



Decentralized Identity vs. Traditional Identity Management

THE ULTIMATE COMPARISON GUIDE

JANUARY 2024

www.gataca.io
hello@gataca.io

user@ga


Issuance date
July 10, 2022

sept

 Verifiable ID
Government

Gov ID n°

Issuance date
January 12, 2023

 Driver's license
Government

V123456K

Issuance date
July 10, 2022

 Acad
Univ

Engine

Issuanc
Janua

TABLE OF CONTENTS

01

Introduction

02

Traditional Identity
Management

03

Decentralized Identity
Management

04

Traditional vs. Decentralized
Identity Management

05

Use Cases

06

Preparing for transition

07

Decentralized Identity
with Gataca

INTRODUCTION

The Impact of Identity Management in the Digital World

BY
Gataca



Identity management has always been a crucial aspect of organizational security and efficiency.

While traditional identity management systems have served us well for decades, they are increasingly scrutinized for their vulnerabilities and limitations, especially in the face of sophisticated cyber threats and growing privacy concerns.

In this context, decentralized identity emerges – a paradigm shift in how we approach identity management. This new approach promises enhanced security, increased privacy, and greater user control.

But what does this shift mean for organizations? How does decentralized identity stack up against traditional systems in practical terms?

This guide aims to demystify decentralized identity and provide a clear comparison with traditional identity management systems. It is designed to be a resource for organizations navigating the evolving identity landscape, helping them make informed decisions about the future of identity management.

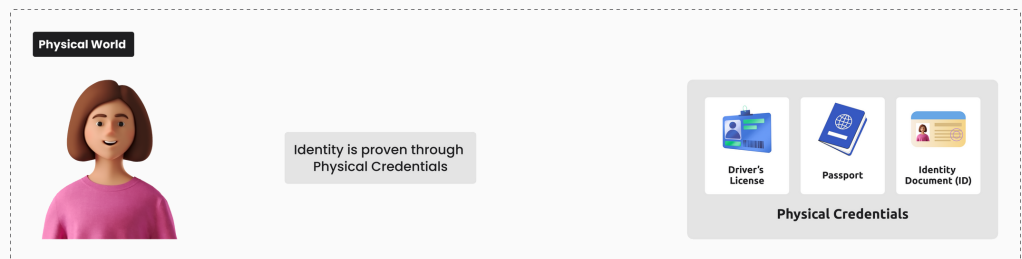
We will explore the technical foundations, practical implications, and strategic considerations of both models.

TRADITIONAL IDENTITY MANAGEMENT

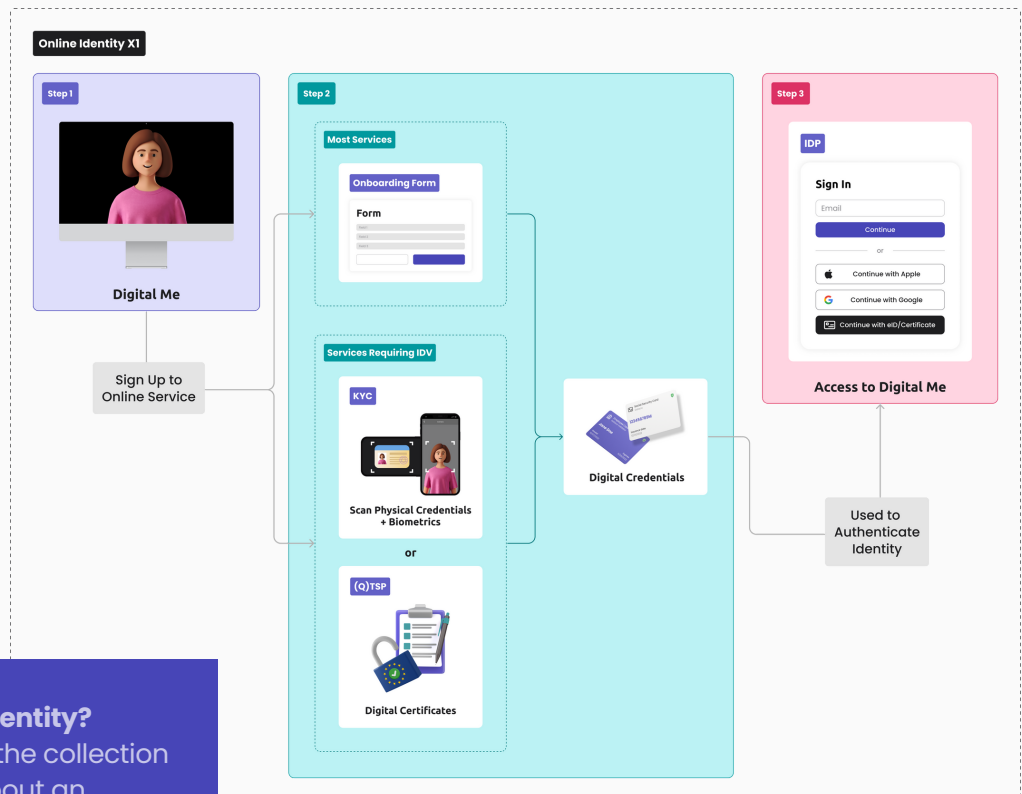
Traditional identity management systems have been the foundation of organizational security for decades, being in charge of identifying, authenticating, and authorizing individuals to access resources.

