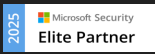




CO-SELLING PLAYBOOK 2025





CO-SELLING PLAYBOOK 2025

VO provides a platform to create, issue, publish, accept, and manage Verifiable Credentials.

Built on Microsoft Azure, VO's solution allows you to take full advantage of Microsoft Entra Verified ID without costly custom development or the need to hire a third party.

With no bespoke code required, our platform can be easily set-up and managed in-house.

VO's turn-key solution is feature rich, integration focused, configurable in just minutes, and provides all the best features of Verified ID at the click of a button.

"Verifiable Credentials are the most promising antidote to synthetic identity fraud — especially as deepfake generation becomes democratized by AI."

— Avivah Litan, VP and Distinguished Analyst at Gartner

Table of Contents

- 1 Microsoft and VO: Stronger Together
- 2 Featured Use Case: Workforce
- 3 Featured Use Case: Customers

MICROSOFT AND VO: STRONGER TOGETHER

When Microsoft and VO sellers work together, combining VO's industry leading identity solution with Microsoft's enterprise platforms, co-sell revenue increases and accelerates.

All offerings are licensed on a software as a service annual subscription or consumption basis and are deployed via the Azure marketplace.

The VO solution addresses needs across all industries, with a focus on:

- Financial Services
- Government
- Education
- Healthcare
- Transport & Logistics
- Retail

VO Contacts

Richard Mallam

CEO

richard@verifiedorchestration.com

Ivan Niccolai

Partner and Sales Engineering Lead

ivan@verifiedorchestration.com

Microsoft Contact

Ivette Morales

Senior Product Manager

Customer Experience Engineering (CxE) | Security Division

ivmoral@microsoft.com

CUSTOMER COMMENTS TO LISTEN FOR



We need to improve our identity risk posture, but every option we've evaluated so far simply introduces risk and complexity elsewhere.



We tried Microsoft Verified ID but it was too complex to use and required too much customisation to fit into our existing enterprise.



We have an issue with onboarding across our internal and contractor workforce. We want to automate onboarding and streamline our identity systems.



We're looking at moving some of our users away from Entra to Okta or Ping, because they say they can implement a better user experience with MFA or biometric validation.

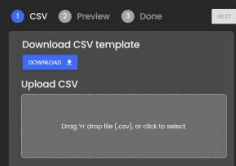
FREQUENTLY ASKED QUESTIONS

Question	Answer
Will this technology work with my existing security tech stack?	Yes. VO is built on Azure and Microsoft Entra ID, and our OIDC capability natively integrates to all major IdPs including Okta and Ping Identity.
Can I easily issue and manage credentials across hundreds or thousands of workers or customers?	Yes. The solution is RBAC enabled and supports bulk issuance. You can onboard thousands of workers or customers in seconds.
Can I choose when to add in a biometric step like Face Check?	Yes. We natively support the configuration of biometric verification for specific transactions or events.
Will VO's Verifiable Credentials work outside of the Microsoft Authenticator app?	Yes. Custom wallets can be developed to meet your organisation's requirements.
What other tools does VO integrate with?	Power BI, Power Platform, Dynamics, any business application that supports OIDC.

15 MINUTES TO ENTERPRISE GRADE VERIFIED ID SUCCESS

Extending and complimenting Microsoft Verified ID; rapidly delivering client value.

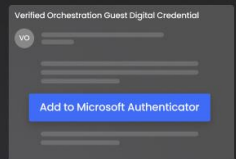
Issue thousands of credentials



STEP 1

Prepare

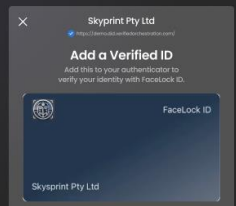
Use the VO Composer to upload a CSV file containing thousands of credential details.



STEP 2

Offer

The Composer will send issuance offers to every contact, with multiple options for identity verification.

