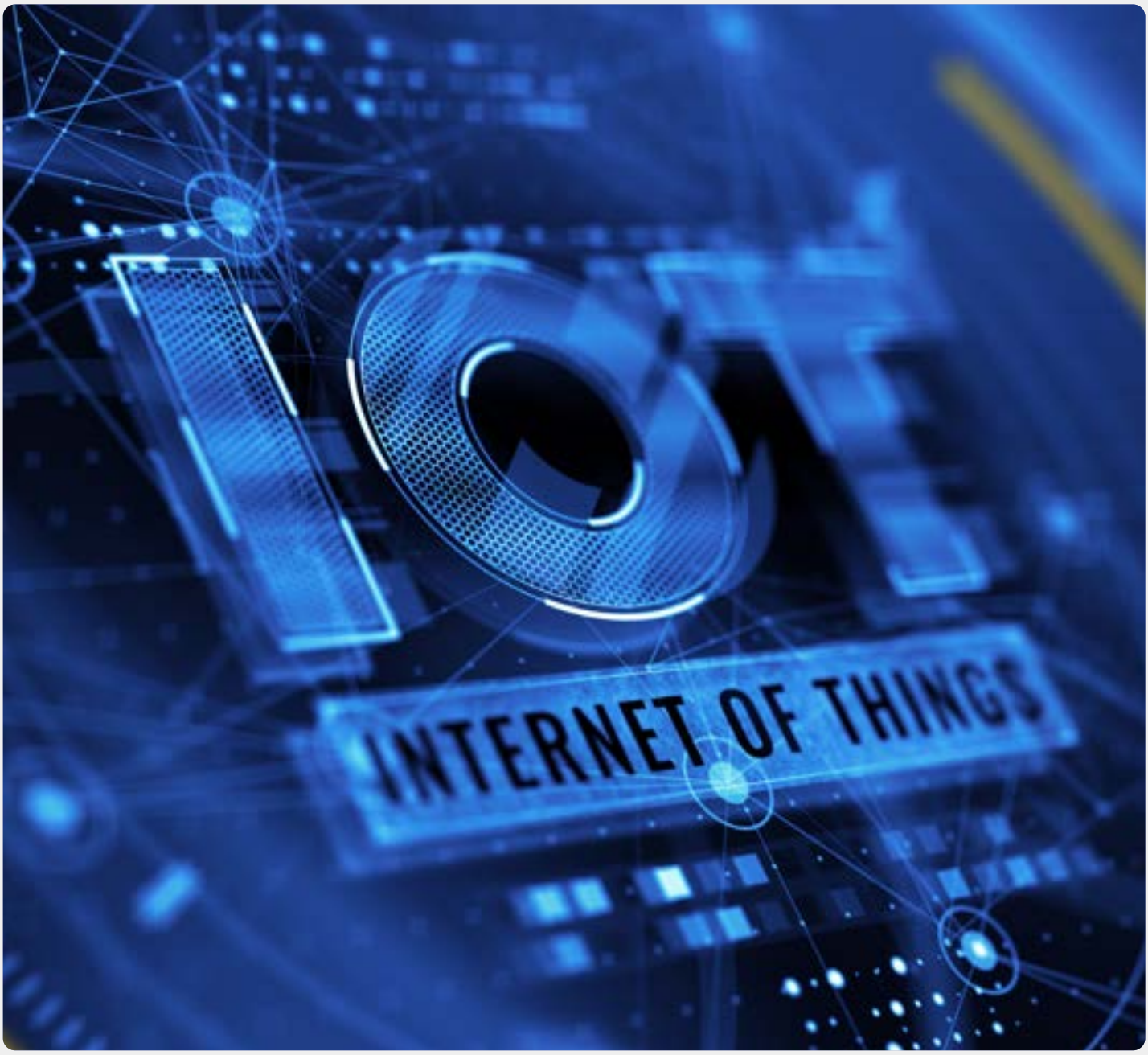
E-Book

# Decentralized Identity

Securing Trust in the Internet of Things (IoT)




Cardano Foundation

# The IoT boom and resulting trust gap

The Internet of Things (IoT), a network of physical objects with embedded sensors and software that connect and exchange data, is expanding fast. These connected devices are forecast to grow from 12 billion in 2021 to a projected 27 billion by 2025.[1] This expansion is changing industries, but it also reveals a significant trust problem. Every new IoT device is a potential target, creating a security risk that enterprises can't afford to ignore.