HOW IT WORKS

In the real world, you use physical credentials like a driver's license or passport to prove your identity.



Online, this process is a bit more complex as you need first to create a *digital me*, representing your digital identity.



What is digital identity?

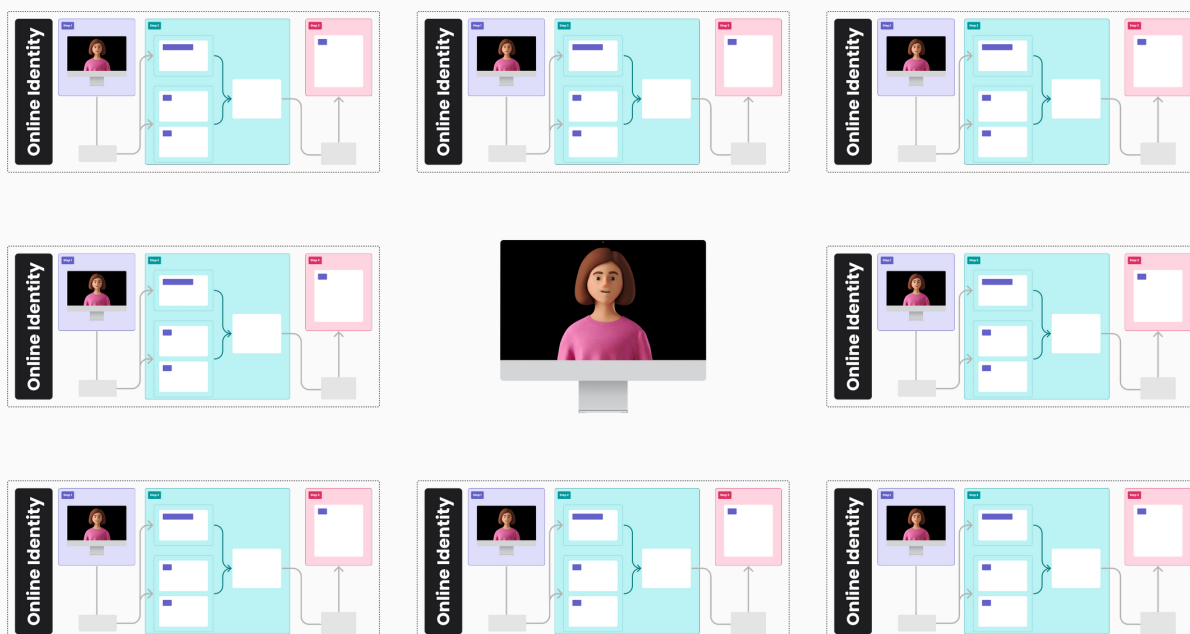
Digital identity is the collection of information about an individual, organization, or thing that exists online. This includes usernames, passwords, personal data, and online activities used to identify and interact in the digital world.