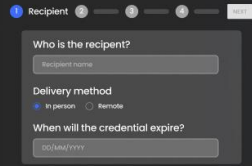


STEP 3

Issue

The VO Concierge will finalise the credential issuance for each recipient, capturing selfies as required and securely completing the issuance.

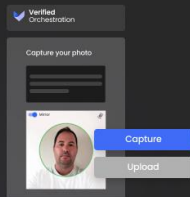
Issue a biometrically bound credential



STEP 1

Offer

Use the VO Composer to offer the credential to a verified contact.



STEP 2

Capture

Your end-user will use our Concierge to verify themselves and capture their selfie.

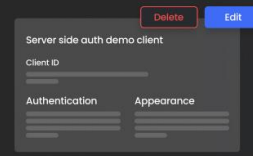


STEP 3

Issue

The VO Concierge will finalise the credential issuance, including the selfie capture as a signed image in the credential.

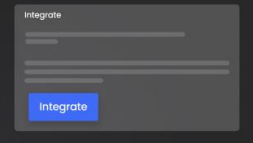
Use a credential for MFA



STEP 1

Configure

Use the VO Composer to configure a new OIDC client

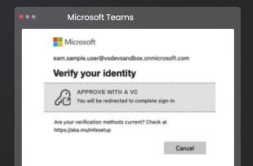


STEP 2

Integrate

Configure your IdP to use our OIDC provider as an authentication factor.

Note: Dependent on IdP support.

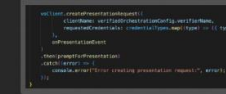


STEP 3

Protect

From the protected application, the user will be challenged for a credential as an additional authentication factor.

Add a presentation request to your NodeJS app



STEP 1

Build

Use our Javascript library to simplify your development. Incorporate a presentation request in less than 10 lines of code.



STEP 2

Issue

Use our Composer to issue a credential to a user.

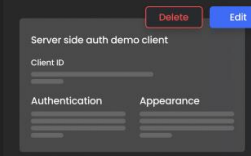


STEP 3

Accept

From your NodeJS app, render the presentation request, capture presentation events and use credential data in your app.

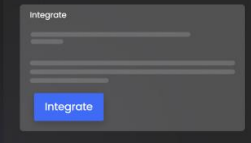
Move from passwords in your current IdP



STEP 1

Configure

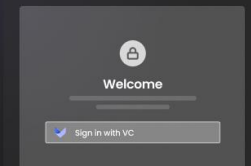
Use the VO Composer to configure a new OIDC client



STEP 2

Integrate

Configure your IdP to use our OIDC provider as your primary authentication factor.



STEP 3

Authenticate

From the protected application, the user will be challenged for a credential as an additional authentication factor.

Where supported.



WORKFORCE IDENTITY

Solutions for:



Frontline Workers



Contractors



Office workers



Sites

Relevant industries:

Financial
Services

Construction



Retail



Higher Ed



Govt

WITH VO YOU CAN:

- ✓ Onboard or offboard workers in 15 seconds or less
- ✓ Eliminate rogue employee onboarding
- ✓ Give workers access to jobs, digital resources, and physical sites without the need for guest accounts
- ✓ Use a secure credential to enforce compliance requirements
- ✓ Use a secure credential to prove training, certifications and/or skills
- ✓ Provide a familiar, easy to use security experience
- ✓ Reduce cyber risk by eliminating centralised authentication credential stores



Customer Pain Point



VO Solution

Risk of rogue employee onboarding due to impersonation or presentation of fake identity credentials.

Tamper-proof Verifiable Credential issuance including an employee biometric captured during the interview.

Poor user experience for end users with multiple credentials, resulting in reduced productivity.

Simplify the experience for end users – one credential to manage all their access, no passwords to remember.

Passwords and OTPs are vulnerable to phishing and impersonation.

Unphishable technology that isn't vulnerable to impersonation.

Workers are sharing credentials and MFA codes, leading to audit and compliance issues.

Easily enable biometric checks for authentication and authorisation events.

System is expensive to manage and maintain, requires complex skills.

Simplified administration and lower cost of ownership.

Storing Personal Information increases the risk of data breaches.

