IMWallet

Un ecosistema volto alla gestione di identità digitali distribuite nella forma di Self Sovereign Identity (SSI), per abilitare Trust Service Providers italiani ed europei all'emissione di nuovi servizi a valore aggiunto.

Powered by
Ethlabora S.r.l.

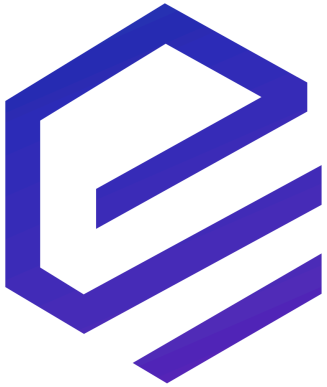


Table of contents

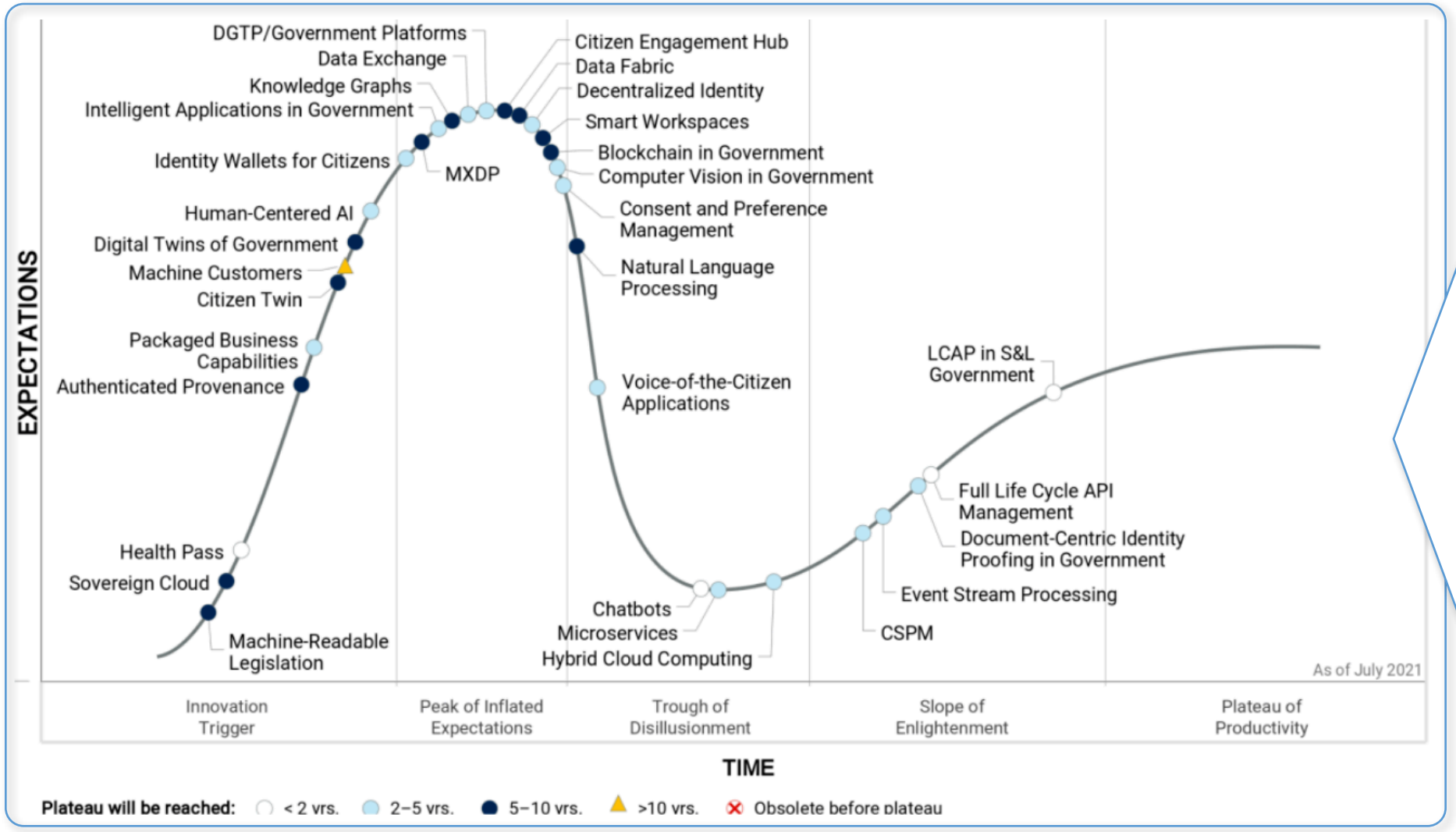
OVERVIEW

Come forma di **Self Sovereign Identity (SSI)**, IMWallet consente un controllo esplicito sulla creazione e gestione dell'identità e certificati digitali per far fronte alle nuove esigenze del mercato italiano ed europeo, assicurando la compliance con l'ultima proposta di modifica del regolamento eIDAS, apparentemente sostenuta dalla maggioranza degli stati membri aderenti al nodo eIDAS.