To create a digital identity, you typically sign up for online services by filling out a form with personal details like your name, email, and address.

For services like banking that require identity verification, you might also undergo a "Know Your Customer" (KYC) process, including providing ID and biometric scans. In Europe, for legal or government transactions, you may alternatively obtain a digital certificate from a Qualified Trust Service Provider (QTSP) as proof of identity.

These processes generate digital credentials, the keys to your digital identity. These credentials authenticate your identity when logging into websites or apps, verified each time by Identity Providers (IdPs).

Consequently, in traditional identity management, you create separate digital identities for each new online service or platform, leading to multiple digital identities across various services.



KEY COMPONENTS OF TRADITIONAL IDENTITY MANAGEMENT SYSTEMS

IDENTITY REPOSITORY

In traditional systems, identity data is stored in centralized databases. These repositories keep user information, such as usernames, passwords, personal details, and access rights.

AUTHENTICATION MECHANISMS

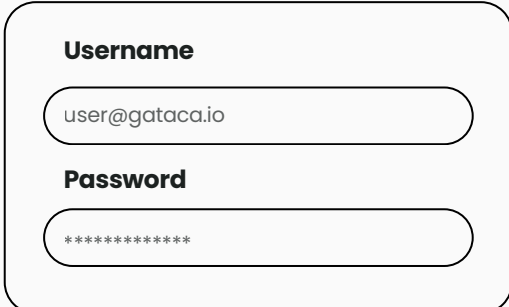
These methods are used to verify a user's identity.

Username/Password

The classic combo

Users create a unique identifier (username) and a secret key (password) for account access.

While widely adopted as it is easy to understand and implement, passwords can be vulnerable to brute-force attacks, phishing attempts, or user negligence.



The image shows a login form with two input fields. The first field is labeled "Username" and contains the text "user@gataca.io". The second field is labeled "Password" and contains a series of asterisks "*****".

Magic Link Authentication

The click-to-enter approach

After entering their username, the user is sent a URL, usually via email or text message, which they can click to log in directly instead of remembering a password.

This method adds an extra layer of security but opens the door to attacks targeting email accounts or interception of verification messages, and if a user's email account gets compromised, unauthorized access to other services could be on the horizon.

Single Sign-On (SSO)

The one-key access



SSO allows users to log in to multiple applications or services with a single set of credentials, such as those provided by Google, Facebook, or Okta. This simplifies the user experience but exacerbates privacy and security risks by further centralizing user data in their databases.

To avoid this, SSO services often use advanced security features like two-factor authentication and SMS OTPs, removing the initial improvement of the UX.

Additionally, when using this authentication method, you delegate your identity management to big techs, who receive the power to manage your access to third-party services while accumulating more and more information about your consumer profile.

Digital Certificates

The Seal of Trust

Using digital certificates for authentication means that users can prove their identity without transmitting a password, reducing the risk of interception or unauthorized access. This method is often used in environments requiring high levels of security, such as financial services, government, or healthcare.

However, they are less commonly used for everyday user authentication due to the complexity of obtaining and managing digital certificates and infrastructure limitations.

AUTHORIZATION AND ACCESS CONTROL

Involves managing and enforcing access rights and permissions for users.

IDENTITY LIFECYCLE MANAGEMENT

This includes provisioning new accounts, updating user details, and deactivating accounts.

Pros:

- **Familiarity:** After all these years, traditional methods have earned worldwide recognition and are easily understood by users.
- **Ease of Implementation:** Many traditional authentication methods are relatively straightforward, requiring minimal technical expertise.
- **Widespread Acceptance:** Because traditional methods have been around for a long time, they are widely accepted and integrated across various services, making them a default standard in identity management.