Limit the storage of PI and significantly reduce the risk of a data breach.

Service-desk tickets create a burden on internal IT and back-office teams.

Allow workers to self-serve access and identity ITSM requests.

TOP 3 SOLUTION BENEFITS



Comprehensive enterprise solution for Verifiable Credentials



Configuration over custom development with friendly UIs for administrators and end users










Pluggable architecture enabling the use of Verifiable Credentials with existing authentication investments

Questions to Ask

- 1 Have you experienced, or are you worried about, the cost of impersonation, fraud or cyber incidents involving the misuse or theft of login credentials?
- 2 Have you tried to eliminate or reduce the use of passwords which has resulted in increased helpdesk costs?
- 3 What are the manual steps involved in verification processes, and how much time and resources do they typically consume?
- 4 How do you currently verify credentials and attributes such as educational qualifications, professional licenses, or certifications?
- 5 Are you thinking of implementing Microsoft Verified ID but want to avoid the costs and complexities of custom development?

HIGH VALUE USE CASES

						
Streamlined and secure onboarding for employees	Transient and mobile worker access	Step-up authentication for administrators	Verified helpdesk for employees and contractors	Fine-grained authorization with tamper-proof credentials	Continuous and verifiable skills and training management	Self-service account recovery
VALUE LEVER	VALUE LEVER	VALUE LEVER	VALUE LEVER	VALUE LEVER	VALUE LEVER	VALUE LEVER
Cost Risk	Cost Risk	Risk	Cost Risk	Risk	Cost	Cost Risk
SIZE OF PRIZE	SIZE OF PRIZE	SIZE OF PRIZE	SIZE OF PRIZE	SIZE OF PRIZE	SIZE OF PRIZE	SIZE OF PRIZE
● ● ● ●	● ● ● ●	● ● ●	● ● ● ●	● ● ●	● ● ●	● ● ●

CUSTOMER IDENTITY

Solutions for:



Consumers



Citizens



Members



Students

Relevant industries:

Financial
Services

Health



Telco



Higher Ed

WITH VO YOU CAN:

- ✓ Allow your customers to activate account security in 15 seconds or less
- ✓ Give customers easy access to their account and require additional biometric authentication for high-risk actions
- ✓ Validate account ownership without ID checking or out of wallet questions
- ✓ Offer a seamless experience across mobile and desktop
- ✓ Securely verify customer identity while on the phone and allow customers to verify agents



Customer Pain Point



VO Solution

Disjointed and unfriendly user onboarding experience, resulting in dropouts during sign-up and checkout transactions.

Simplify the experience for end users; onboard quickly and easily without having to remember complex passwords.

Passwords and OTPs are vulnerable to phishing and impersonation.

Unphishable technology that isn't vulnerable to impersonation.

Out of wallet identity checks are vulnerable to impersonation, via data available from breaches.

Easily enable biometric checks for authentication and authorisation events, reducing fraud risk.

Storing Personal Information increases the risk of data breaches.

Limit the storage of PI and significantly reduce the risk of a data breach.

Consumers are wary of inbound calls from call centers due to fraud attempts.

Enable two-way identity validation for call center workers and consumers, reducing fraud and improving trust.

TOP 3 SOLUTION BENEFITS



Easily issue and manage Verifiable
Credentials at scale



Reduce the cost of fraud by providing a better
customer experience





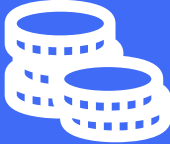



Significantly reduce your identity attack surface
by eliminating centralized customer login stores

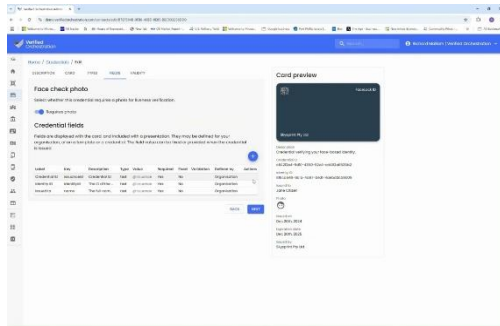
Questions to Ask

- 1 What are your costs of fraud that involve impersonation attacks?
- 2 Have you experienced or are you worried about a data breach involving customer PII?
- 3 Are you looking to implement additional biometric controls but are concerned about impacting user experience?

