iProov

G-Cloud 15 iProov Decentralised Identity Service Definition

Service Overview

In our increasingly digital world, ensuring trust and security in online interactions is paramount. Digital identity verification has revolutionised remote onboarding processes, but it's only one piece of the puzzle. For a safe and healthy digital society, governments need ongoing identity assurance throughout a constituent or employee's lifecycle.

This is why digital identity wallets will become the cornerstone of our digital infrastructure. They turn a one-time onboarding process into digital proofs that individuals can use to prove who they are across systems and applications. In a seamless, mobile-first experience, governments can securely verify someone's identity, issue fraud-proof credentials to their smartphone, and request those credentials for passwordless multi-factor authentication and identity re-verification at any point in time.

By decentralising identity, governments put people in control of their data, fostering trusted interactions with constituents and employees. Nothing is shared without the user's explicit consent. They manage and disclose the information necessary for specific transactions, like the fact that they're over 18 rather than their whole ID. Selective disclosure and decentralised data storage minimise the risk of data breaches and facilitate compliance with stringent data protection standards, like GDPR.

The benefits of decentralised reusable identity extend beyond individual empowerment to encompass broader societal advantages. By fostering trust and security in online and in-person interactions, this approach promotes confidence and reliability in digital transactions, ultimately contributing to a safer and more efficient digital ecosystem. Furthermore, its interoperability enables seamless integration across diverse systems and applications, driving greater efficiency, collaboration, and innovation across industries and sectors.

In the current context of synthetic identity fraud and deepfakes, it's imperative governments invest in secure digital infrastructure. It's time to challenge existing processes and break down silos between digital onboarding and authentication.

Summary of iProov Decentralised Identity

iProov Decentralised Identity is an infrastructure to enable governments to simplify identity verification and issue phishing-resistant credentials to an individual's smartphone. These credentials can be leveraged for secure multi-factor authentication and identity re-verification throughout the identity lifecycle.

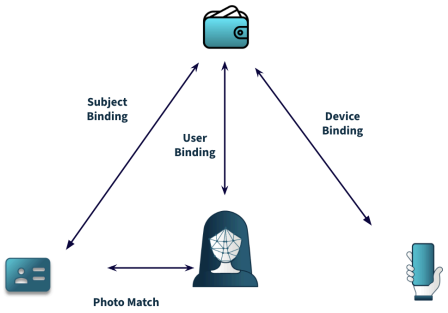
The solution gives access to world-leading biometric technology that streamlines onboarding and mitigates fraud. By binding the user's biometrics to their identity and device, governments can foster trusted interactions with employees and constituents that protect privacy and boost security. Advanced biometric technology powered by iProov Dynamic Liveness gives unwavering assurance it's a real person, the right person, and they're authenticating right now - a critical tool for any government in the current climate of deepfakes and generative AI.

iProov Decentralised Identity enables governments to issue verifiable credentials to an existing mobile app or the ready-made, third-party Partner wallet app. To request credentials, relying parties simply configure an OpenID Connect (OIDC) authentication flow to adopt the technology within existing systems without writing a line of code.

Identity Verification

In a simple, mobile-first onboarding process, individuals are bound to their real-world identity by capturing their ID document and facial biometrics. The smartphone's in-built NFC reader cryptographically verifies biometric identity documents, and the user is matched to their identity with face matching and liveness detection technology. Alternatively, government bodies can verify identity by connecting to government databases, such as the DVLA, or leveraging the on-device wallet, such as Apple Wallet. The Partner application is an Identity Service Provider for onboarding and identity proofing of individuals.

The user's smartphone is transformed into a cryptographically secure hardware token by creating a private/public key pair on the device and linking it to the onboarding process. This secure three-way binding of the user, identity, and device is leveraged to authenticate and reverify individuals at any time. This provides very high protection of services using iProov Decentralised Identity for multifactor authentication.



Device Binding: establishing and maintaining a connection between the Partner app and the device upon which it is installed

Subject Binding: establishing that the user is the subject of the identity evidence used in the proofing process

User Binding: establishing that the user at enrolment remains the user of the Partner app using liveness-verified biometrics, mitigating the risk of identity takeover

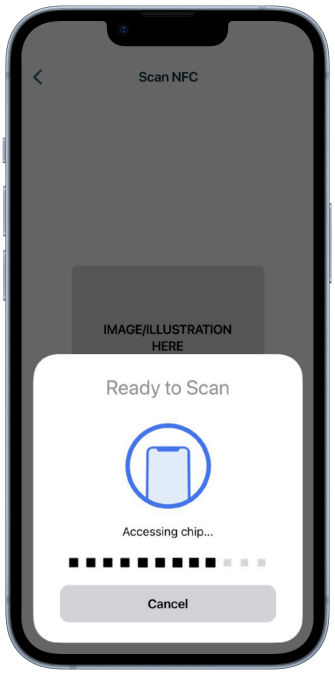


Figure 1: Typical Identity Verification Process

1. Individuals scan the e-chip in their ID document with the in-built NFC reader in their smartphone. The data is extracted and cryptographically verified.