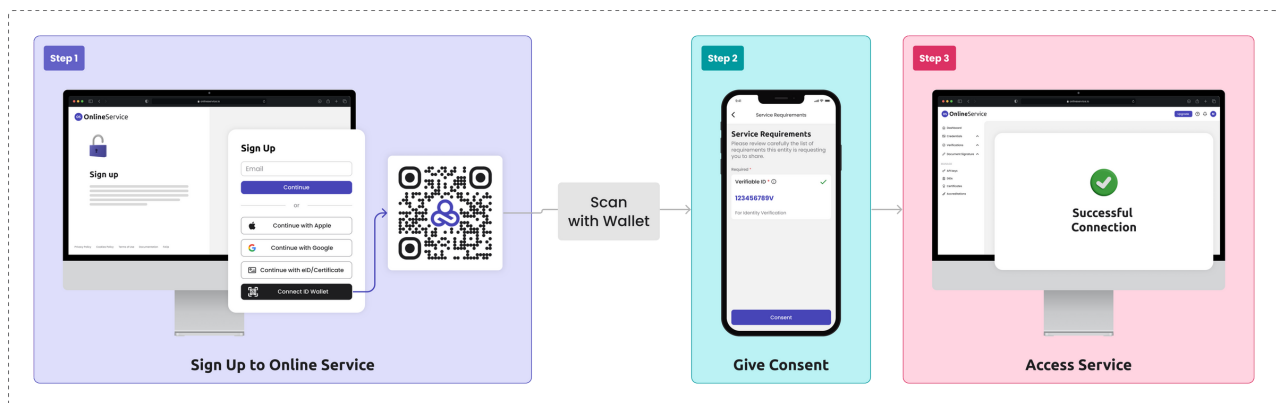
Cons:

- **Security Vulnerabilities**
 - **Centralized Data Storage:** Traditional systems often store personal user data in centralized databases, making them potential targets for hackers.
 - **Single Point of Failure:** Should a centralized system suffer a breach, it could lead to unauthorized access across multiple services — a domino effect we'd rather avoid.
- **Privacy concerns:** Users often have to trust service providers with their personal information, with limited ability to control how this information is used or shared.
- **User Experience:** Issues like password fatigue and complex authentication processes, especially during onboarding, can lead to a poor user experience.

DECENTRALIZED IDENTITY MANAGEMENT

HOW IT WORKS

The decentralized identity management process differs from traditional identity management systems in how digital identities and credentials are created, managed, and used.



Instead of getting credentials from each service you sign up for, you obtain your digital credentials – the documents or data that verify your identity or qualifications online – from a government entity, a Qualified Trust Service Provider (QTSP), or sometimes, you can create them yourself.

Here's where things turn interesting: these credentials are stored in an ID wallet, an app on your phone. This ID wallet allows you to store, share, and manage access to your digital identity.

You no longer have to surrender control of your information to the organizations you interact with. You are now in complete control of your data across the web, deciding who can access your data and including the option to revoke access whenever you choose.

How does this work in practice? Imagine you're accessing an online service. Instead of going through a lengthy and tedious onboarding process, you simply scan a QR code on the service's website using your ID wallet.

You then consent to share the necessary credentials for identity verification, and voilà – you're in. This method provides seamless and compliant identity verification in just seconds.

The key difference between traditional and decentralized identity management lies in who controls and how personal information is distributed.

Decentralized Identity Principles

01 Privacy

Individuals can decide when, where, and with whom they share their personal information. This aligns perfectly with data protection regulations, given that the pre-verified identity documents (Verifiable Credentials) also allow users to disclose only the necessary information for their verification.

02 Authenticity

Decentralized Identity uses cryptographic techniques to ensure the integrity and authenticity of identity information. So when a user proves who they are, there's no room for doubt.

03 Portability

Instead of creating a new identity for each service, you have a single identity that you control and can use across different services and platforms. This makes it easier and more efficient to manage your online presence.