HIGH VALUE USE CASES

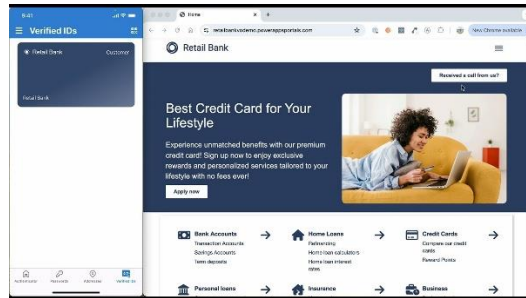
					
Protect high-value transactions from cybercrime	Enhanced reputation via phishing-resistant security	Implement privacy-preserving technology and reduce PII data	Enable frictionless sign-up	Share entitlements across partners to drive new revenue streams	Personalized loyalty programs
VALUE LEVER	VALUE LEVER	VALUE LEVER	VALUE LEVER	VALUE LEVER	VALUE LEVER
Risk Cost	Risk	Risk	Revenue	Revenue	Revenue
SIZE OF PRIZE	SIZE OF PRIZE	SIZE OF PRIZE	SIZE OF PRIZE	SIZE OF PRIZE	SIZE OF PRIZE
● ● ● ● ●	● ● ● ● ●	● ● ● ● ●	● ● ●	● ● ●	● ● ●

ONLINE VIDEO RESOURCES



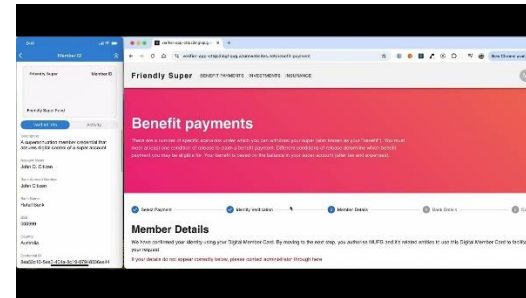
Welcome to the VO Composer

A quick overview of the composer where you manage credentials.



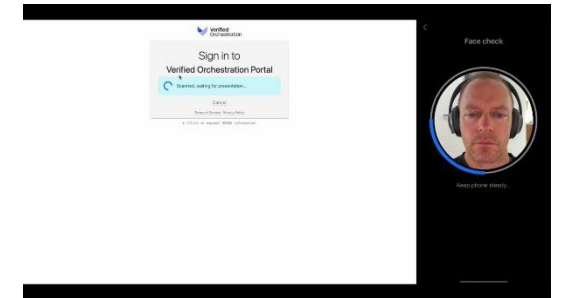
Agent and help desk verification

See how a digital customer ID can be used to verify the organisation, the calling agent and the customer.



KYC integration for straight through processing

See how a Verifiable Credential including sensitive personal information (bank account details) can authorise a benefits payment from a superannuation account.