---

## Prevalent vulnerabilities

Over half of all IoT devices have known critical flaws.

## Default passwords

A fifth of IoT devices still ship with easily hackable default passwords.[2]

## Larger attack surface

Traditional security can't handle the millions of devices connecting from everywhere.

## Mission-critical risks

A compromised device can shut down production lines, energy grids, and supply chains.

# Identity: The foundation of IoT security

Amid the complexities of IoT security, a foundational principle emerges: a secure identity for every connected device is the cornerstone of trust. While cybersecurity has long focused on securing the identities of individuals and applications, the next phase demands a secure, unique digital identity for every IoT device—from a sensor on a factory floor to a smart meter on the grid.

A robust identity system enables the verification of a device's authenticity, its authorized access to systems and data, and its integrity against tampering. Without it, any other security measure is insufficient and can be compromised.

---

## Prevalent trust gap

Devices need to trust every other device on the network, a level of assurance that is impossible to achieve without verifiable identity.

## Zero trust default

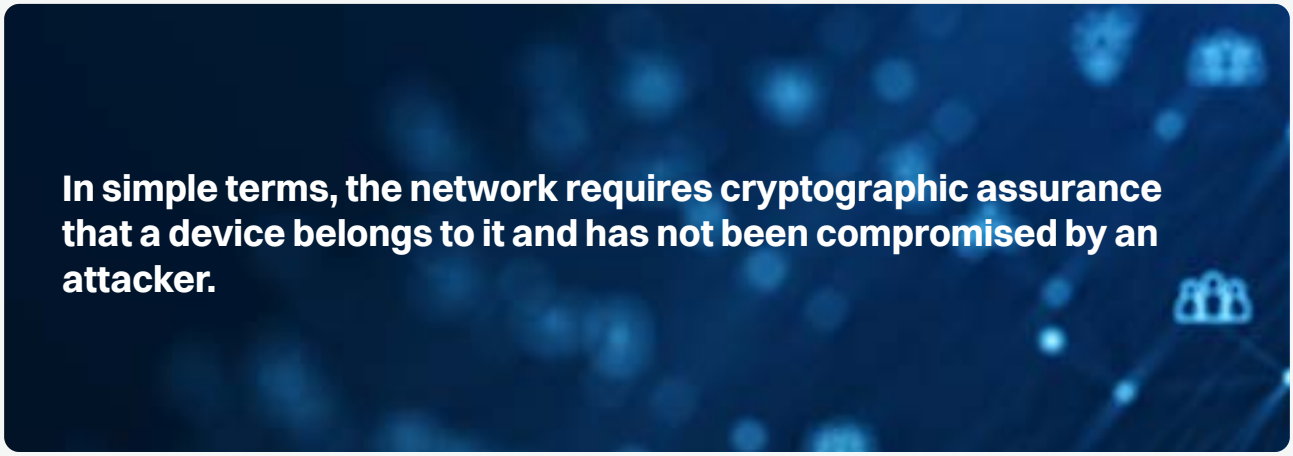
If a device's identity cannot be verified, the only secure posture is to assume zero trust.

## Machine-to-machine authentication

Devices must authenticate their peers before exchanging data or commands, a protocol essential for preventing unauthorized access.

## IoT identity is equitably critical

For enterprises, IoT device identity is now as critical as human identity.



# The operational value of verified identity

## Operational reliability

A strong IoT identity ensures that only machines with verified identities can initiate processes, which protects data integrity and operational safety.

## Prevention of rogue devices

This approach prevents an infiltrated device from masquerading as a legitimate one, guarding against data falsification and malicious commands.

## Enhanced accountability

Robust identity provides accountability by allowing every device action to be logged and cryptographically traced to a trustworthy source. This is crucial for forensic analysis and compliance.

## Assurance in critical sectors

This level of security is particularly valuable in sectors like healthcare and critical infrastructure, where the cost of a breach is immeasurable.

# The limitations of a traditional approach

Legacy identity and access management (IAM) systems were not built for billions of devices; they were designed for people. As a result, existing approaches fail to cope with the exponential scale and diversity of the IoT landscape.

## Exploring the status quo problem

Traditional identity methods are fragmented, vulnerable, and lack visibility. They can‘t keep pace with the modern threat landscape, leaving organizations without consistent, scalable trust.

