

# Decentralized Identity

at Microsoft



# 2018: Incubation hypothesis

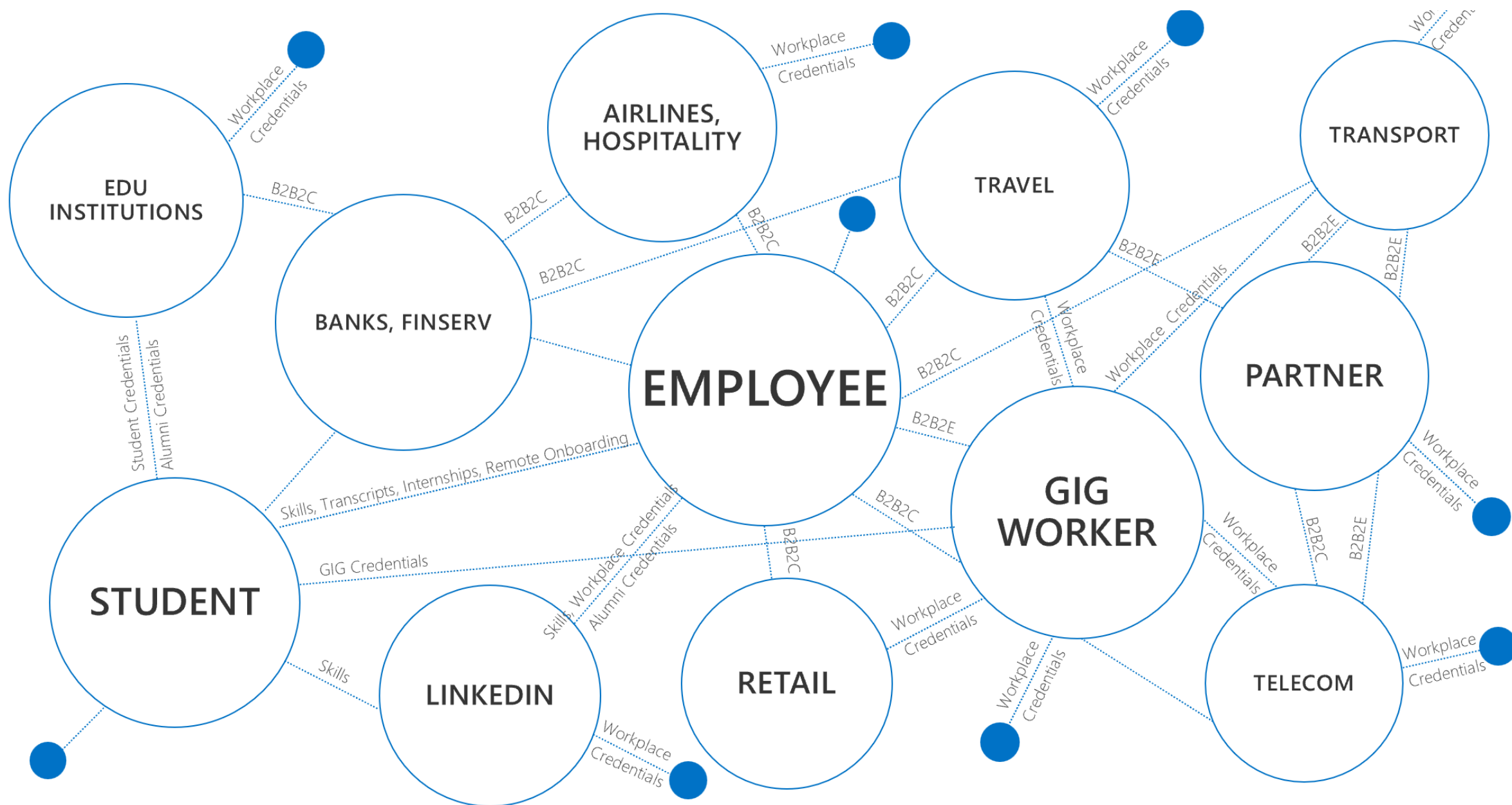
## 2022: First Release!

Each of us needs **digital identity we own and control**, one which securely and privately stores **all elements of our digital identity**.

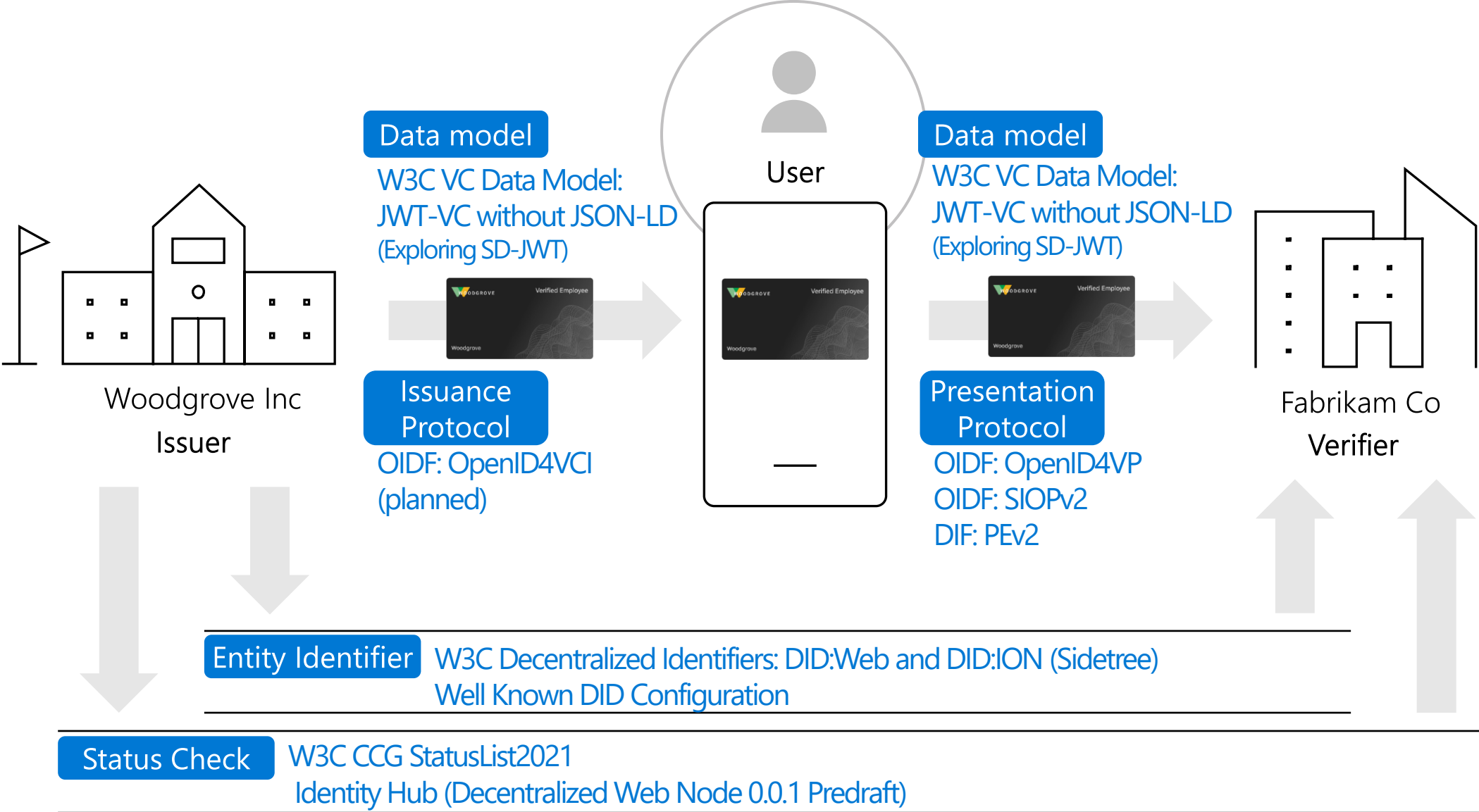
This self-owned identity must **seamlessly integrate into our lives** and give us **complete control over how our identity data is accessed** and used.