KEY COMPONENTS

Verifiable Credentials (VCs)

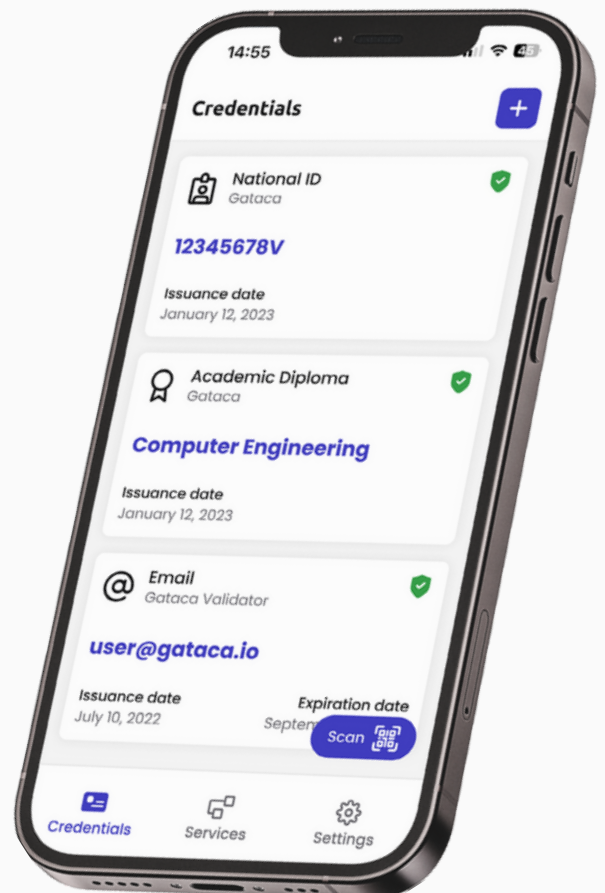
These are secure digital documents containing information about a person or entity that can be easily shared and automatically verified.

ID Wallets

Mobile or web apps where you can keep all your identity documents as Verifiable Credentials and use them to authenticate in digital services, managing your data across the web.

Decentralized Identifiers (DIDs)

DIDs are like your digital fingerprints — unique and globally resolvable identifiers. They serve as the foundation for establishing self-sovereign control over identity.



Pros:

- **Increased Security:** Decentralized identity enhances security using biometrics, strong encryption, and distributed storage. This minimizes the risk of large-scale data breaches, ensuring data integrity and reducing the likelihood of identity theft.
- **Reduced Identity Fraud:** Credentials are issued and cryptographically signed by trusted authorities, making automatic identity verification possible. This ensures that only verified individuals can access your organization's services.
- **Enhanced Privacy and Control:** Individuals have greater control over their data. They can choose what data to share and with whom, increasing data protection and reducing the risk of privacy breaches.
- **Improved User Experience:** Users can enjoy passwordless access to online services by simply scanning a QR code with their ID Wallet to share their credentials. This reduces onboarding abandonment rates and increases user retention.
- **Cross-border Interoperability:** Decentralized identity technology is designed to work seamlessly across different industries and countries, not just in the European Union.
- **Cut Costs:** Decentralized identity offers potential efficiency gains by reducing operational expenses related to customer identity verification processes, lowering expenditures on fraud prevention, and reducing storage costs for attributes and attestations.



Cons:

- **Adoption Challenges:** It may take some time until the general public gets familiar with the concept of managing their own digital identity, especially for users who are not tech-savvy.
 - Educational campaigns and easy-to-use interfaces can help ease the transition for users.
- **Regulatory Challenges:** The regulatory environment for decentralized technologies is still developing.
 - Nevertheless, different jurisdictions around the world are making significant developments in digital identity, such as eIDAS 2.0 in Europe, the Improving Digital Identity Act in the US, Australia's newly introduced Digital ID Bill, and the UK's Digital Identity and Attributes Trust Framework (UK DIATF)

- **Lack of Short-term Interoperability:** Global standards and governance for decentralized identity are still in progress, so you may encounter situations where the identity app you've chosen isn't recognized by a vendor you want to work with, requiring different identity apps.
 - Adopting open standards and protocols is key to ensuring interoperability in the long term, and the industry as a whole is working toward this end goal.