IMWallet mira a creare un ecosistema di Self Sovereign Identity (SSI) basato sulla tecnologia **IOTA** ed un **identity wallet** fruibile grazie ad un'app mobile associata, che sia in grado di gestire il **ciclo di vita completo** di un'identità digitale e certificati digitali dalla **creazione** alla **verifica**, con opzioni avanzate di **gestione** e **revoca.**

IMWallet permette ad un utente di ottenere **"credenziali verificabili"** in aggiunta alla propria identità digitale, come un certificato che attesta il possesso della licenza di guida, o i proprio titolo di studio.

GARTNER HYPE CYCLE



- il paradigma relativo a **Decentralized identities (self Sovereign identity)** è in una fase di transizione tra PoC sperimentali e lo sviluppo di robuste soluzioni istituzionali, raggiunte dai 2 a 5 anni.

- La distribuzione di un **Identity Wallet** in versione Mobile per i cittadini europei sarà raggiunta tra i 2 a 5 anni.

CONTESTO EUROPEO

Il 3 giugno 2021 la Commissione europea ha diffuso una proposta di revisione del regolamento eIDAS per stabilire un quadro comunitario che supporti un'Identità Digital europea, insieme a un documento di raccomandazioni per lo sviluppo di un nuovo Digital Wallet paneuropeo.
Nella proposta emergono nuovi servizi a valore aggiunto che potranno essere erogati autorità accreditate all'interno degli stati membri, tra cui **un nuovo servizio fiduciario di gestione dei registri distribuiti qualificati**.

I registri elettronici qualificati soddisfano i requisiti seguenti:

DISPOSIZIONI SUGLI STANDARD IMPIEGATI

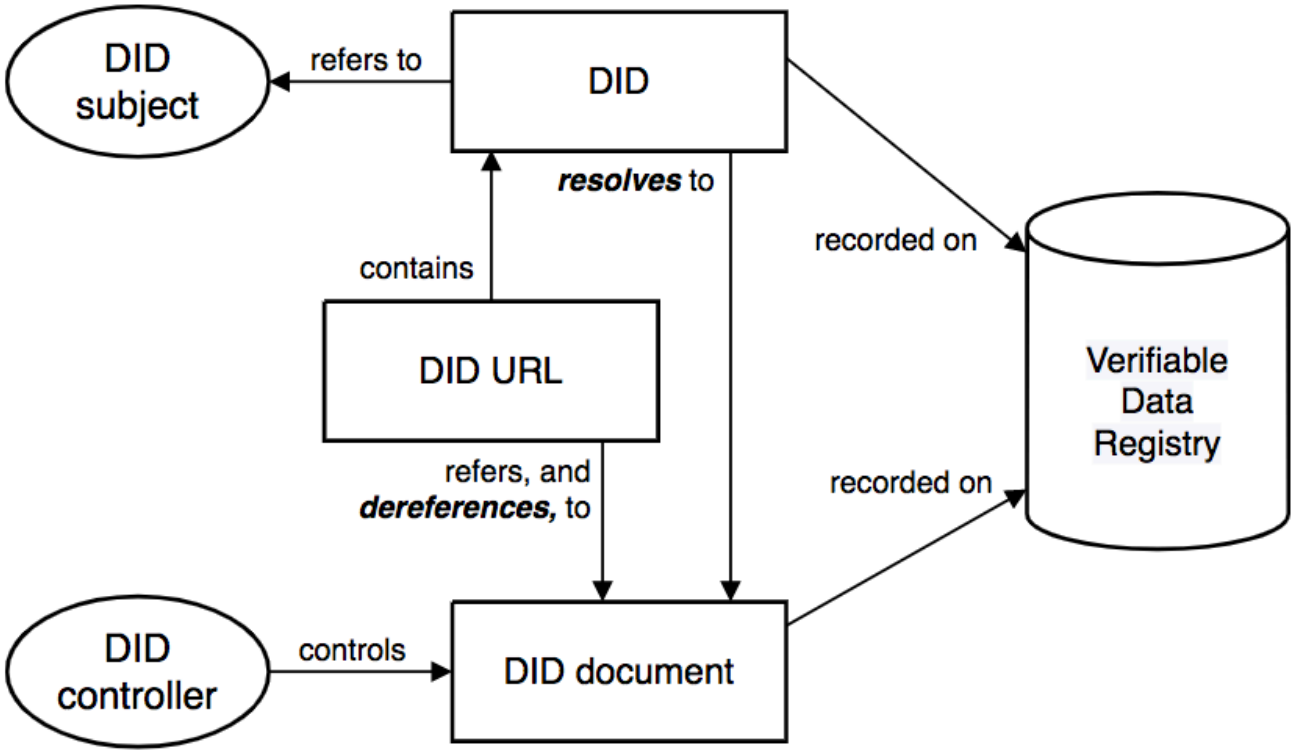
Basandosi sugli standard proposti dal W3C Community Group per gli identificatori decentralizzati (DID) e Credenziali verificabili, l'Unified Identity Protocol della IOTA Foundation consente a persone ed organizzazioni di identificarsi online. Con questo sistema, gli utenti potranno dimostrare che le loro informazioni vengono verificate e approvate da terze parti attendibili e vengono condivise in modo peer-to-peer, incrementando sia la privacy che la fiducia. Le transazioni di dati possono ora avere fonte identificabile, assicurando fiducia sulla provenienza delle transazioni.