# Credentials to power the trust fabric for the internet



# Standards used



# 92%

of organizations  
perform identity  
verification today



Onboarding for employees,  
contractors, customers



Access to high-value apps  
and resources



Self-service account  
recovery

# 82% of organizations wish there was a better way



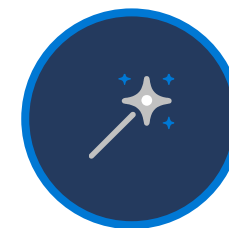
More protection against breaches  
Credentials verified by reliable parties  
Meeting regulatory requirements by default

**Safer**



No custom integration  
No need to store users PII  
No wait times for id verification

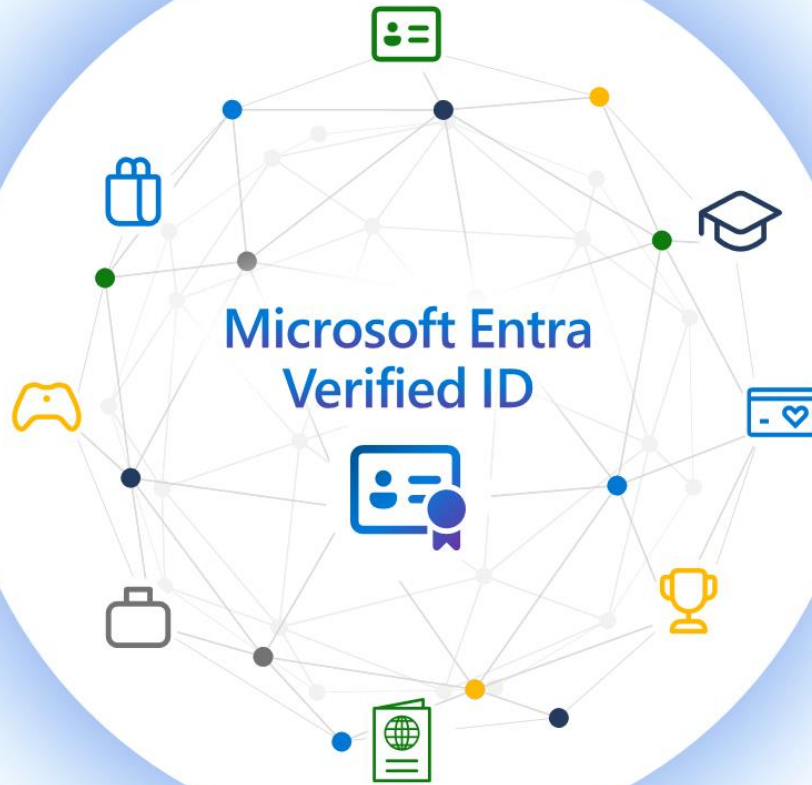
**Faster**



Lower cost  
As easy using digital cards  
Verify once, use everywhere

**Easier**

Microsoft Entra  
Verified ID



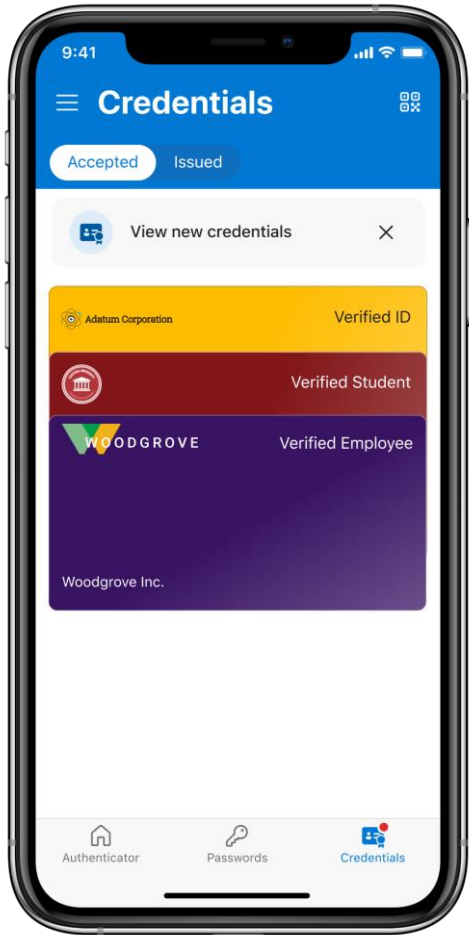
# Demonstration: ID verification based on open standards