TRADITIONAL VS. DECENTRALIZED

	Traditional	Decentralized Identity
Digital Identity Provider	Service providers	Users
Data Storage Location	Organizations typically store user data in centralized databases	Users store their data on their devices or cloud storage
Data Control	Organizations hold and manage the data users share with them	Users have complete control over their personal data
Data Disclosure	Organizations often demand more information than required	Users can disclose only the information needed for authentication
Portability	Users must create separate accounts and profiles for each service	Users can use the same identity across multiple services
Security	Security focuses on the safeguarding of central databases	Strong encryption and distributed storage

CONSIDERATIONS AND CHALLENGES

01

Privacy & Consent

Organizations should carefully evaluate their privacy and user control needs, with special attention to regulatory compliance and meeting consumer expectations.

Decentralized identity gives users precise control over the data they share with different entities. In contrast, traditional systems may offer limited control, leading to the collection and sharing of user data without informed consent.

Moreover, decentralized systems prioritize data minimization, sharing only essential information and reducing the risk of unnecessary exposure. Traditional systems, however, may collect more data than needed for user verification, posing potential privacy risks.

Security

Security is a key factor when choosing between decentralized identity and traditional solutions.

Decentralized Identity's cryptographic techniques and architecture boost security, lowering the risk of major data breaches by avoiding a single point of failure for personal information.

In contrast, traditional systems, reliant on centralized databases, face more security challenges. A breach in the central repository could result in significant privacy and security issues.

02

03

User Experience and Usability

User experience is essential for successfully implementing any identity management solution, whether decentralized or traditional.

According to the [European Commission impact assessment study](#), the estimated savings from more efficient onboarding procedures for financial services in the EU would range between \$860 million and \$1.7 billion per year.

In traditional systems, users often juggle multiple usernames and passwords, leading to password fatigue and a suboptimal user experience. Additionally, identity verification processes tend to take time and effort.

Decentralized Identity improves the user experience by eliminating passwords and maintaining a single digital identity that can be used across various platforms and services.

Regulatory Compliance

04

Regulatory compliance is vital for organizations but has traditionally been complex and resource-intensive as centralized data storage poses challenges in ensuring privacy and data protection compliance.

Decentralized identity solutions align with privacy-focused regulations such as GDPR, HIPAA, or CCPA by giving users greater control over their data.

05

Interoperability and Adoption

The selected approach should match existing systems, industry norms, and user expectations for smooth integration and widespread acceptance within the organization and the larger ecosystem.

Decentralized identity's potential for seamless integration and cross-platform use can boost user convenience and experiences. While traditional methods may be familiar, they might restrict interoperability across various services and platforms.

Implementation Complexity

Implementation complexity is crucial because it directly affects the feasibility, cost, and success of adopting decentralized identity or traditional solutions.

Organizations must assess their technical capabilities, available resources, and willingness to navigate the complexities associated with each option to make informed decisions aligned with their specific needs and goals.

Decentralized solutions may need initial adjustments to existing systems, while traditional solutions face ongoing complexities in managing and adapting to evolving security challenges to mitigate centralized risks.

06



DECENTRALIZED IDENTITY USE CASES

Customer onboarding (KYC / KYB) —

Streamline compliant onboarding processes by enabling individuals to securely prove their identity and provide the necessary information in one click. This can reduce the time and resources needed for identity verification and improve the user experience.

User authentication (SSO) —

No more username and password logins. Combine the simplicity of a Single Sign-On (SSO) with government-grade secure identity systems to provide the best user experience, reduce identity fraud and comply with data protection regulations.

Physical Access Control —

Provide secure access to your facilities in proximity scenarios, where you can seamlessly verify identity information in seconds. Combine SSI technology with smart locks or turnstiles to automate access control in office buildings, hotels, or airports.

Issuance of identity credentials —

Issue tamper-proof digital certificates, qualifications, badges, tickets, and other personal data or identity attributes, and let users store them in a mobile ID wallet. Users can securely access your services or share them with third parties.