### Lack of standardization

Different manufacturers use proprietary identity schemes, creating silos that prevent devices from different ecosystems from trusting each other.

### Static credentials

Many devices ship with default or hard-coded passwords that are rarely, if ever, changed.

### Fragmented integration

A single enterprise might deploy devices from dozens of vendors, each with its own identity scheme, creating an integration nightmare.

### Operational overload

Traditional IT teams lack the tools to manage credentials for thousands or millions of embedded devices.

### PKI scaling

Legacy Public Key Infrastructure (PKI) systems were not built for the high-volume automation required to manage millions of certificates for IoT devices.

### Cross-organizational trust

Establishing trust between devices from different organizations is cumbersome, if not impossible, leading to insecure shortcuts.

# From SSI to M2M Trust: Decentralized Identity for IoT

To solve the IoT trust challenge, enterprises are adopting an emerging paradigm: Self-Sovereign Identity (SSI) implemented through decentralized identifiers (DIDs) and verifiable credentials (VCs). These technologies, originally developed to give individuals control over their digital identities, are proving equally powerful for IoT devices. At their core, DIDs and VCs provide a standardized method for establishing trust without relying on a single authority.

## Decentralized Identifiers (DIDs)

A new kind of identifier that is globally unique and cryptographically verifiable. Unlike a serial number, a DID is recorded on a distributed ledger and controlled by the device owner, allowing a device to authenticate anywhere by proving possession of a key.

## Verifiable Credentials (VCs)

Tamper-evident, cryptographically signed digital attestations that a device can carry. For example, a VC could be a statement from a manufacturer that a device was produced on a specific date and is certified to a certain standard.

## Universal Interoperability

This framework breaks the identity silos that plague IoT. Because DIDs are universal, devices can mutually recognize each other's credentials even if they have never communicated before. The Industry IoT Consortium (IIC) has shown that blockchain-backed DIDs can create a unified device registry and connect IoT application silos at a global scale.[4]

# The benefits of decentralized identity

## Enhanced security and control

Device owners can hold the keys to their device's identity, giving them direct control and eliminating the need to use a manufacturer's proprietary system.[5]

## True machine-to-machine (M2M) trust

Machines can authenticate each other using decentralized credentials, just as humans present IDs in the physical world. This happens instantly, without the need for a central server.

## Streamlined management

A decentralized identity framework enables organizations to manage device credentials throughout the entire device lifecycle, from deployment to decommissioning.

## Data integrity and accountability

Decentralized identities allow for cross-ecosystem authentication and authorization at the device level, enhancing trust and transparency in the data those devices generate.

**SSI brings a scalable, interoperable trust layer to IoT. By leveraging DIDs and VCs, organizations can create an Internet of Trusted Things where data can be verified and actions authorized with high assurance.**

# IoT Identity in Action: Use Cases Across Industries

A theoretical understanding of decentralized IoT identity is essential, but seeing how it applies to real-world scenarios is even more compelling.

## Smart Manufacturing: Securing Industry 4.0

Modern manufacturing floors are showcases of the Industrial Internet of Things (IIoT), filled with robotic arms, computer numerical control (CNC) machines, and autonomous vehicles. While this connectivity drives efficiency, it also creates a substantial trust gap. A single compromised device can disrupt production, leading to recalls, downtime, or even physical damage.

Trust among machines is critical. Every sensor and controller must be authenticated. However, most factories still rely on inadequate security measures, such as ad-hoc credentials or basic network segmentation. As one expert noted, „establishing and securing a trusted identity that is unique to every device is mission-critical“ in manufacturing.[4]

### The Problem

**Ad-hoc security**

Factories often rely on insecure or easily compromised methods for device authentication.

**Widespread vulnerability**

A breach in one device can allow an attacker to impersonate other machines on the assembly line.

**Operational risk**

Without per-device trust, a single malicious actor can disrupt production or cause physical damage.

### The Solution: Decentralized Identity

Decentralized identity offers a tailor-made solution for Industry 4.0. Imagine if every machine in a factory came equipped with a Decentralized Identifier (DID) and Verifiable Credentials (VCs) issued by its manufacturer. When a device communicates with a controller, it presents its credentials. The controller instantly verifies them without needing to contact a central authority. This establishes trust in microseconds, automating and strengthening the onboarding and authentication of every machine.