2. Individuals capture their face biometrics, which are matched to their ID document and analysed for liveness to ensure it's a real person, not a spoof.

Authentication and Re-verification

After the initial identity verification process, employees and constituents can safely store fraud-proof identity credentials on their smartphone. Organisations can use these credentials for phishing-resistant, passwordless authentication based on defined policies. This may be single-factor or multi-factor authentication, or full re-verification by re-reading the document chip using NFC technology.

Single or Multi-factor cryptographic authentication:

1. **Device possession:** Links a public/private key pair connected to the user's smartphone and can be protected by a PIN or on-device biometrics.
2. **Biometric authentication:** Compares the user's face with their enrolled biometric template using Dynamic or Express Liveness.
3. **ID document possession**: Validates an onboarded ID document by re-reading its chip using NFC technologies.

The biometric and document-driven authentication methods are unique as they link back to the user's legal identity. This process is recommended for high-risk scenarios, such as account creation, affirmation of entitlements and certificates by employees, high-value transactions, and account recovery.

Credential Issuance and Selective Disclosure

iProov Decentralised Identity facilitates consent-driven, data-minimised interactions that adhere to stringent data protection standards, such as GDPR. A selective disclosure mechanism ensures organisations only request the details they need, which they do by configuring a QR code and adding it to their website or app. Users scan the QR code with their wallet app (or tap a button on mobile) to approve the data-sharing request.

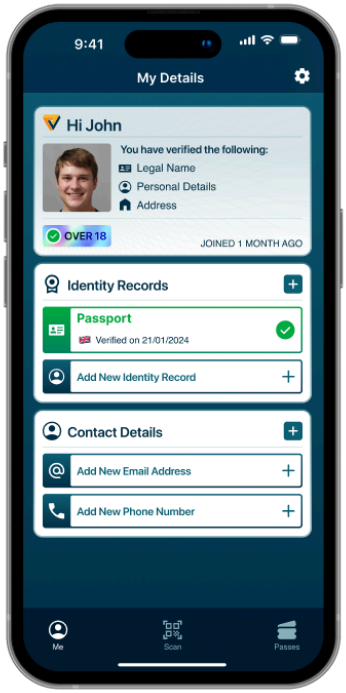


Figure 2: Credential Issuance

After successful onboarding, identity details are stored in the user's wallet as Verifiable Credentials.

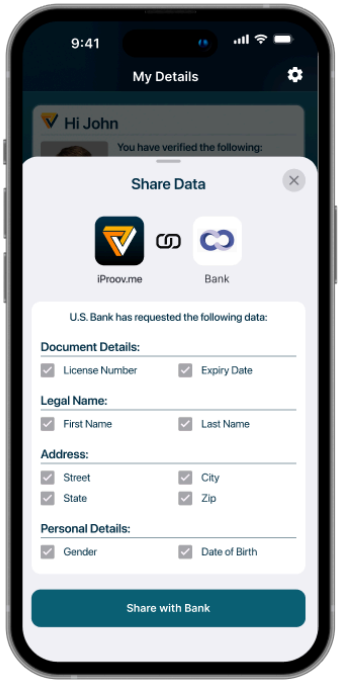


Figure 3: Credential Sharing

Users scan a QR code on the relying party's website with their app and approve or reject a request to share selective credentials.

There are three main entities involved in this decentralised identity ecosystem.

1. **Issuer:** An entity, such as a government agency, can issue, update, and revoke fraud-proof digital credentials to a user's smartphone.
2. **User**: The user has complete ownership over their digital credentials, which are stored locally on their smartphone within the Holder Service Provider. They cannot be shared without explicit consent granted via their mobile wallet app.
3. **Relying Parties:** An entity, such as a government body or private company, can request and authenticate user credentials without **manual processing.**