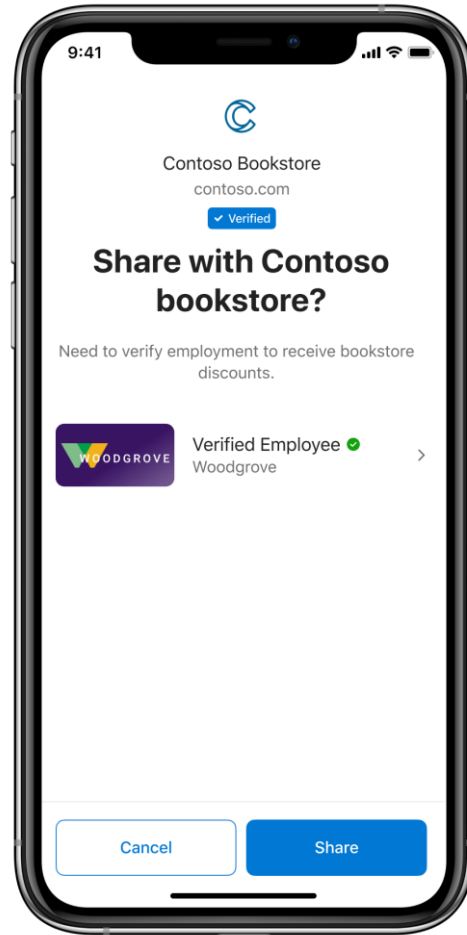
<http://aka.ms/diddemo>



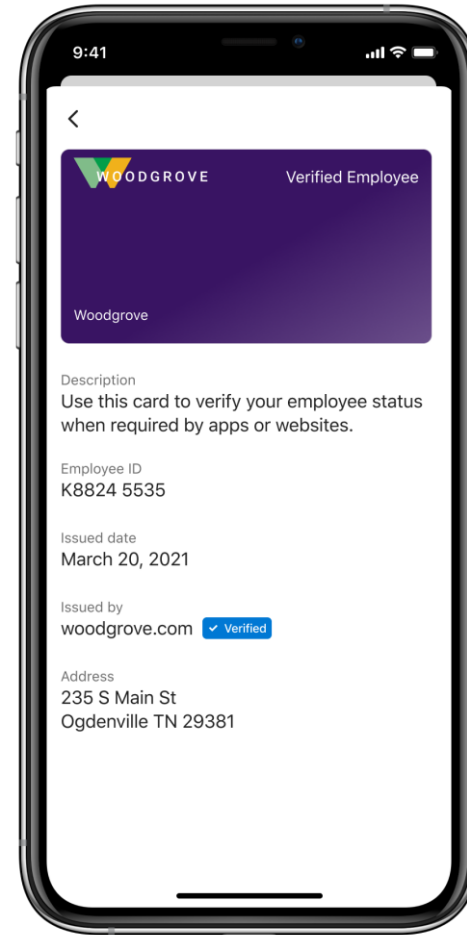
# Entra Verified ID: a better way to verify



