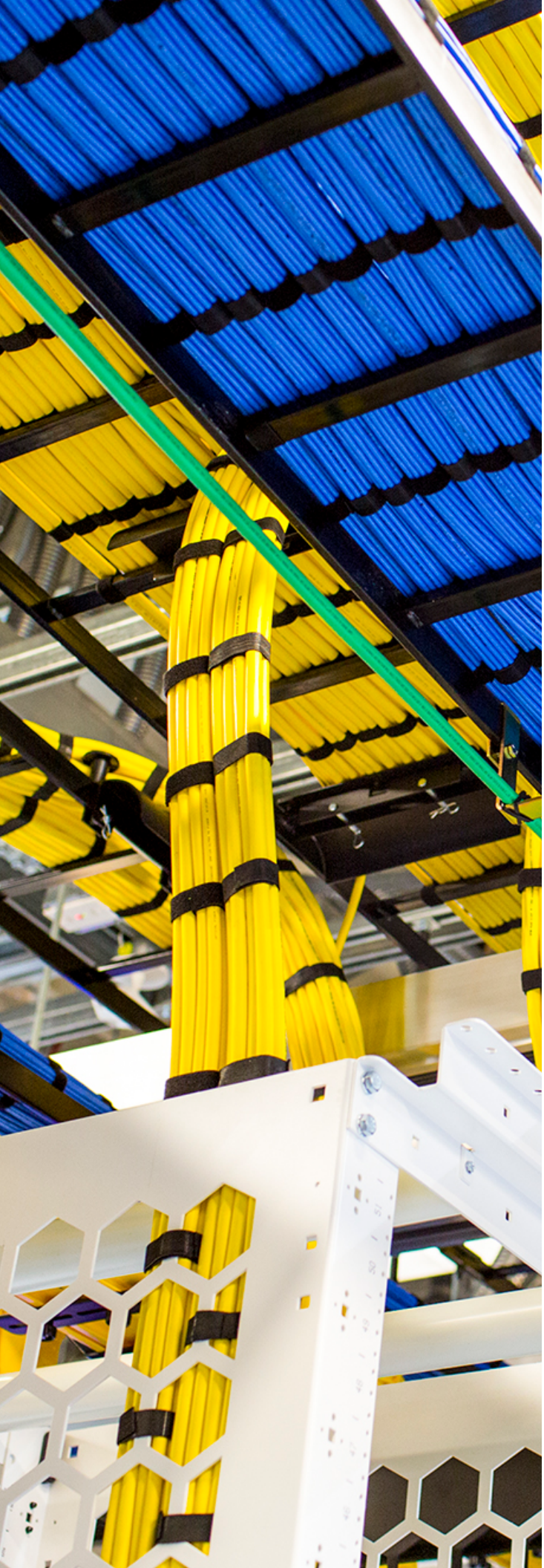
Microsoft Security

Decentralized identity and verifiable credentials

Ownership, control, and trust for a digital world



Executive summary

With our world becoming more connected, how can people take control of their digital identities?

Everyone should have the right to a self-owned digital identity. This identity should seamlessly integrate into each person's life, preserving their privacy while giving them complete control over how their identity data is accessed and used. These identities should form a path toward digital inclusion, allowing everyone to benefit from a new digital ecosystem.

To help build this path, Microsoft is collaborating with the members of the Decentralized Identity Foundation (DIF), the W3C Credentials Community Group, and other groups (see our documentation for more information) to identify and develop critical standards. Meanwhile, Microsoft is building simple customer experiences into our identity solutions to ease and accelerate adoption of the new self-owned digital identity based on the new open standards.

This white paper covers the challenges for individuals and organizations in validating digital identities—and how interoperable and standards-based decentralized identity solutions can help.

The landscape of digital identity

Digital transformation is changing our lives in unprecedented ways—necessitating new trust fabrics for digital identities.

The landscape of digital identity is growing at an exponential rate due to the digitization of nearly every service or interaction imaginable. This proliferation of digital identities is creating impacts at both the individual and organizational level. People are struggling to keep track of how they're sharing their personal data across the various digital platforms they use, while organizations must secure massive amounts of customer data accumulated from these identities.

Today, there's no simple digital equivalent to a universally accepted identity like a state-issued driver's license or social security card. Consider what makes a traditional driver's license a good form of identification. You can present your driver's license in a wide variety of interactions—like passing through airport security, verifying your identity with an employer, or opening a bank account. Not only do recognizable security features make your license trustworthy and easy to verify, but you also control whom you share it with and when. And a license is inherently decentralized; since you can carry it with you, no central service is required to present it on your behalf.