Signature of contracts and other documents —

Enhance your business security, efficiency, and convenience, and reduce costs with electronic agreements. Automatically fill in signee information in legal agreements, contracts, and other important documents, and enable qualified electronic signatures.





Electronic voting —

Provide a more secure, transparent, and trustworthy way of conducting electronic voting for elections, corporate decisions, membership voting, opinion surveys or market research. Using SSI technology in electronic voting reduces the risk of errors and increases confidence in the democratic process.

USE CASES EXAMPLES BY SECTOR

Here are select use case examples from three sectors, showcasing decentralized identity solutions' versatility and wide-ranging impact, which extend well beyond these examples.






DIGITAL BANKING AND FINANCIAL SERVICES

 Customer onboarding (Reusable KYC) Reduce the time and effort required for identity verification while complying with regulatory requirements with a verifiable KYC credential	 Issuance of financial certificates Issue digital certificates to customers, which can be securely stored in their ID wallet. Examples like credit scores or titles of ownership can trigger new revenue models
 Loan applications Streamline the application processes by accepting verifiable background information such as academic qualifications or salary certificates	 Secure payment transactions Verify the identity of customers during payment transactions, reducing the risk of fraud and increasing security








GOVERNMENT SERVICES



 Issuance of government documents Issue tamper-proof government documents in a standard, digital format that can be securely shared globally	 Citizen identity verification Allow secure identity verification of citizens in the public and private sectors by empowering the use of Verifiable IDs	 Access to E-government services Drive accessibility to e-government services, including tax filing, license applications, fine payments, and more
 Benefit transfer Allocate easily and soundly government benefits, such as social benefits or grant applications to citizens	 Electronic voting Securely verify voters' identity and ensure the voting process's integrity	

EDUCATION

 Issuance of digital education credentials Issue tamper-proof educational credentials such as diplomas, transcripts of records, certificates, or student cards in a standard, digital format	 Student authentication Improve identity verification of students for admission processes, course registrations, or exam attendance, reducing the risk of academic fraud	 Campus access Manage secure entry to campus buildings, systems, and resources, such as student portals, libraries, and laboratories
 International mobility Share educational credentials easily cross-borders in a standardized format for international mobility of students and staff	 Job application Offer tamper-proof, self-verifiable credentials for job application processes and eliminate the need to manage authenticity requests	



Check out the [success story of ERUA](#) and the [University of the Aegean](#) in implementing Verifiable Credentials!

NEXT STEPS

PREPARING FOR TRANSITION

The transition from traditional identity management to decentralized identity is a multifaceted process that requires a holistic approach to address data privacy, security, and user experience.

Step 1: Assess Current Systems and Processes

Evaluate your organization's existing identity verification and authentication processes and identify which customer data you are collecting and their sources of trust (who issues/attests to the veracity of the information).

Step 2: Define Specific Use Cases

Identify specific scenarios or problems that decentralized identity management can solve and evaluate complexity, necessary stakeholders, generated impact, and capability to scale. Create user stories and journey maps to visualize how users interact with the ID Wallet in the selected use case.

Step 3: Engage Stakeholders

Engage and get commitment from all impacted stakeholders, including internal teams, decision-makers, customers, national authorities, regulators, and partners.

Step 4: Choose the Right Technology Partner

Consider factors like a strong track record and expertise in decentralized identity technology, deployment options (on-premise versus cloud strategies), industry expertise, implementation times, scalability, customization, user-friendliness, and support quality.

Step 5: Build a pilot

Conduct a pilot project with a duration of 6-12 months to assess the feasibility and gather insights before implementing decentralized identity technology organization-wide.

Step 6: Scale Up the Pilot

Once the pilot is successful and refinements are made, gradually scale up the project. This could involve expanding the user base, adding more use cases, or extending the system to additional platforms or services.