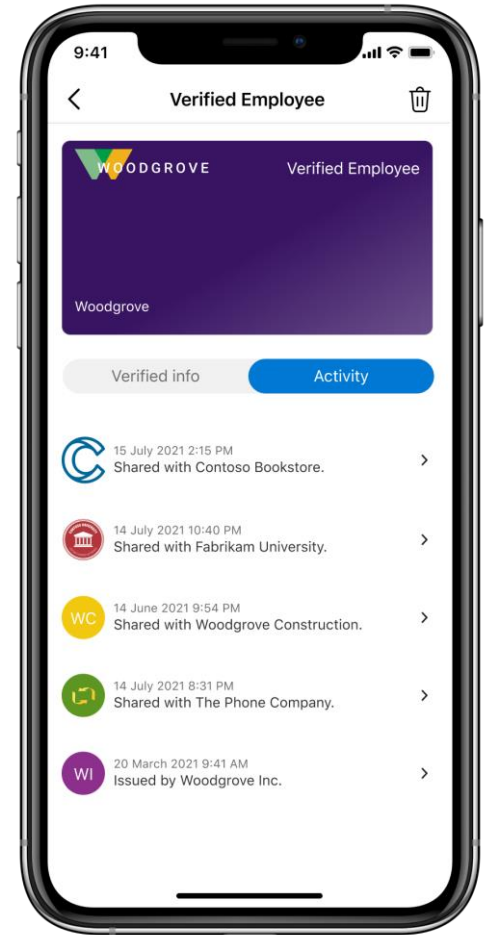
Easy to use and secure



Verifiable

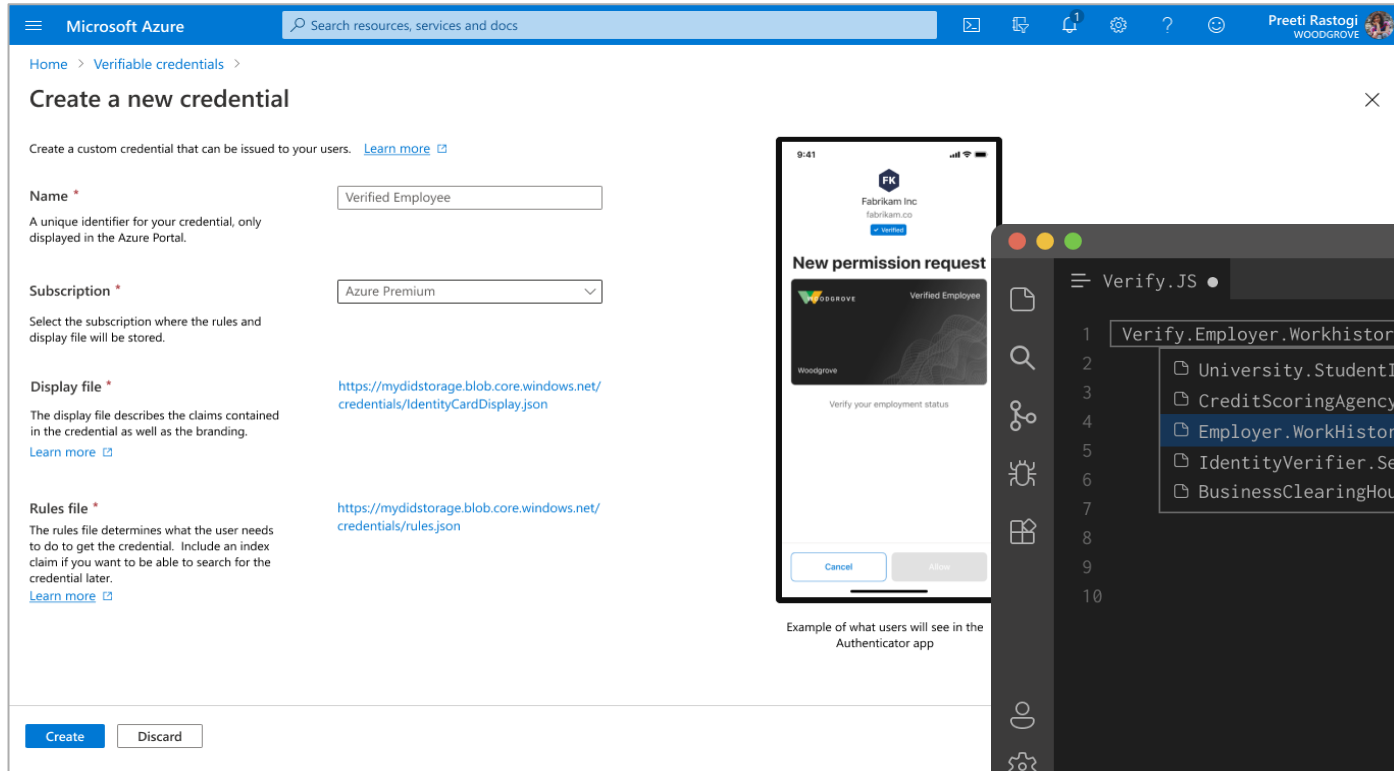


Transparent

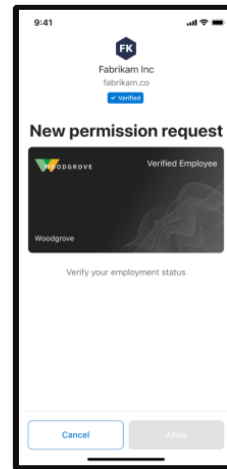


Convenient

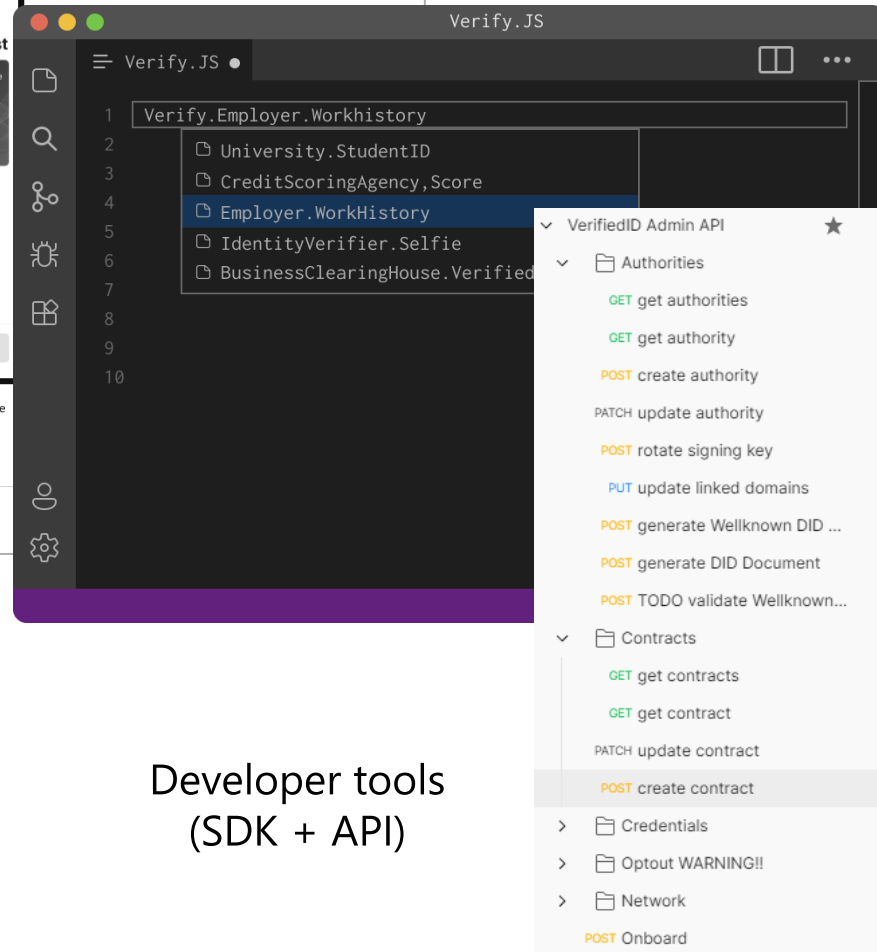
# Decentralized Identity Platform by Microsoft



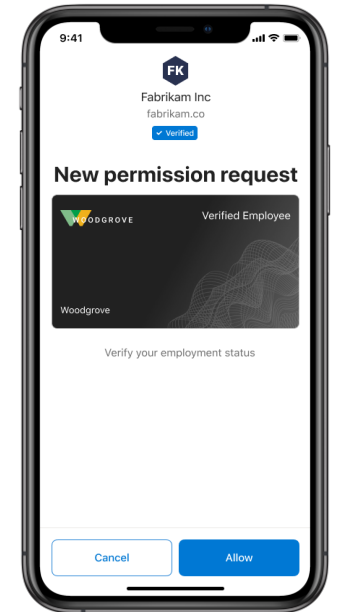
Issuer interface  
(Entra Verified ID)