Until now, no digital identity could offer similar benefits. Whether for a popular social platform or a work account, a digital identity has always been controlled by the organization that issued it. As the digital sphere takes a foothold in every aspect of our lives, this needs to evolve.

The global digital identity solution market is projected to grow from **23.3 billion USD in 2020** to **49.5 billion USD in 2026**. The rapid market growth is driven by increasing instances of **identity fraud**, **data breaches**, and new **government regulations**.[1]

Why a decentralized approach is the future

It's clear we need solutions that solve tomorrow's problems today.

People use their digital identities at work, at home, and across every app, service, and device they engage with—when purchasing tickets for an event, checking into a hotel, or ordering lunch. Yet currently their identity and digital interactions are owned and controlled by other parties, some of which users may not even be aware of.

At the same time, there's a rising need for decentralized identity systems across industries. Organizations are adopting multi-cloud strategies, cyberattacks have evolved and become more complex, and ubiquitous decentralized computing is becoming an adopted practice.

Moving forward, modern identity solutions need to fit seamlessly into the flow of daily life while being secure, sustainable, and reliable.

- **Individuals** deserve the opportunity to know that their vital information is safe and within their control while having the ability to recover and self-service their accounts quickly, efficiently, and with minimal effort.
- **Organizations** need better means of verifying identity for fast, remote onboarding procedures to keep pace in a hybrid world.
- **Temporary workers and contractors** need identity solutions that provide access to high-value, mission-critical applications within minutes.

A decentralized approach delivers on these needs by bringing an individual's digital identities together into a system that they own, while making digital identities portable in a way that's trusted and secure.

By 2025, an estimated 70 percent of the workforce will be working remotely at least five days a month. Organizations and individuals require identity solutions that support rather than inhibit this new work model.[2]

By 2030, digital identities will be user-centric, convenient to use, and regulated by a few economic superpowers.[3]

Five guiding principles for a decentralized identity system

The following guiding principles are key to realizing the promise of a decentralized identity system.

1. **Secure, reliable, and trustworthy.**
   A person's digital identity shouldn't be easy to hack or impersonate. A user should always be able to access, use, and securely recover their digital identity, plus view a detailed log of every time they've used their digital identity, whom they used it with, and what it was used for.

2. **Privacy protected and in the user's control.**
   Users shouldn't be tracked across unrelated services without their consent and they should be able to delete all aspects of their digital identity—including any associated data and log files—from wherever they choose to store them.

3. **Inclusive, fair, and easy to use.**
   A user's digital identity must be usable, available, and accessible regardless of race, ethnicity, abilities, gender, gender identity, sexual orientation, national origin, socio-economic status, or political status.

4. **Supervisable.**
   A user should be able to designate which family or friends can access their digital identity, if needed. In addition, parents or custodians should have oversight and control over digital identity solutions used by their children in a classroom setting.

5. **Environmentally responsible.**
   Creating and using a digital identity should be ecologically sustainable and not cause long-term environmental harm.

To learn more, read Microsoft's five guiding principles for decentralized identities.

How a decentralized system works

A decentralized identity is rooted in a Trust System, which is an underlying network based on either blockchain or non-blockchain technology protocols. A blockchain-based system, such as the Identity Overlay Network (ION), establishes trust through a linear progression maintained and updated by many independent nodes. The progression comprises a digital ledger of transactions duplicated and distributed across an entire network of computers, which collaborate based on a rule set established by protocols. In contrast, a non-blockchain system such as DID:Web establishes trust based on a web domain's existing reputation.

Regardless of the protocol, a Trust System is always available to you—no matter where you are or when you need access.

What supports the Trust System's functionality are two essential components: **decentralized identifiers** and **verifiable credentials**. Decentralized identifiers are IDs that users create, own, and control independently of any organization or government. A verifiable credential is attested information about a subject.

Together, decentralized identifiers and verifiable credentials comprise a new digital identity that enables trust for users and protects their privacy across organizational boundaries. With their new digital identity, an individual can take ownership and control of their credentials, presenting these to websites, apps, and organizations to confirm their identity.

To understand decentralized identifiers and verifiable credentials better, let's dig deeper into each of these terms.