#### Results

**Automated gatekeeping**

An unauthorized device plugged into the network will lack the necessary credentials, causing other machines to automatically reject its commands and data.

**Enhanced security**

The factory can instantly revoke a device's credentials when it is decommissioned, ensuring it can no longer be trusted anywhere.

**Streamlined onboarding**

A new machine can be onboarded by simply scanning its DID QR code and issuing it a factory credential through a management console, eliminating manual configuration.

**Verifiable trust**

Decentralized identity creates "zero-trust manufacturing networks," where every machine interaction is verifiable, ensuring automation and autonomy are safe from manipulation.

# Utilities and Smart Grids: Protecting Critical Infrastructure

Few sectors face the scale and stakes of IoT trust like utilities. In a smart grid, millions of intelligent endpoints—from smart meters to transformers—connect to core utility networks. This connectivity helps balance loads and integrate renewables, but it also dramatically expands the attack surface. Cyberattacks on energy infrastructure have moved from hypothetical to real; a single hacked smart meter could disrupt grid stability or serve as a pivot point into broader utility controls.

## The Problem

**Expanded attack surface**

Millions of distributed devices, often customer-owned, are now connected to historically closed utility networks.

**Insufficient security**

Utilities relied on network segmentation, which no longer protects against attacks that can pivot from a single compromised device.

**High-stakes breaches**

A rogue IoT device can manipulate billing data, disrupt grid stability, or compromise utility controls, posing a threat to national security.

## The Solution: Decentralized Identity

Unique identity and credentials for every smart grid device are becoming the linchpin of cybersecurity. Rather than trusting a meter simply because it has an ID in a database, a utility can adopt a Decentralized Identifier (DID) model. Each meter presents Verifiable Credentials (VCs) to prove its manufacturer and ownership. The utility's systems can instantly verify these credentials and reject any data or commands from a device that can't produce a valid credential chain. This protects against impersonation and man-in-the-middle attacks.

### Results

**Zero-trust networks**

Decentralized identity provides utilities a way to implement network-wide zero trust, where every device or message must prove itself at every interaction.

**Agile compliance and management**

A utility can use a single, auditable source of truth to manage device lifecycles. Revoking a compromised device is as simple as flagging its DID, with the change propagated instantly across the entire grid.

**Verifiable data integrity**

A substation sensor can sign its telemetry data with its DID, allowing the control center to verify the data's origin and integrity, preventing false information from causing a system overload.

**Confidence in automation**

By embedding trust at the device level, utilities can confidently roll out smart infrastructure without creating vulnerabilities — a critical factor as grids become increasingly automated.

# Connected Logistics: Ensuring Integrity Across the Supply Chain

Global supply chains are a complex network of assets and companies, making them a perfect fit for IoT to improve visibility. IoT trackers and sensors now monitor everything from a container's location to the temperature inside a truck. But this connectivity also raises a critical question: how can all parties involved—from the producer to the retailer—trust the data and devices that originate from outside their organization? Simply put, trust in IoT data is directly linked to trust in the devices behind that data.

## The Problem

**Lack of data integrity**

Without a unified trust framework, a distributor must rely on a producer's sensor data without a way to verify its origin or integrity, opening the door to fraud.

**Complex multi-party ecosystems**

Global supply chains involve numerous companies and systems, making it difficult to establish a single source of trust.

**Vulnerability to tampering**

From customs seals to temperature logs, the data from IoT devices can be manipulated, which can lead to financial losses and safety risks.

## The Solution: Decentralized Identity

Decentralized identity provides a framework to embed trust directly into the processes of a supply chain. Each IoT device can be issued a Decentralized Identifier (DID) and Verifiable Credentials (VCs) by its owner and other oversight bodies. These credentials can attest to the device's model and its current assignment. As a container moves, any stakeholder can retrieve and cryptographically verify the device's credentials. This means trust is baked into the data itself, not dependent on trusting a single company's IT system or a PDF report.

### Results

**Fraud and counterfeiting prevention**

If someone swaps a device or inserts false data, the credentials won't match, making it difficult to introduce fraudulent information.

**Automated compliance and audits**

It can be automatically verified that all IoT-reported metrics for a shipment are backed by credentials from calibrated devices and approved companies.

**Unbroken chain of custody**

Each time a package changes hands, the new party can issue a VC to the package's DID, creating a verifiable and unbroken chain of custody that reduces disputes and speeds up insurance claims.

