

Microsoft Entra Verified ID

Trustworthy interactions for a digital world





Get to know Verified ID

Microsoft Entra Verified ID enables trustworthy, secure, and efficient digital interactions between people and organizations.

Learn how companies use Verified ID to increase productivity, save time and money, and reduce the risk of identity-based attacks.



Businesses struggle with keeping their information secure, managing access to important applications and resources, and quickly onboarding new employees in a hybrid work environment.

Microsoft Entra Verified ID enables organizations to customize identity verification solutions to address their specific needs. Using Verified ID, organizations can provide quick, transparent, and more secure verifications for their end-users and employees while reducing costs, risks, and business inefficiencies.

Reduce fraud



Verified ID can help determine if the right person is attempting to access an account, improving a company's security by limiting impersonation threats.

Prevalent impersonation threats

There are over 4,000 password attacks per second, up from 1,287 per second in 2022.¹ Making sure individual accounts are secure is a key part of any organization's cybersecurity infrastructure.

In Japan, Skype saw an increase in fraudulent use of Skype numbers, which endangered customer accounts and data and increased regulatory risk.

Safeguarding customer identities

To directly fight these threats, Skype partnered with LexisNexis to implement Verified ID into the customer account creation process.

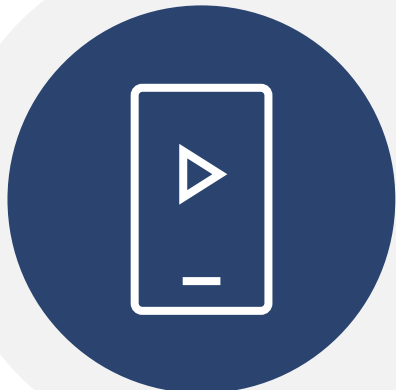
After users purchased a Skype number, they were asked to provide identifying details such as their name, phone number, email, date of birth, a government-issued ID that would confirm their identifying information, and a selfie.

Using this information, LexisNexis could verify the user's identity in seconds and activate their Skype number.

Impact

Since implementing Verified ID, **fraudulent use of Skype numbers in Japan has decreased by 90%.**

Due to the success of Skype's Verified ID implementation, the company is looking into additional scenarios in which they could use Verified ID to further bolster security.



Since implementing Verified ID, fraudulent use of Skype numbers in Japan has decreased by **90%.**

Grant access quickly & securely



Verified ID provides fast and secure verifications so staff can access the systems they need and can quickly respond in time-sensitive or delicate situations.

Delays in a complex ecosystem

The National Health Service (NHS) in the United Kingdom has over 200 separate hospital organizations and many skilled healthcare providers that move between these groups to provide care for patients.

Many of the hospital organizations do not share the same systems, documentation, or databases, and moving staff from one organization to another requires multiple days of administrative processing.

Crucial, safe, & rapid verifications

The NHS wanted to find a way to move staff between sites more efficiently. Using Verified ID, the NHS gave its medical staff the ability to own and control their healthcare

verifications in their digital wallets instead of waiting several days on administrative checks before providing care.

NHS staff can present a verifiable credential from their phone to securely share their skills and experience and begin providing care more rapidly.

Impact

Rather than waiting days for administrative work to process, NHS medical staff now can use Verified ID to **prove their medical certifications in a matter of minutes.**

Verified ID gives NHS staff more flexibility, saves administration time and money, and most importantly, can improve outcomes for patients by getting the right healthcare workers to the right patients in a much quicker fashion.



Rather than waiting days for administrative work to process, NHS medical staff can now use Verified ID to prove their medical certifications in a **matter of minutes.**

Streamline onboarding and credential verification

Verified ID can help create efficient remote onboarding processes that decrease the timeline for new hires and contractors to start their work.

Repetitive administration tasks

Agilus Work Solutions, a Canadian recruitment firm that places highly skilled workers, partnered with Credivera, a workforce digital identity platform provider, to get their clients on the job more quickly with Verified ID.

For each jobseeker, Agilus had to manually verify their credentials to ensure the candidate fit the job requirements. Jobseekers often have 10 or more credentials to verify, each requiring individual emails or phone calls before validation. Agilus manages thousands of active jobseekers, creating a heavy volume of repetitive communications.