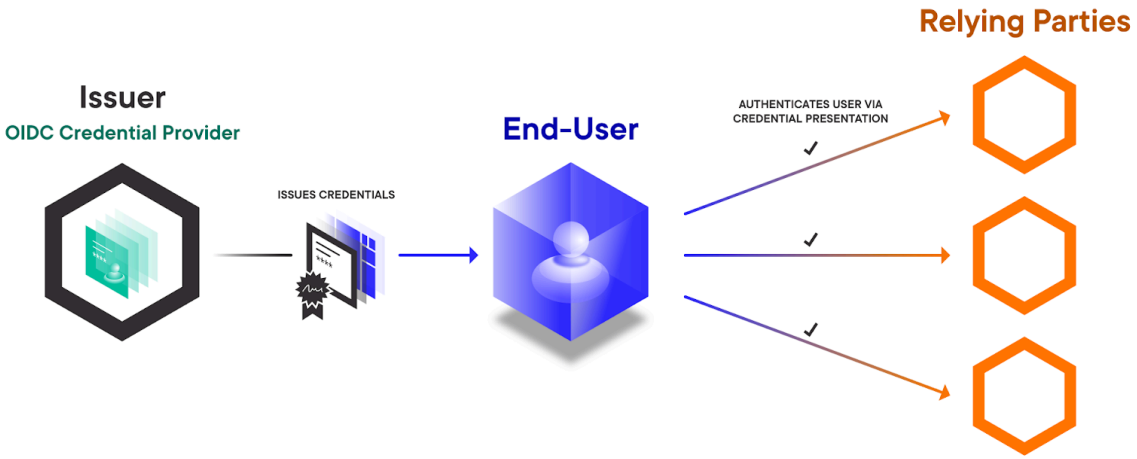


Figure 4: The Ecosystem of Decentralised Identities

Revocation lists

Revocation lists serve as a means for issuers to withdraw any type of issued credentials. The solution enables the use of W3C-based revocation lists to track and invalidate compromised or expired Verifiable Credentials.

Deployment

End-User Mobile Wallet (Frontend)

There are two ways to leverage verifiable credentials - an SDK integration with an existing mobile app or via a white-label version of the Partner wallet app, technology powered by iProov Identity.

Mobile Wallet App	Integration Method	Best For
Proprietary mobile app	SDK	An integrated experience managed by the organisation
Partner app	White-labelling	White-label deployment for faster time to revenue. iProov supports partners who offer End-user facing decentralised identity applications

Configuration with Business Application (Backend)

iProov Decentralised Identity connects with OpenID Connect (OIDC) as an Orchestration Service Provider (OSP) to enable organisations to adopt verifiable credentials without a line of code.

OpenID Connect (OIDC) is the open authentication protocol that allows individuals to authenticate their identity with credentials they hold with another provider. Each time users sign on to an application or service using OIDC, they're redirected to their OpenID Provider, where they authenticate and are then redirected back to the application or service.

By leveraging OIDC, iProov Decentralised Identity facilitates the integration of verifiable credentials into existing OIDC authentication flows for relying parties. With a simple configuration of required credentials and the addition of a QR code on their website (or a mobile button), organisations can seamlessly request and authenticate verifiable credentials within their authentication flows.

Differentiated Features

1. **Issue, update, or revoke Verifiable Credentials to mobile wallet apps like Partner App:**
    a. Issue Verifiable Credentials representing end user identity attributes in a secure and tamper-evident format.
    b. Store and manage Verifiable Credentials in mobile wallet apps like Partner App, ensuring easy access and control for end-users.
    c. Provide the ability to update or revoke Verifiable Credentials as needed.

2. **Secure, remote digital onboarding using facial biometrics:**
    a. Onboard end users remotely through digital channels using face biometrics for identity verification.
    b. Utilise advanced face liveness technology to ensure that the person onboarding is genuine and physically present.
    c. Provide an auditable record of all end users' onboarding.

3. **Remote identity proofing using ICAO-compliant government-issued documents:**
    a. Verify the identity of end users remotely using government-issued identity documents such as biometric passports, residence cards, or national identity cards, in line with UK Right to Work, Right to Rent, and DBS schemes.
    b. Extract the data from the cards using the mobile device’s built-in NFC reader.
    c. Validate the data with the issuing authorities' cryptographic keys.

4. **Risk-based multifactor cryptographic biometric authentication of end users:**
    a. Implement multifactor authentication using a combination of cryptographic and biometric factors to enhance security.
    b. Assess the risk level of each authentication attempt and adapt the authentication requirements accordingly.
    c. Provide a user-friendly and secure authentication experience.

5. **Re-verification of end users with secure real-world identity linkage:**
    a. Periodically re-verify the identity of end users by linking their digital identities to their physical identities through secure channels.
    b. Utilise a combination of biometrics, government-issued identity documents, and other verification methods to ensure accuracy of re-verification.
    c. Comply with regulatory requirements for ongoing identity verification.