Example of what users will see in the Authenticator app



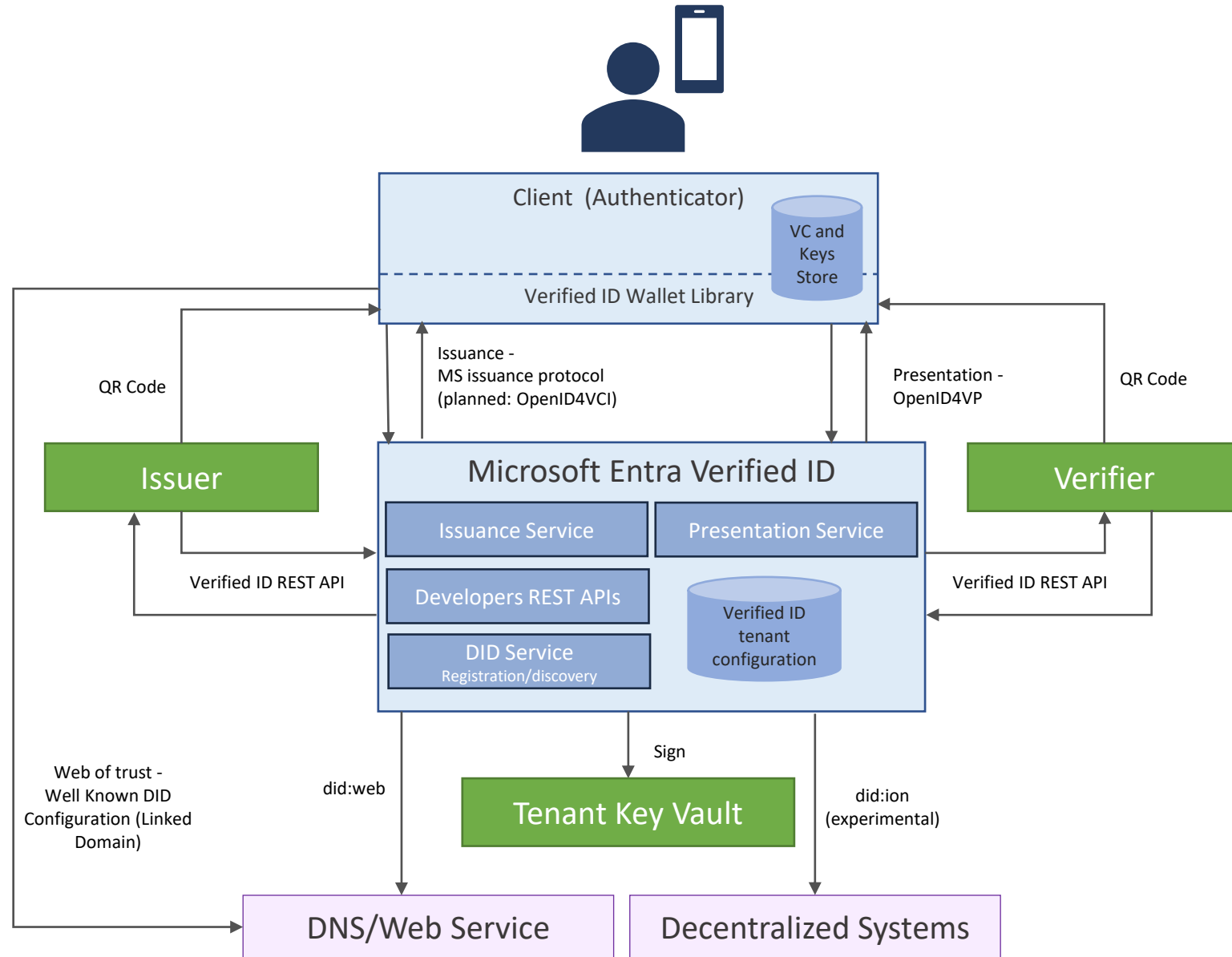
Developer tools  
(SDK + API)



End user wallet  
(Microsoft Authenticator)

# Architecture goals:

1. Decentralized system to request and verify credentials at scale
2. Ensure interoperability as standards and partnerships evolve
3. Simple APIs to ensure consistent interactions that abstract standards and cryptography





## Verified ID

Enable more secure interactions while respecting privacy with an industry-leading global platform.

### 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.

# Ongoing value journey: Worker productivity



**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**

Completes **trainings**, attested to workplace credential for **compliance** and access

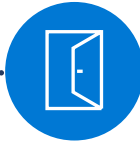
Receives **workplace credential**, enabling access & benefits

Uses verifiable credential to **remotely access** and set up new account

Efficient access to **employee perks** and ongoing life tasks

# Secure access to applications

Quickly verify credentials and get access to sensitive resources that have advanced security requirements



## Sign in

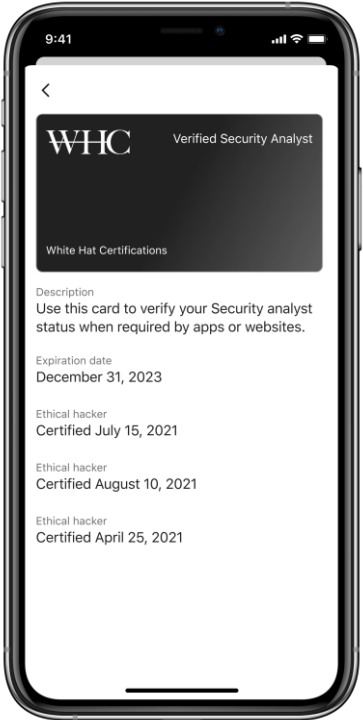
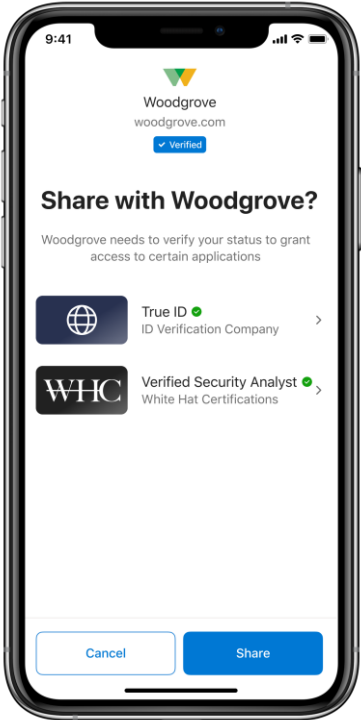
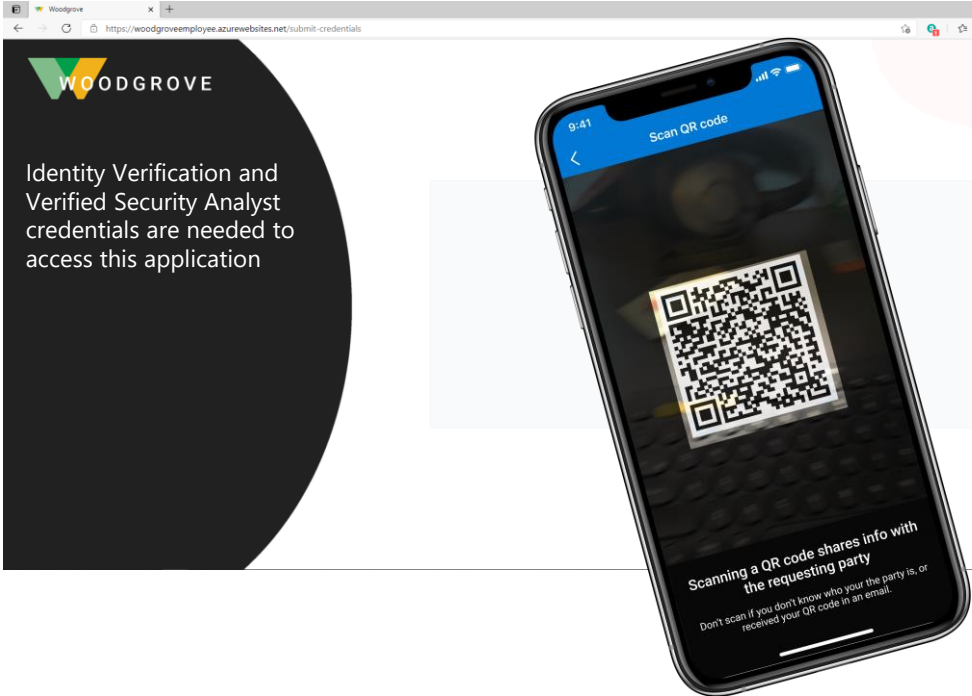
User attempts to sign in to a high-privilege app at Woodgrove

