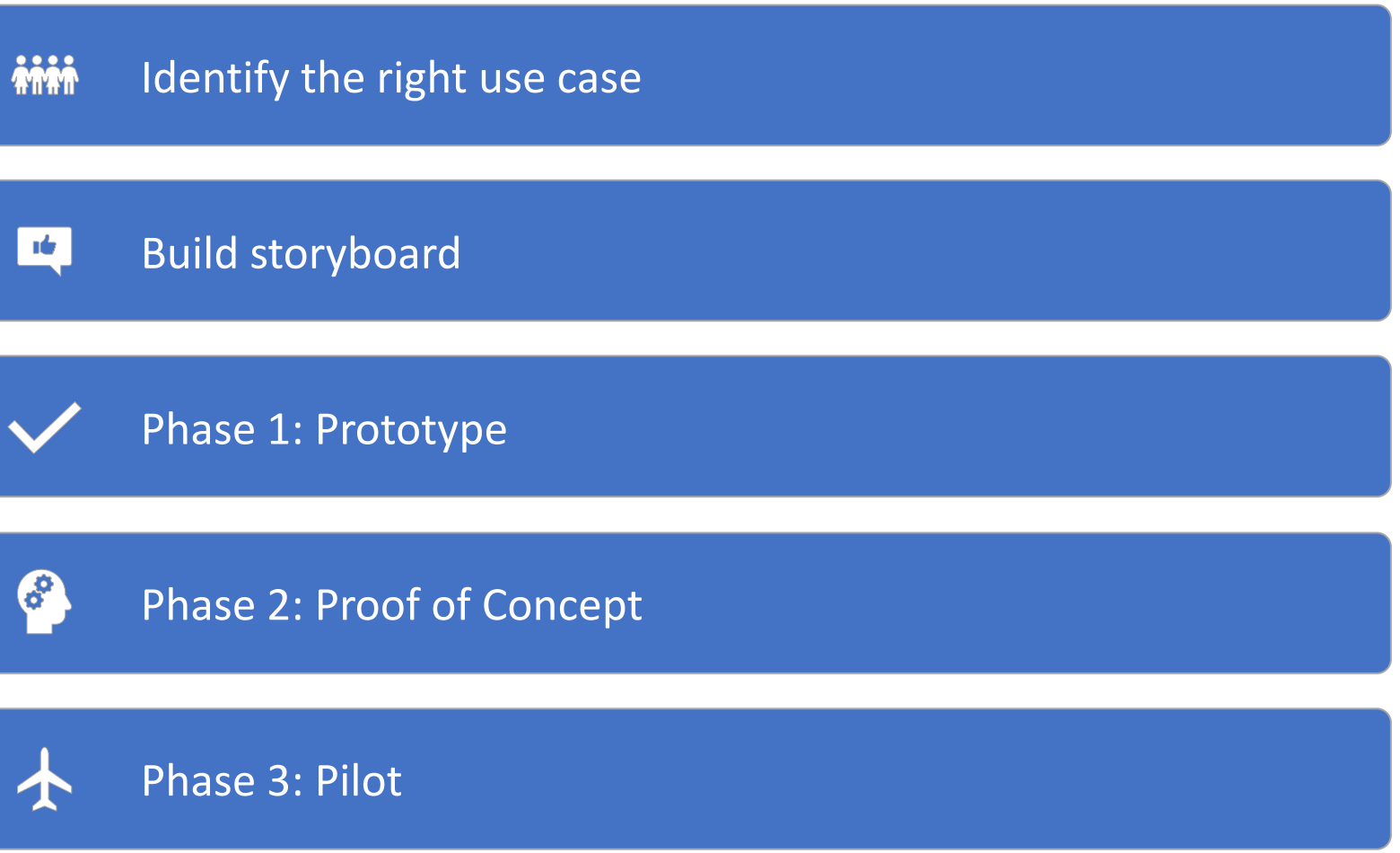
Adoption acceleration with technical solutions

AffinitiQuest.io · avanade · condatis a sitekit company · UNIFY SOLUTIONS · ITOCHU Techno-Solutions Corporation

Developed with global standards

DIF · ION · W3C CCG

From idea to pilot with Microsoft Entra Verified ID



Existing users MFA onboarding

To Alice Smith
From contoso IT
Subject MFA migration

Please help us get more secure. Please navigate to our onboarding portal with instructions how to setup your personal phone and help contoso be more secure.