Automate credential verification

To minimize the waiting period, Agilus implemented a Verified ID-based system

that automatically asks jobseekers to submit their credentials to start the verification process, which Agilus can track in real time. After verification, the jobseekers are issued verifiable credentials that they own and control in their digital wallets.

Impact

Thanks to Verified ID, **Agilus saves about 45 minutes per candidate onboarded, significantly decreasing the administrative workload of manually processing verifications for thousands of candidates.**

The candidate onboarding timeline that could take three to four weeks in some cases has been reduced.

Thanks to time savings enabled by Verified ID, Agilus employees can spend more time focused on personal interactions with clients to help them achieve better outcomes and better fitting jobs.



Agilus saves about **45 minutes per candidate onboarded**, significantly decreasing the administrative workload of manually processing verifications for thousands of candidates.

Automate the helpdesk



Verified ID helps streamline and secure helpdesk functions, decreasing the risk of impersonation attacks and eliminating the need to call the helpdesk for password resets and account recovery, which accounts for **20-50% of helpdesk calls**.²

Streamline & secure account recovery

BEMO, an SMB-focused cyber security and IT solution provider, integrated Verified ID in its helpdesk offering to provide an easier and more secure experience for the 600+ companies it manages.

BEMO's Verified ID-powered helpdesk challenges C-level employees and IT administrators to present a verifiable credential from their employer to gain access to the helpdesk.

After the credential is accepted, the caller completes a Face Check to verify their identity.

Upon gaining entry, users can self-select which helpdesk function they need from options such as password reset, temporary access pass, multi-factor authentication (MFA) onboarding, and account updates.

Since developing their Verified ID-powered helpdesk, BEMO already has over 100 of its clients successfully using Verified ID today.

Impact

BEMO's new helpdesk offering **greatly decreases the risk of identity fraud for the employees who have access to the most sensitive information and resources** in the companies using this solution.

BEMO is improving its digital security with Verified ID by protecting the most sensitive accounts from impersonation.



Verified ID eliminates the need to call the help desk for password resets and account recovery, which account for **20-50% of help desk calls**.²

Verified ID in practice

Microsoft Entra Verified ID is a managed verifiable credential service, based on open standards, where organizations can build unique user-owned digital identity scenarios. Confidently issue and attest to identity claims, credentials, and certifications designed for trustworthy, secure, and efficient interactions between people and organizations. To protect individual privacy and data, users own and control their verifiable credentials and can choose to present them when asked.

How Verified ID Works

Using Verified ID begins with an organization who issues a digitally signed verifiable credential to an individual who stores and manages the credential in a digital wallet on their personal device.

An issuer could be a government agency, an employer, a university, or any organization that can confirm information that individuals give about their identity.

After receiving a verifiable credential from an issuer, the individual can present their credential to a company or organization that wants to verify something about their identity.

Open Standards

Verified ID is an inclusive product that can work with identity verification systems that other businesses or developers may create in the future.

With members of the Decentralized Identity Foundation (DIF), the W3C Credentials Community Group, and the wider identity community, Microsoft continually identifies, develops, and implements critical standards which make Verified ID compatible with other identity verification services.

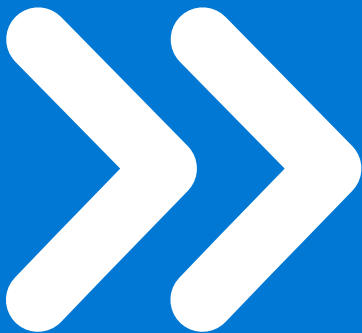


Get started with Microsoft Entra Verified ID

The power of verifiable credentials is at your fingerprints.
Unlock user-owned identity scenarios for your
organization today.

Get started today

[Learn how to configure your tenant for Verified ID](#)



Find an implementation partner

[Visit the Security partner portal](#)

Chat with a representative

Call 1-800-642-7676 to learn how to get started
with **Microsoft Entra**

Learn more about Microsoft Entra Verified ID

[Explore the website](#)

[Read the Verified ID and Face Check blog](#)

¹ Microsoft Security Blog - [Microsoft Inspire: Prepare for the future of security with AI](#)

² InfoSecurity Group, [Password Management: Getting Down to Business](#)