## Presentation

User shares the requested verifiable credentials

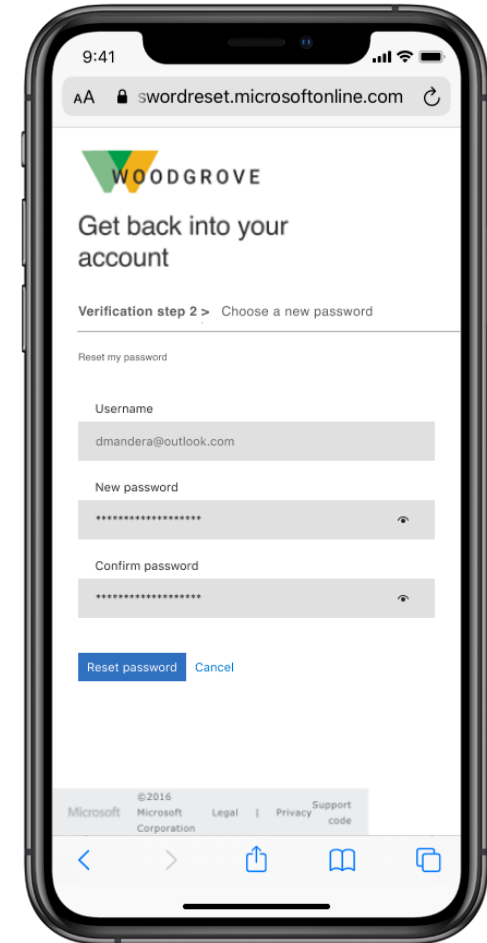
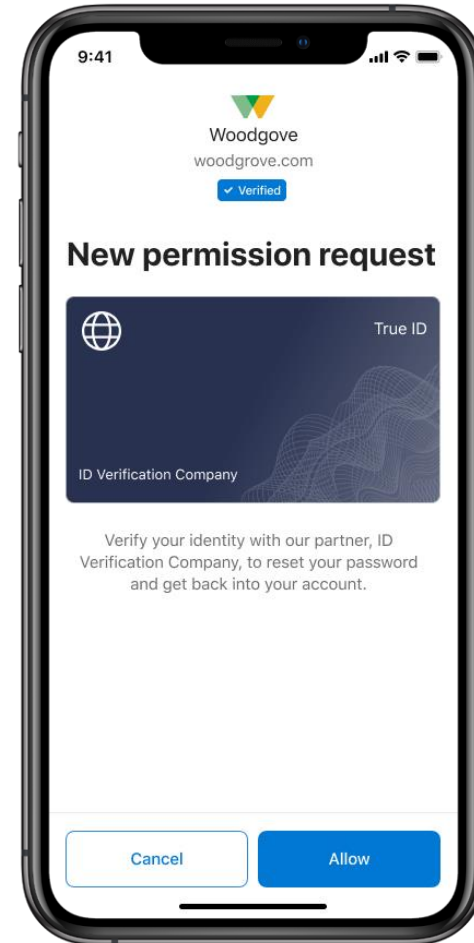
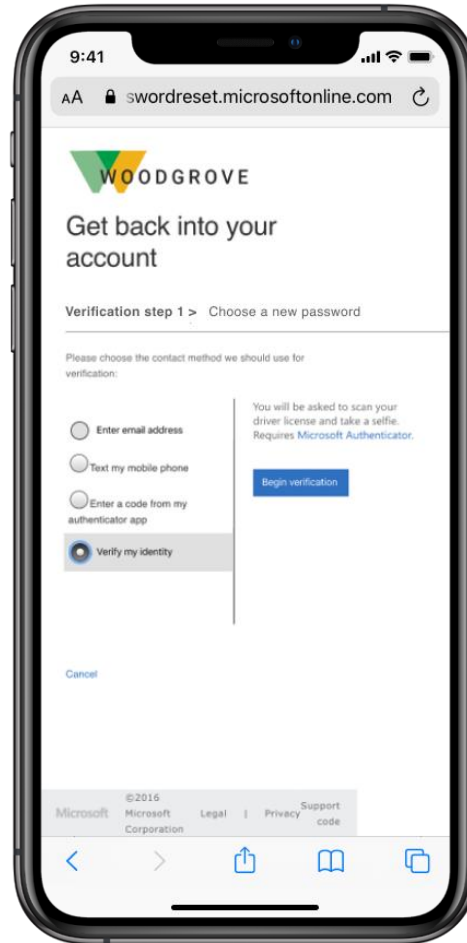
## Detailed view

User confirms which claims are being shared



# Account Recovery

Reduce support phone calls and security questions with a simpler, more secure process to verify identity.



# Trustworthy, faster, cheaper way to verify



## Onboard employees, partners, customers

Trustworthy self-service enrollment and faster onboarding by digitally validating information with industry leading ID verification providers.



## Access to high-value apps and resources

Quickly verify credentials and get access to sensitive resources that have advanced security requirements



## Self-service account recovery

Reduce support phone calls and security questions with a simpler, more secure process to verify identity.