Understanding decentralized identifiers

To understand decentralized identifiers (DIDs), it helps to compare them with current digital identifiers—notably, email addresses and social network IDs. While these human-friendly aliases give users a way to collaborate online, they weren't designed to serve as comprehensive digital identifiers and don't offer users enough protection or control. In contrast, DIDs are user-generated, globally unique, and verifiable across any platform—allowing users to control their data.

Many people have multiple emails and IDs that they use to make online purchases, sign up for streaming services, post on social media, or engage in other collaboration scenarios. These aliases can be challenging to manage across various services and for data access across many scenarios beyond collaboration. Plus, access to these IDs can be removed by the email provider, social network provider, or other external parties—taking the control out of the user's hands.

DIDs are different. These identifiers possess unique characteristics, a greater assurance of immutability, censorship resistance, and tamper evasiveness. Rooted in Trust Systems like ION or DID:Web, DIDs prevent single points of failure and promote enhanced security. These are critical attributes for any ID system intended to provide self-ownership and user control. If a user chooses, they can delete all data associated with their decentralized identity and eliminate their digital presence. A DID provides users with the ability to share what data they choose to, whom they want to share it with, and who can access their data.

However, in a world where anyone can create a fake account, how can an organization be sure someone's DID-based identity is real? This authenticity is key to how decentralized identity systems work. DIDs require attestations from existing trust providers such as businesses, educational institutions, and governments, plus independent verification of who issued an endorsement and when. By accumulating these verifiable credentials, an identity establishes greater legitimacy over time.

Understanding verifiable credentials

To understand verifiable credentials, it helps to relate them to the physical credentials people use to confirm their identity—such as a driver's license, social security card, diploma, and more. Verifiable credentials are user-controlled instances of this type of data that can confirm their identity in a digital environment.

Imagine a new employee verifying their identity in the onboarding process. Prior to the use of verifiable credentials, they'd present their new employer with multiple forms of physical identification. That company would then make and retain copies of their data. With verifiable credentials, the employee can choose the data they're sharing, which is issued as a verifiable credential that can be confirmed against a decentralized data registry through the use of a Trust System.

There are three entities in a verifiable credential ecosystem:

1. User

The user controls the verifiable credential and stores the credential in their digital wallet, which is generally an application that only that user has access to either via a PIN number or biometric identifier solely unique to them.

2. Issuer

A trusted corporation or entity confirms a *user's* claims about their identity and grants a digitally signed credential to them.

3. Verifier

A trusted corporation or entity requests verification of a *user's* credential and, upon receipt, verifies that claims in the credentials satisfy requirements.

A sample scenario

Alice is a professional at Woodgrove, Inc. seeking an employee discount from an affiliate organization, Proseware.

1. Alice requests a verifiable credential showing proof of employment from Woodgrove, which attests Alice's identity and issues a signed verifiable credential that Alice can accept and store in her digital wallet application.
2. Alice presents this verifiable credential as a proof of employment on the Proseware website.
3. After a successful presentation of the credential, Proseware offers a discount to Alice and the transaction is logged in Alice's wallet application.
4. In her wallet application, Alice can now track where and to whom she has presented her proof-of-employment verifiable credential.