6. **Privacy-preserving management of end-user identity credentials:**
    a. Manage end users' identity credentials in a privacy-preserving manner, ensuring that personal information is protected and used only for authorised purposes.
    b. Introduce a streamlined selective disclosure functionality for sharing identity information with Relying Parties.
    c. Comply with data protection regulations and best practices.

7. **Selective disclosure of cryptographically verifiable claims:**
    a. Allow end users to selectively disclose cryptographically verifiable claims about their identity without revealing unnecessary personal information.
    b. Utilise zero-knowledge proofs and other cryptographic techniques to ensure the privacy and integrity of disclosed claims.
    c. Empower individuals with control over their personal data.

8. **GDPR-consent management mechanism:**
    a. Provide a GDPR-compliant consent management mechanism that allows individuals to grant and manage their consent for the processing of personal data.
    b. Ensure greater transparency and control for individuals regarding the collection, use, and disclosure of their personal information.
    c. Comply with the requirements of the GDPR and other data protection regulations.

9. **Device-based attribute storage and management with AES-256 encryption:**
    a. Store and manage end-user attributes on the device in an encrypted format using AES-256 encryption.
    b. Utilise secure key management practices to protect the encryption keys.
    c. Ensure the integrity and confidentiality of end-users' attributes.

10. **Full compliance with OIDC for easy integration with Relying Parties:**
    a. Implement OpenID Connect (OIDC) compliance to enable seamless integration with Relying Parties that support OIDC.
    b. Provide a standardised and secure way for Relying Parties to authenticate end users and access their Verifiable Credentials.
    c. Simplify the integration process for Relying Parties.

Differentiated Benefits

1. **Certified to UK Digital Identity and Attributes Trust Framework:**
   The solution is certified against the UK Digital Identity and Attributes Trust Framework. It demonstrates iProov commitment to security, privacy, and interoperability.
2. **Reusability: Onboard once, and reuse many times:**
   Users can create a single digital identity that can be used across numerous applications and services, eliminating the need to undergo multiple onboarding processes.
3. **Privacy: Gives individuals greater control over their own data:**
   The solution provides individuals with granular control over their personal data, allowing them to choose what data they share and with whom.
4. **Fraud: Reduces rates of identity fraud including deepfakes:**
   The solution uses advanced biometric technology to prevent identity fraud, including deepfakes.
5. **Cost: Reduces the total cost of ownership managing constituents/employees:**
   The solution eliminates the need for physical identity cards and hardware-based tokens, reducing the cost of managing constituents and employees.
6. **Eliminate the use of passwords and costly hardware-based tokens:**
   Provides a more secure and convenient authentication method than passwords and hardware-based tokens.
7. **Simplifies the process of updating and revoking attributes and accreditations:**
   The solution provides an easy-to-use interface for updating and revoking attributes and accreditations.
8. **Auditable consent for data sharing to assist with GDPR compliance:**
   The solution provides auditable consent for data sharing, which assists organisations with GDPR compliance.
9. **Supports Passports, residence cards, and National IDs from 145 countries:**
   The solution supports passports, residence cards, and National IDs from 145 countries, making it an ideal solution for global organisations.
10. **Leverages smartphone NFC technology to read ICAO 9303 standard document:**
    The solution leverages smartphone NFC technology to read ICAO 9303 standard documents, making it easy for users to verify their identity.