# Customer stories



Keio  
University



National  
Health Service



Government  
of Flanders

and [many more...](#)

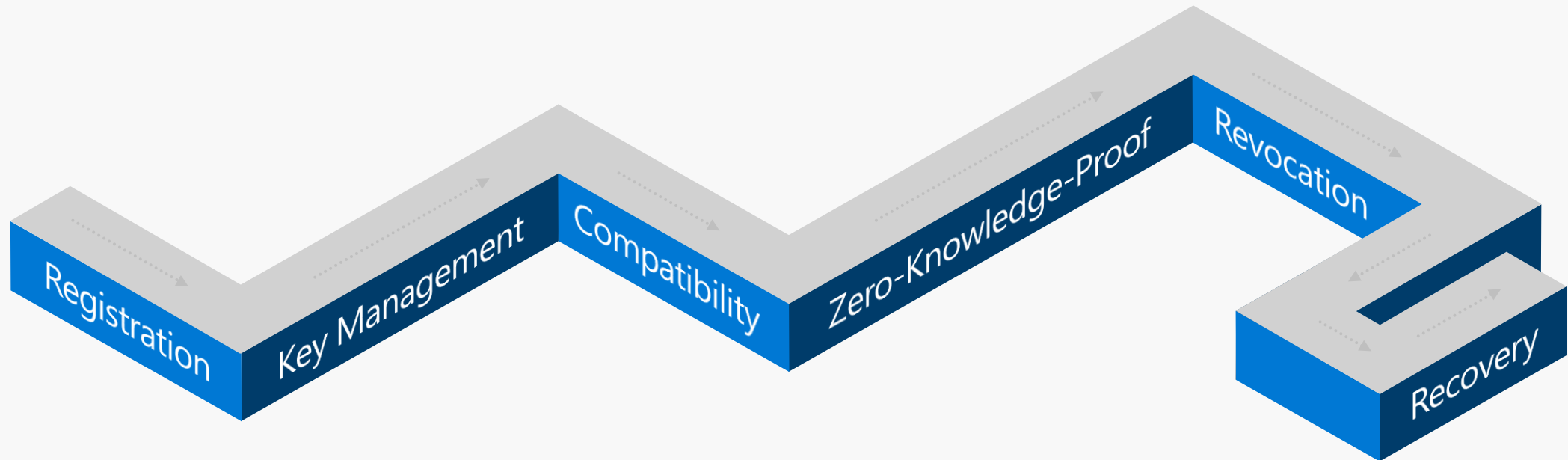
# Next steps

---

# The next 3 steps to making the ecosystem real

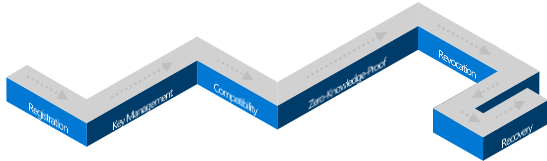
## 1. Ease of use

- ✓ Registration
  - ✓ Key management
  - ✓ Interoperability
- Recovery and revocation
- Selective Disclosure & Zero-knowledge-proof



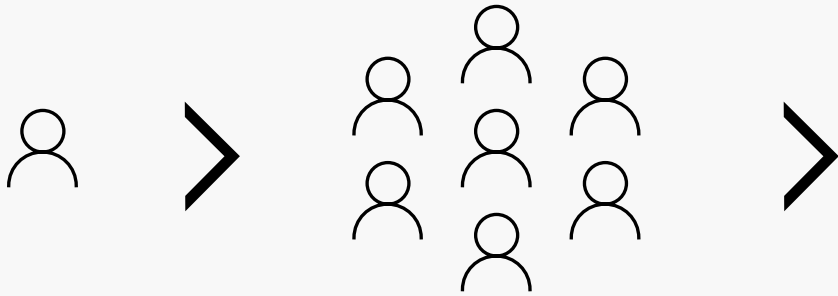
# The next 3 steps to making the ecosystem real

## 1. Ease of use



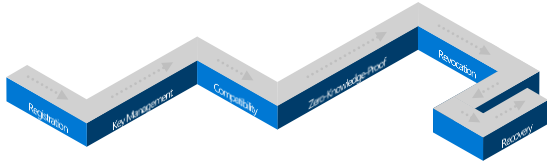
## 2. Performance & Scale

- ✓ DID:Web
- DID:ION (public preview)
- Other methods?



# The next 3 steps to making the ecosystem real

## 1. Ease of use



## 2. Performance & Scale

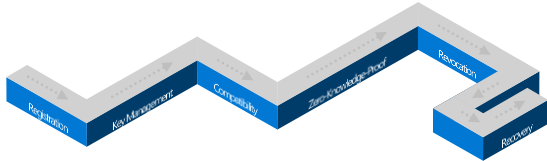


## 3. Join, collaborate, and contribute



# The next 3 steps to making the ecosystem real

## 1. Ease of use



## 2. Performance & Scale



## 3. Join, collaborate, and contribute



Thank you.

# Resources

1. <http://identity.foundation> Industry working group for all things Decentralized ID (DID)
2. <http://aka.ms/didwhitepaper> White paper by Microsoft: approach for DID + Verifiable Credentials
3. <http://aka.ms/didexplained> Quick overview
4. <https://youtu.be/Whc9Im-U0Wg> Overview for developers: scenario walk-through and how-to
5. <http://aka.ms/didfordevs> Developer documentation
6. <http://aka.ms/azuread/did> -> Blogs (including scale and performance and self-owned key recovery)
7. <https://aka.ms/vcinterop> VC Interop profile
8. <https://aka.ms/diddemo> Demo site