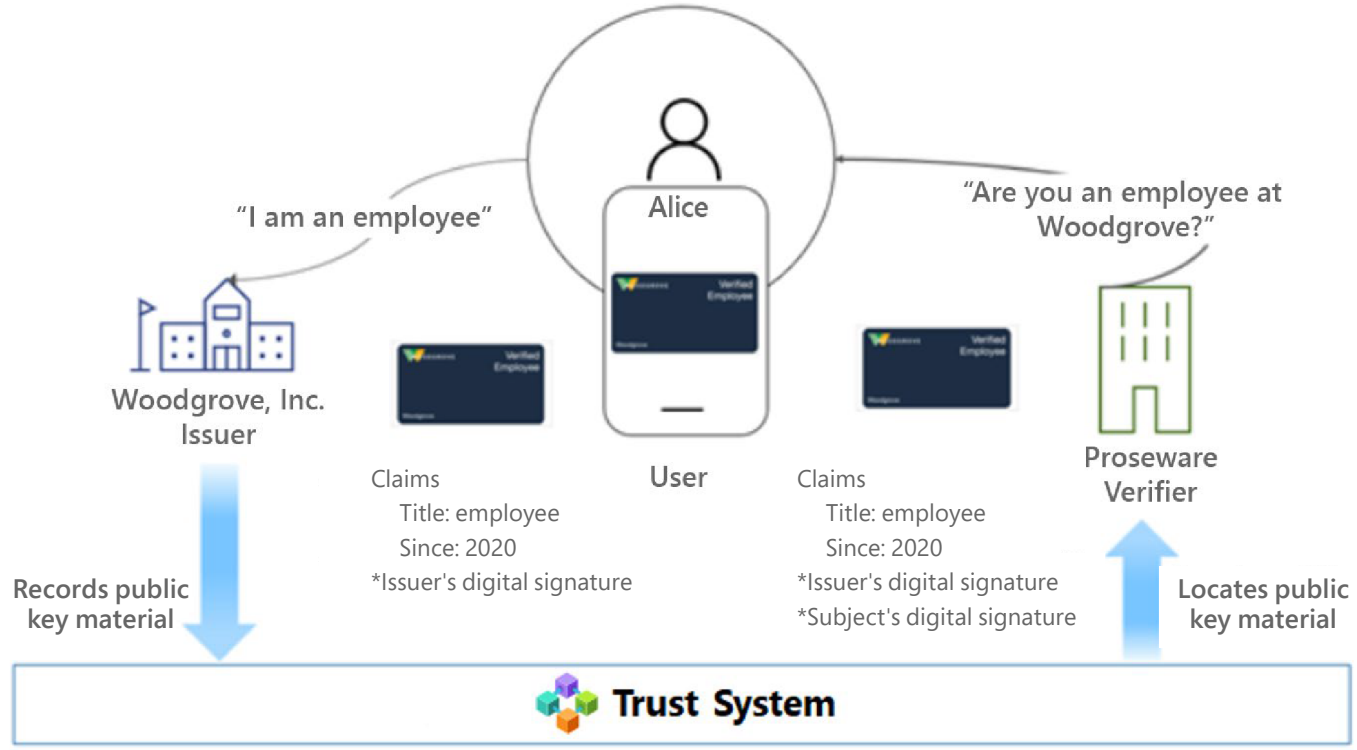


Figure 1. Verifiable credential scenario

Decentralized systems

Blockchains and ledgers

Microsoft's stance on identity

At Microsoft, we're committed to an individual's right to control and own their digital identity.

Microsoft is helping to create a future for standards-based decentralized identities through modern digital identity solutions that are:

1. **Legitimate and lawful**, ensuring that digital identities don't encourage illegal activity, enable corruption, or expose people to undue risk or unlawful access.
2. **Interoperable and accessible**, ensuring that technical and policy interoperability among domestic and international stakeholders is easy to use and offers broad inclusion and equity of access for everyone.
3. **Safe**, placing user safety and security at the center of our decentralized identity system design.

Working with our fellow members of the DIF, W3C, and other communities,[4] Microsoft is firmly committed to bringing a holistic solution to identity management needs—so everyone's data can be private, secure, and easily accessible only to them or those they choose to share it with. This challenge may seem daunting, but we're excited for this opportunity to bring everyone better solutions for digital identities.

> "The world we live in relies on digital interactions and a trust fabric that will give us the ability to instill assurance into every single one of them. When we have trust, we don't need gatekeepers. We can be fearless."
>
> **Joy Chik**
> *Corporate Vice President, Microsoft*

Microsoft Entra: Own and control your digital identity

The future of owning your digital identity starts today.

To help individuals and companies take more control over their digital identities, we're introducing Microsoft Entra, a new product family that encompasses all Microsoft identity and access capabilities. The Microsoft Entra suite includes Microsoft Entra Verified ID, which specifically addresses the need for decentralized identities.

To verify all types of identities and secure, manage, and govern access to any resource, Microsoft Entra will:

- Protect access to any app or resource for any user.
- Secure and verify every identity across hybrid and multi-cloud environments.
- Discover and govern permissions in multi-cloud environments.
- Simplify the user experience with real-time intelligent access decisions.

Learn more about Microsoft Entra and how we can help you control your digital identity.

Interested in taking a deeper dive into the world of decentralized identity? Please read our blog, Secure access for a connected world meet Microsoft Entra.

[1] Justina Alexandra Sava. Global digital identity solution market value 2020 and 2026. Statista. February 2022.

[2] Jason Allan Scott. By 2025, an estimated 70% of the workforce will be working remotely! LinkedIn. March 2021.

[3] Maximilian Moehring. 3 predictions for digital identity in 2030. LinkedIn. February 2021.

[4] Microsoft Learn. Microsoft Entra Verified ID-supported standards—Microsoft Entra.