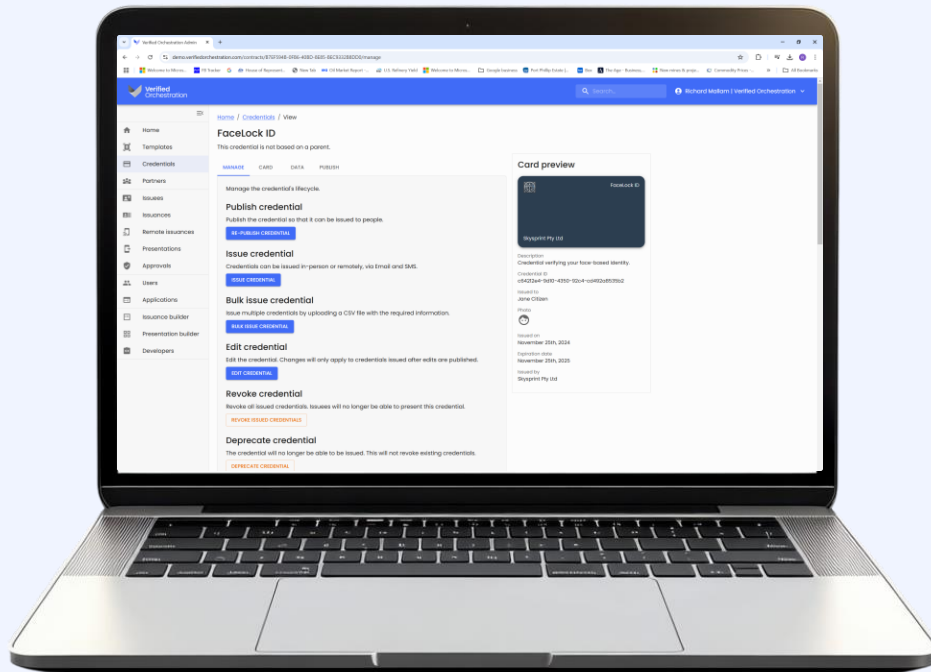


Biometric Auth

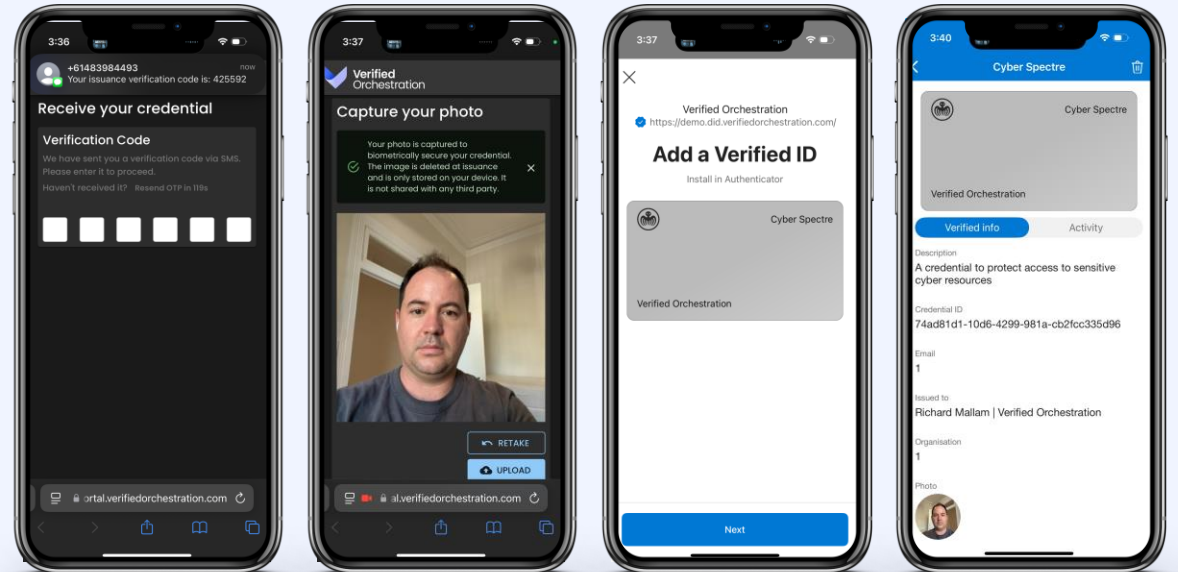
Demonstrates our ability to biometrically secure authentication to an application, including returning a confidence level on the biometric matching.

OUR PRODUCT

Enterprise grade technology



With intuitive user experiences





Thank You

VO Contacts

Richard Mallam

CEO

richard@verifiedorchestration.com

Ivan Niccolai

Partner and Sales Engineering Lead

ivan@verifiedorchestration.com

Microsoft Contact

Ivette Morales

Senior Product Manager

Customer Experience Engineering (CxE) | Security Division

ivmoral@microsoft.com