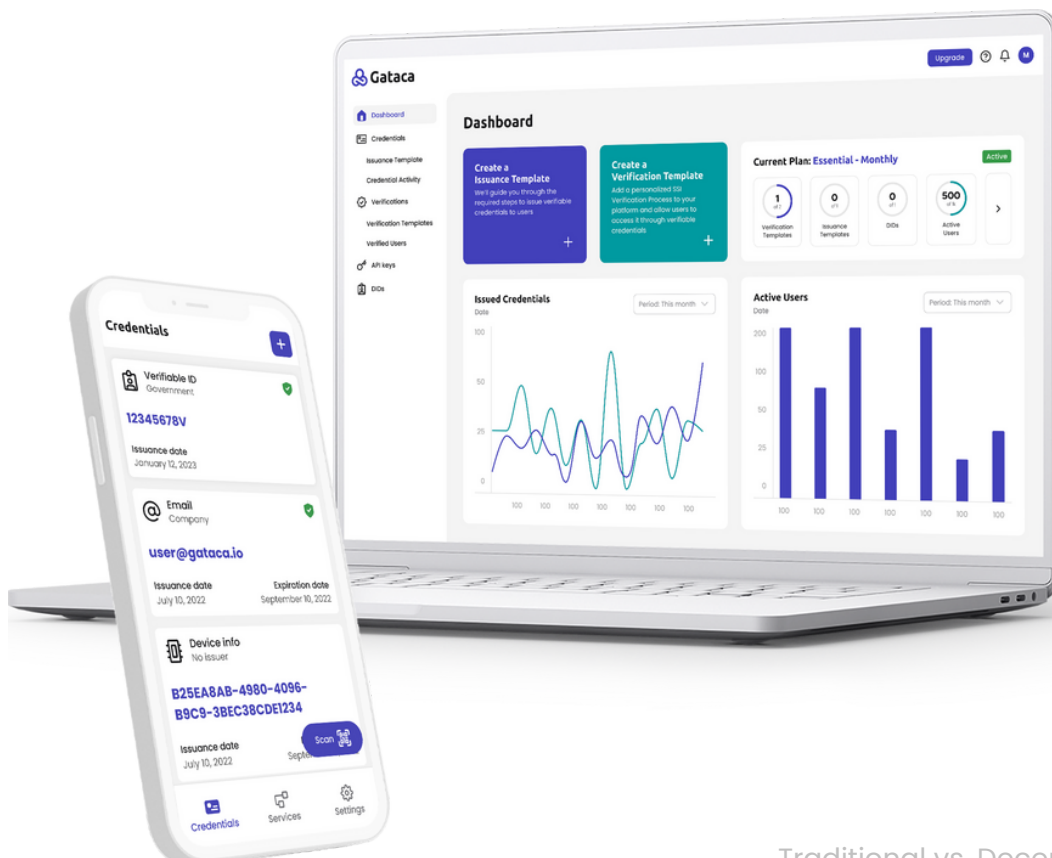
Step 7: Plan for Phased Production Deployment

Develop a phased approach for rolling out the decentralized identity management system. This should include timelines, resource allocation, training for users, and strategies for integrating with existing systems.

ABOUT GATACA

Gataca is an all-in-one decentralized identity platform for organizations.

Corporations and institutions around the globe use Gataca for compliant identity verification in seconds, interacting with ID Wallets to eliminate identity fraud and improve user experience.



Gataca Wallet

Gataca Wallet is a mobile app providing users with unlimited, encrypted storage of verifiable credentials, allowing them to authenticate themselves seamlessly in digital services.

These credentials, say a national ID, an academic diploma, or an employee card, are digitized following W3C Verifiable Credential standards, cryptographically signed by authorities to guarantee their authenticity, and protected with biometrics and strong encryption so only the users can decide who can access their data, including the option to revoke access.

Gataca Studio

Gataca Studio is a cloud platform solution that allows the issuance, verification, and management of verifiable credentials from a simple dashboard.

It provides credential issuance features for Trusted Authorities and Single Sign-On authentication tools for service providers, which can be integrated seamlessly with our plug-and-play deployment system.

Our platform provides flexible integration capabilities with diverse blockchain networks, databases, and centralized Public Key Infrastructures (PKIs), enabling end-user interoperability.

Get in touch

www.gataca.io

hello@gataca.io