<http://aka.ms/vcdetails>



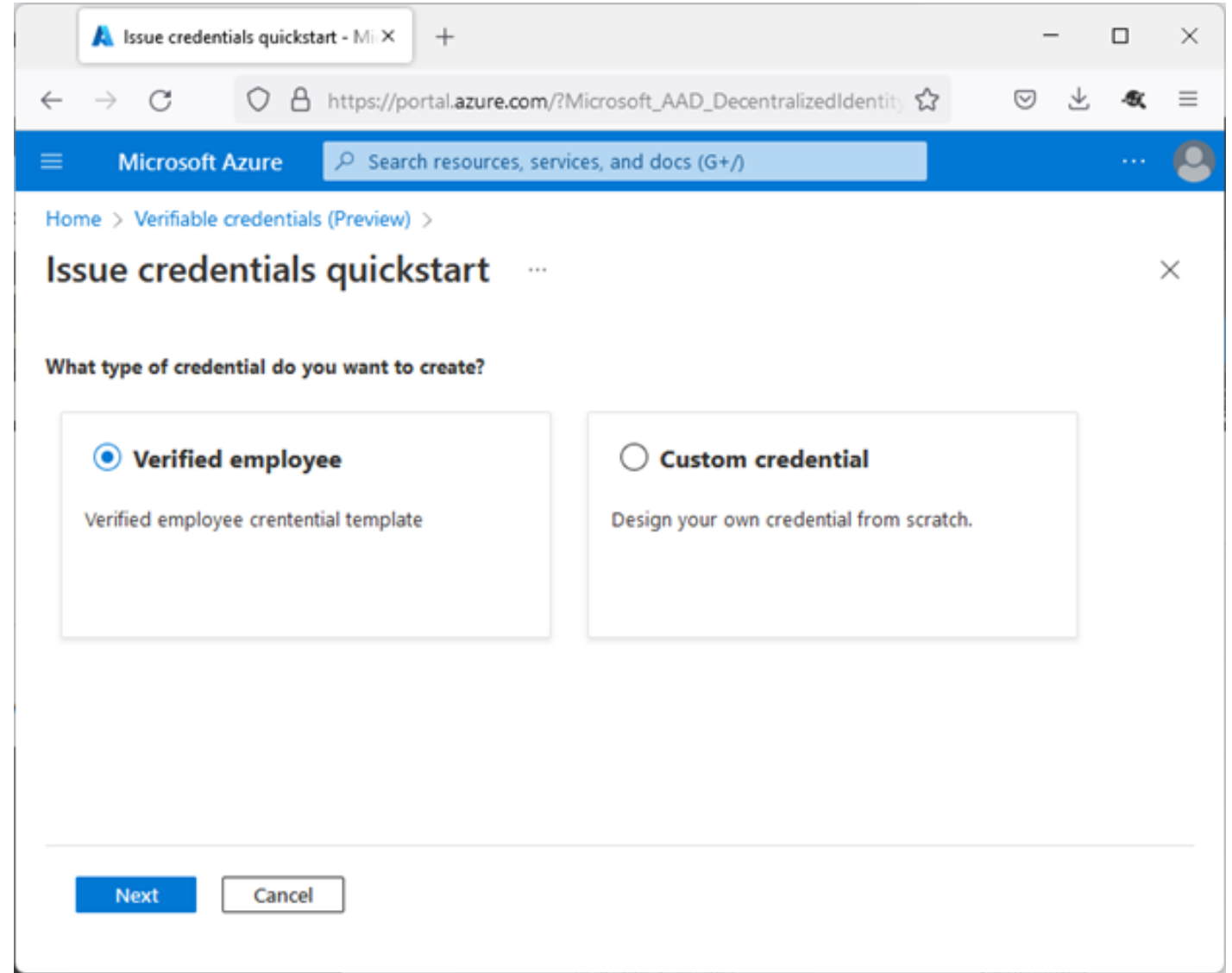
@AzureAD

Thank you



# Quickstart for Directory based claims

Effortlessly create a credential where the claims come from a user profile in the directory of the **Azure AD tenant**



# Quickstart for Custom credentials

When using the Quickstart, just enter all details in the Azure portal and create a custom credential on a single page

The screenshot shows the 'Create a new credential' page in the Azure Portal. The browser address bar shows the URL: `https://portal.azure.com/?Microsoft_AAD_Decimalized`. The page title is 'Create a new credential'. Below the title, there is a 'Got feedback?' link. The main content area is titled 'Create a new credential' and contains the following sections:

- Credential name \***: A unique identifier for your credential, only displayed in the Azure Portal. The input field contains 'VerifiableCredentialExpert'.
- Display file \***: The display file describes the claims contained in the credential as well as the branding. A code editor shows the following JSON:

```
1 {
2   "locale": "en-US",
3   "card": {
4     "title": "Verified Credential Expert",
5     "issuedBy": "Microsoft",
6     "backgroundColor": "#000000",
7     "textColor": "#ffffff",
8     "logo": {
9       "uri": "https://didcustomerplayground.blob.core.w
10      "description": "Verified Credential Expert Logo"
```

Below the code editor, there is a link: [Learn how to create a display file](#).

- Rules file \***: The rules file determines what the user needs to do to get the credentials. Include an index claim if you want to be able to search for the credential later. A code editor shows the following JSON:

```
1 {
2   "attestations": {
3     "idTokens": [
4       {
```

On the right side of the page, there is a mobile app preview showing the 'Add a credential' screen. Below the preview, there is a text box explaining: 'This is what users will see in the Authenticator app. The card branding, title and color come from the display file. The acceptance requirements, such as "sign in to your account" are covered by the rules file.'

# Microsoft Entra Verified ID Network

Search for published credential types and schemas in the Entra Verified ID Network to easily generate a presentation request

Select issuer - Microsoft Azure

https://portal.azure.com/?Microsoft\_AAD\_DecimalizedIdentity\_didQuickStart=true&Microsoft\_AAD\_Dece

Microsoft Azure Search resources, services, and docs (G+)

graphexplorer@cljunga... CLJUNGAADVCS (CLJUNGAAD...

Home > Verifiable credentials (Preview) >

## Setup a verification request

Select issuer(s) Review

Select which issuers you want to accept credentials from. After selecting an issuer, you can specify the credential types you're looking to accept. [Learn more](#)

+ Select issuer </> Add custom issuer

Issuer	Linked domain	Credential type

Select first issuer

### Select issuer

Select an issuer of verifiable credentials from the Azure AD network. The choose which types of credentials to include in verification request.

#### Step 1 - Search/select issuers

Search for and select a verifiable credential issuer. Only issuers with verified domains will be searchable.

https://did.woodgrovedemo.com/ from Woodgrovedemo

Name Woodgrovedemo

Linked domain https://did.woodgrovedemo.com/

#### Step 2 - Select credential type(s)

Select the credential types to present to your user for verification.

- BankofWoodgrovedentity  
givenName, familyName
- VerifiedEmployee  
displayName, givenName, jobTitle, preferredLanguage, surname, mail, revocationId, photo

Add

Previous Review

**Verifying credentials using Microsoft Entra Verified ID Network**

# Jumpstart with partners

## Leading Identity verification partners



## Accelerate adoption with a growing ecosystem of partner solutions



192 Countries

6000 Identification documents

1000's Organizational attributes

Millions Individual ID attributes

Decades

of experience to go from idea to implementation in hours

# Entitlement Management with Verified ID



Verify granular attributes from a wide set of issuers



Reduce approval fatigue



Automatically revoke access when VC is revoked



Better compliance posture

Microsoft Azure Search resources, services and docs

Identity Governance > Create a policy >

## Create a policy

Configure policy | Approval | Requestor information | Lifecycle | Review

Choose which users or applications can request access. By default, admins can always assign users to the access package. You can also designate other users or applications to request access on behalf of the users and applications within the scope of the policy.

Users who can get access

For users not in your directory

Specific connected organizations  
+ Add directories

All configured connected organizations

All users (all connected organizations + any new external users)

Users who can make requests

Admin  
Admin can't be turned off because admins will always be able to assign users to an access package

Self

Manager

Internal Sponsor

External Sponsor

Users to provide Verifiable Credentials

Add

Issuer	Domain	Credential types	Claims
--------	--------	------------------	--------

Previous Next