**Universal interoperability**

Decentralized identity is platform-agnostic. As long as all parties adhere to the DID/VC standards, devices from one company can present trustworthy information to another's system, regardless of the IoT platform.

# Smart Cities: Building Trust in Urban IoT Networks

Cities are deploying millions of IoT devices—from traffic sensors to smart streetlights—to become more efficient. But this creates a complex, heterogeneous environment with devices from many different departments and vendors. This scale poses a significant security challenge: how to secure an urban environment where millions of devices are interacting with city infrastructure and citizens? Public trust is at stake; a single incident, like hacked surveillance cameras or manipulated traffic signals, can erode confidence in smart city initiatives.

## The Problem

**Heterogeneous ecosystems**

A smart city integrates devices and systems from numerous departments and vendors, creating a fragmented security landscape.

**Public trust is on the line**

A single security failure can erode public confidence in smart city initiatives and a government's ability to protect its citizens.

**Security and interoperability**

Without a common trust framework, even basic data sharing between agencies and systems can falter, and autonomous systems can't operate safely outside of "walled gardens."

## The Solution: Decentralized Identity

Digital identity is as fundamental to smart cities as it is to the people within them. This concept extends to every smart device or system, including drones, robots, and traffic sensors. With Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), a city can ensure that autonomous systems, like a bus, can present a credential to a smart traffic light, proving its identity and authorization. This mutual authentication ensures safety and reliability in real time, with no central server needed to verify every interaction.

### Results

**Guardian of civility and privacy**

Decentralized identity ensures city cameras only share data with authenticated law enforcement requests that carry a proper warrant credential, preventing unauthorized access.

**Enhanced resilience**

By decentralizing the identity layer, no single vendor or government entity holds all the keys. This distributes trust and enhances resilience against both cyber threats and abuse of power.

**Auditable and accountable systems**

Every connected device or algorithm has an auditable identity and credential history, ensuring technology operates with integrity and accountability.

**Regional interoperability**

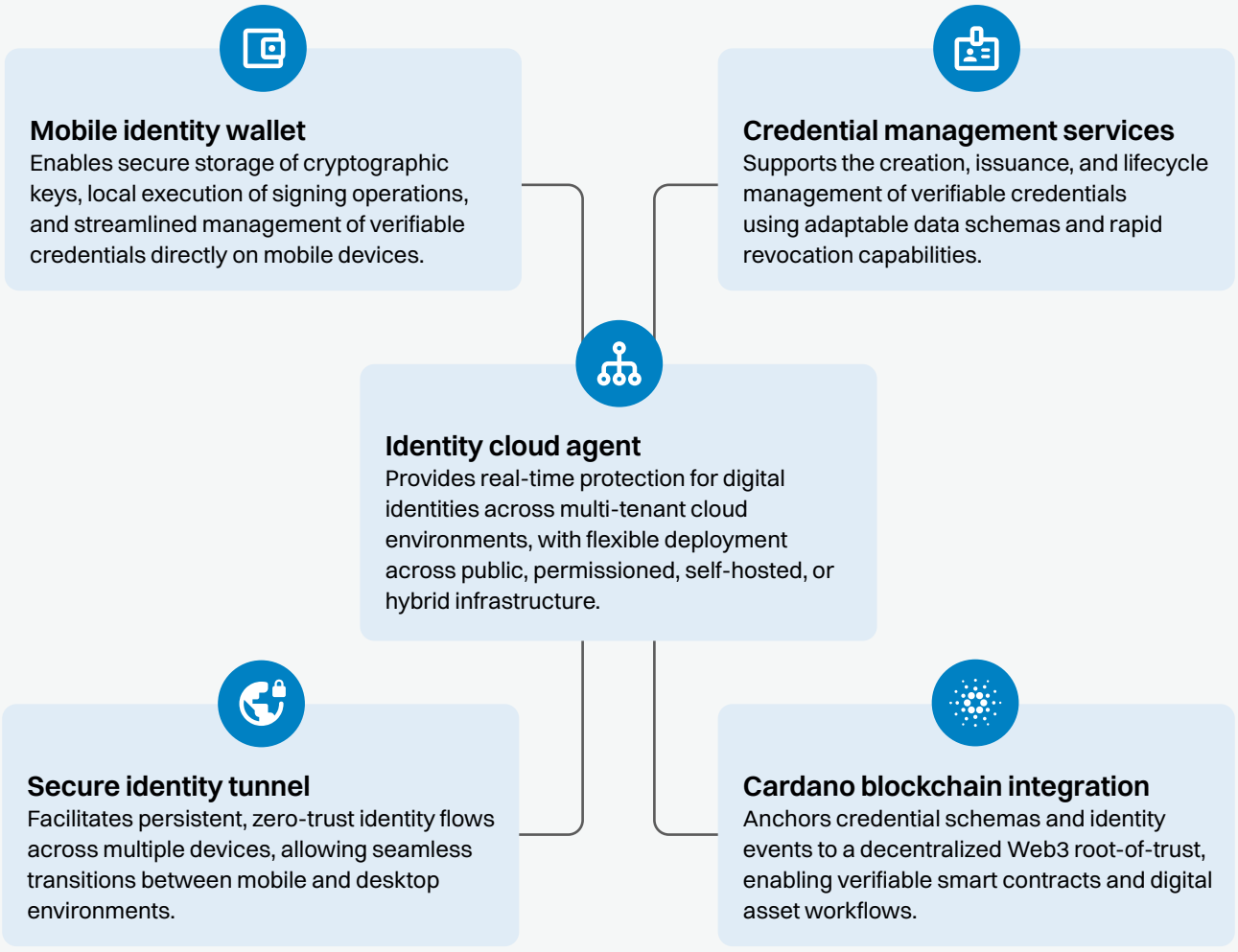
If nearby cities adopt similar standards, their devices can trust each other's credentials, which is critical for regional services like transportation and disaster response.