Principles of iProov Digital Identities

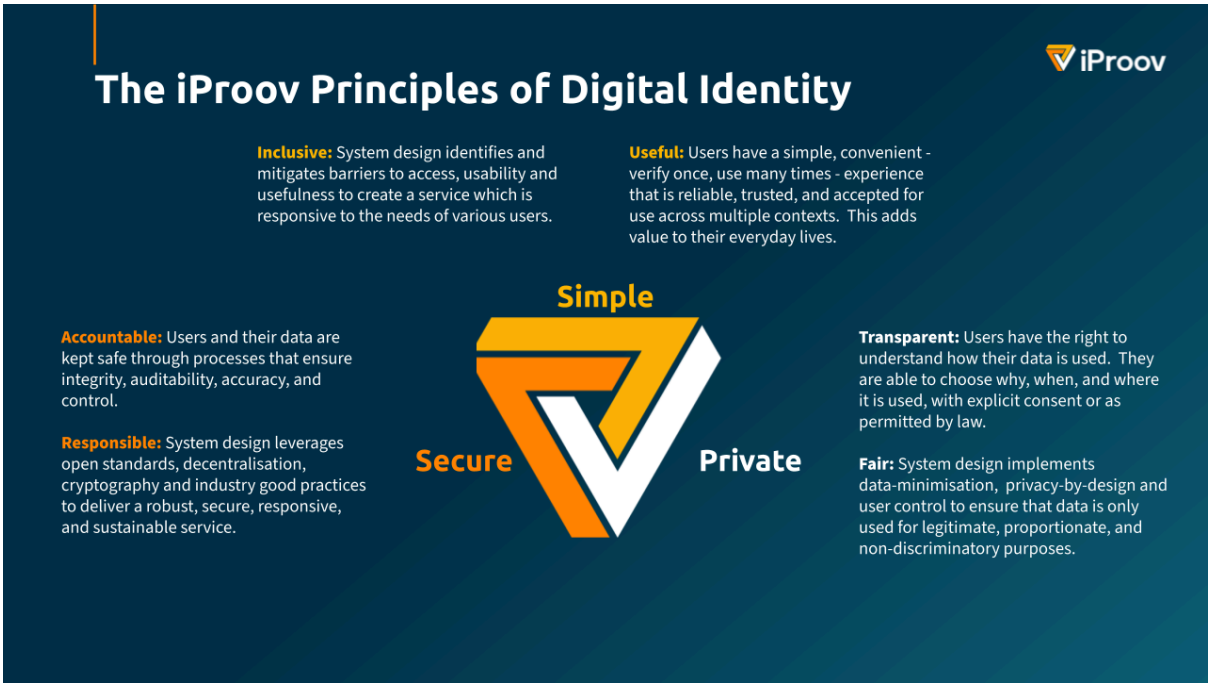


Figure 5: The iProov Principles of Digital Identity

Technical standards

iProov Decentralised Identity adheres to globally recognised standards. The table below offers a comprehensive overview of both established and emerging technologies currently supported or projected for support.

Component	Standard	Organisation
Data model	Verifiable Credentials Data Model v1.1	W3C
Authentication	Open ID Connect	OIDC
Issuer identifier	did:web	W3C
Subject/User identifier	did:key	W3C
Credential format	JSON-LD v1.1	W3C
Algorithms/signature	BBS+ / EdDSA (Ed25519) (Only P-256 supported in Secure Enclaves)	W3C
Revocation	Verifiable Credentials Status List v2021	W3C
Interoperability	Self Issued OpenID Provider (SIOPv2) OpenID4vP Presentation Exchange v1	OIDF
Trust	OpenID Federation OpenID for Identity Assurance	OIDF
Credential issuance	OID4VCI	W3C
Mobile Driver Licence	ISO/IEC DTS 18013-5	ISO
Mobile Driver Licence	ISO/IEC DTS 18013-7	ISO
Digital Identity wallet	EU-ARF	EU

Certifications and Audits

- **Digital Identity and Attributes Trust Framework (DIATF)**
- Conforms with **WCAG 2.2 AA and WCAG 2.1**
- **SOC 2 Type II, ISO 9001, CSA Star Attestation**
- Certified to **ISO/IEC 27001:2013** Information Security Management System
- iProov meets the biometric verification requirements of **NIST SP 800-63-4** through independent ISO-accredited testing and supporting certifications for accessibility, data privacy, and cybersecurity.
- Independently evaluated to **CEN/TS 18099** for injection attack detection by Ingenium Biometric Laboratories.
- **FIDO Face Verification Certification** affirming unparalleled defense against evolving threats throughout the entire identity lifecycle
- Complies with **GDPR (EU) 2016/679**
- **iBeta Level 1 and Level 2** tested, conforms with **ISO/IEC 30107-3** for Presentation Attack Detection
- Conforms with **ISO/IEC 19795-1:2006** for testing biometric verification performance, audited by the UK National Physical Laboratory (NPL)
- **eIDAS - conforms to EN 319-401 for Qualified Signatures**, certified by independent auditors including TÜV & Ernst & Young for conformance to **eIDAS Clause 24 1(d). Compliant with ETSI EN 319 401 and ETSI EN 319 411-1/2** to provide verification and authentication services as a Trust Service Service Provider to Qualified level for Modular Certification
- US DHS commissioned extensive testing by an external Red Team. Advanced techniques were employed to spoof the system, yet iProov effectively blocked them. “The iProov authentication process was robust against digital impersonation techniques.”
- Verified by the **UK, Singapore, and Australian Governments** as part of their National Due Diligence
- Complies with **iRAP** (Information Security Registered Assessor Program) and **IP3** (Identity proofing level three) in Australia
- Production deployments of **W3C Verifiable Credentials & ISO/IEC 18013-5 mDL**