MFA Portal

Email as part of a campaign from contoso

mfa.contoso.com

Welcome to MFA Onboarding portal Alice Smith

Please follow the below steps

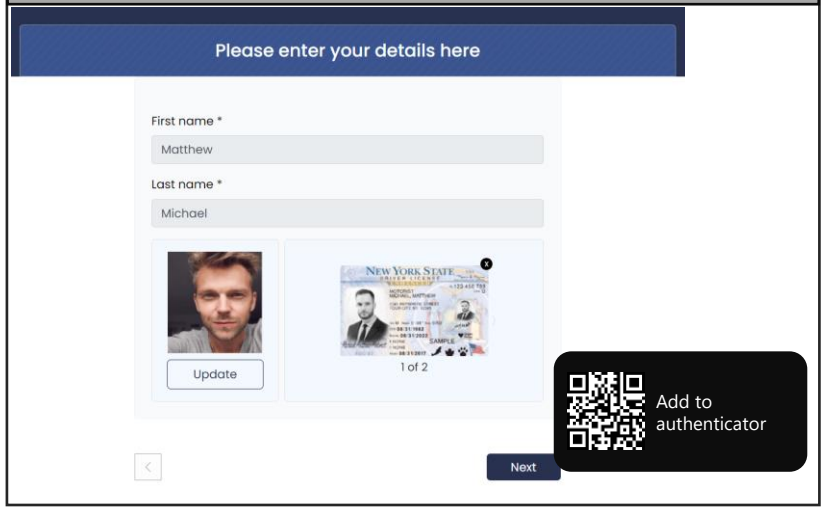
Install Authenticator — Step 1

Get Verified with the Identity proofing partner — Step 2

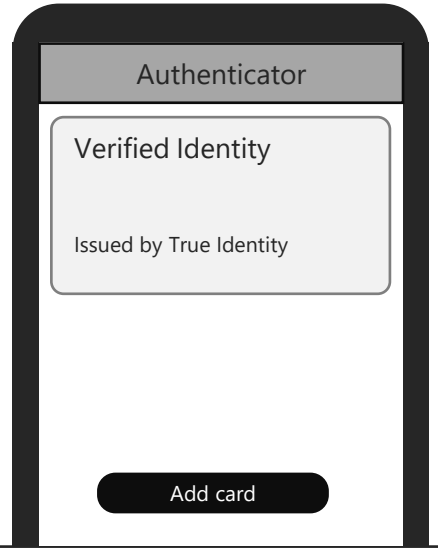
Present your VC — Step 3

User signed into MFA onboarding portal

trueudentity.com/contoso



Get ID Verified on IDV partner SAAS portal



Accept a card

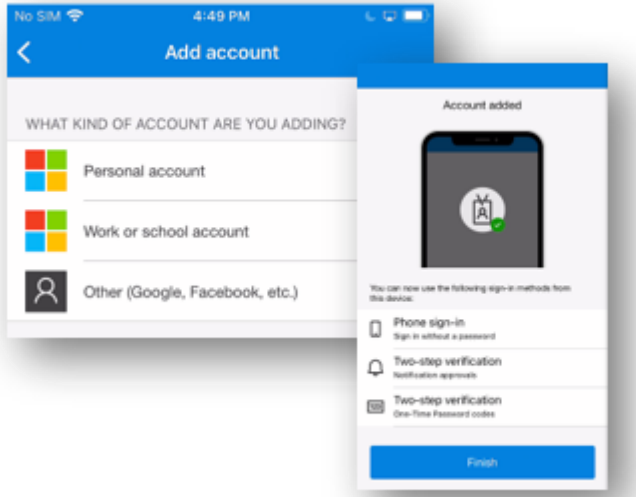
mfa.contoso.com

Welcome back to the MFA Onboarding portal Alice Smith

Proof your identity

Here are some instructions how to setup MFA on your phone....

Present the proof to the contoso employee portal



Finish MFA setup

Resources

http://aka.ms/verifyonce
Verified ID website

Microsoft Entra Product Page

http://aka.ms/ownyouridentity
Learn more about decentralized identity

http://aka.ms/didfordevs
Developer documentation

http://entra.microsoft.com
Get started for free

https://aka.ms/vcdemo
Demo Site

Go do’s

Try it out yourself
https://aka.ms/diddemo

Build it yourself
https://aka.ms/ilovecats

Thank you!

Twitter: @wiele

Mastodon: @wiele@infosec.exchange