Veridian

# The identity platform built for tomorrow

As the need for a decentralized IoT identity becomes clear, enterprises and governments are looking for practical solutions. Veridian is the Cardano Foundation's open-source, enterprise-ready identity infrastructure, built for compliance, scalability, and interoperability. It provides a foundational layer of trust for IoT ecosystems, from smart grids to global supply chains.

## Secure digital identity management



# Using the Cardano blockchain to support trusted digital interactions

Building digital trust is crucial for humanitarian aid to scale effectively, ensuring support reaches those who need it most. This case study explores how the UNDP Tadamon Accelerator leveraged the Cardano blockchain to create a system for issuing trusted, verifiable credentials to Civil Society Organizations (CSOs) worldwide.

## The need for universally verifiable credentials

The Tadamon Accelerator for Food Security, led by UNDP, faced growing challenges verifying the legitimacy of CSOs across 57 member countries. Manual processes, inconsistent approvals, and unverifiable digital records created barriers to scale, transparency, and fraud prevention in delivering humanitarian support.

## Scaling trust in Civil Society Organizations with Veridian

Tadamon partnered with the Cardano Foundation to launch a Proof of Concept using Veridian, a digital identity platform, to issue portable, verifiable credentials to CSOs. This blockchain-based system enhances trust, enables secure digital approvals, and creates a scalable model for future public sector verification and development programs.

### Expanded reach

Tadamon aims to become the world's largest interactive CSO database by 2029.

### Reduced fraud risk

Verifiable digital identity decreases impersonation and forgery.

### Faster verification

On-chain records significantly reduce time and manual effort.

### Full transparency

Immutable data supports real-time application monitoring.

### Empowered CSOs

Verified credentials improve access to funding and partnerships.

### Portable identity

DID-compliant credentials usable across platforms and programs

***"We are confident that this partnership will strengthen our collective presence in OIC Member Countries and empower, inspire, and connect CSOs in their mission to improve the socio-economic well-being of marginalized communities."***

**Robert Pasicko**
**UNDP Program Coordinator**

**Sources**


[1] https://www.iotforall.com/state-of-iot-2022

[2,3] https://jumpcloud.com/blog/iot-security-risks-stats-and-trends-to-know-in-2025

[4,5] https://www.iotforall.com/state-of-iot-2022

[6] Ted Shorter, “Six Steps For Establishing Trust In IoT Device Manufacturing Supply Chains,” Forbes, November 25, 2020.


---

Cardano Foundation

The Cardano Foundation is an independent, Swiss-based not-for-profit advancing Cardano as a public digital infrastructure across a wide range of industries.


Dammstrasse 16 • 6300 Zug Switzerland


Explore more

cardanofoundation.org