Il protocollo è costruito con *"Data protection and Privacy by design*" ed è conforme alle leggi sulla privacy e sulla gestione dei dati in tutto il mondo, come il Regolamento generale europeo sulla protezione dei dati (GDPR).

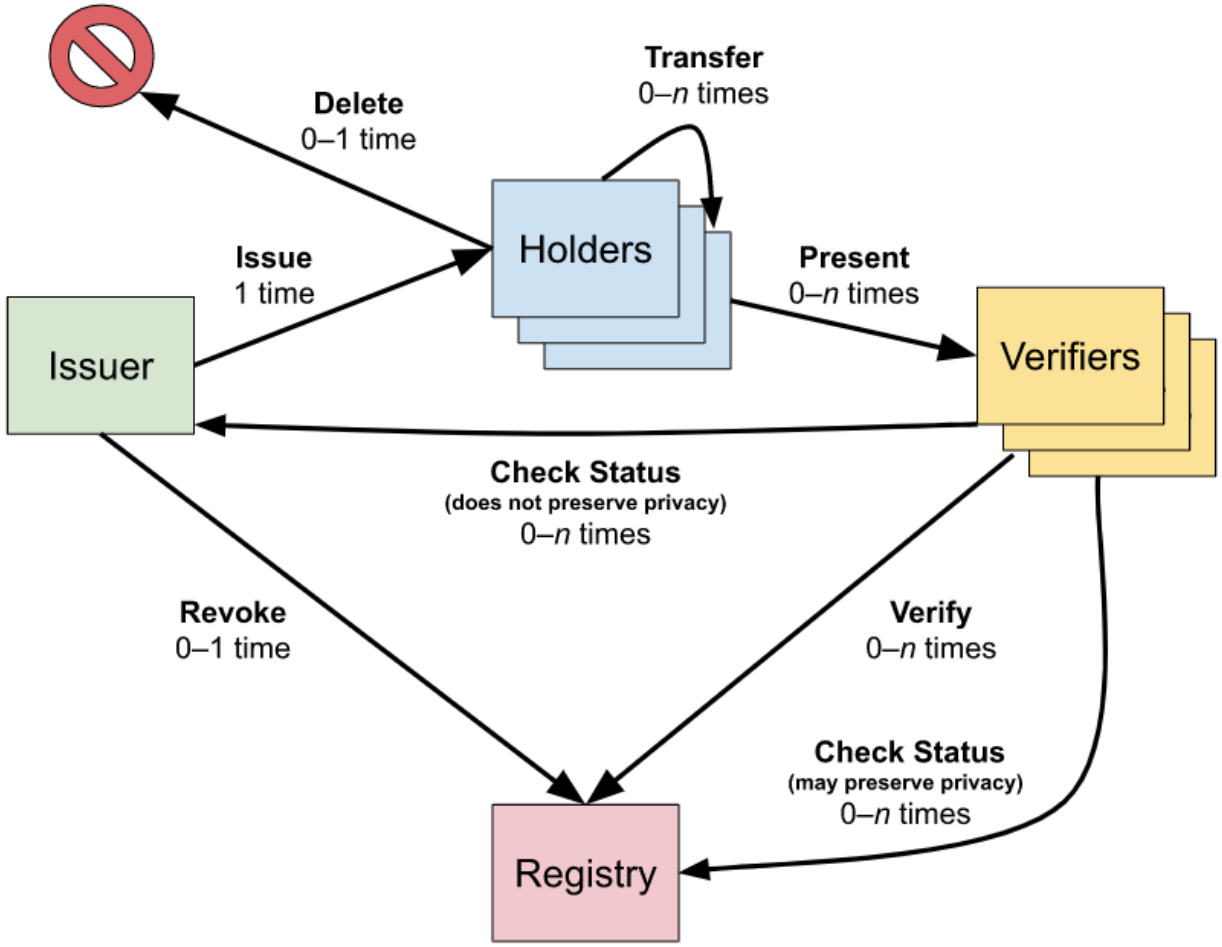
DISPOSIZIONI SUGLI STANDARD IMPIEGATI

Utilizzando Unified Identity Protocol (UIP) come implementazione dell'identità digitale su IOTA, una nuova identità digitale può essere creata da chiunque o da qualsiasi cosa in qualsiasi momento. A tal fine, viene generato un DID (Decentralized Identifier), che funge da riferimento a un documento DID (DDO). Il documento DID (DDO) contiene chiavi pubbliche e altri meccanismi per consentire al soggetto di dimostrare la propria associazione con il DID. Tuttavia, un DID da solo ti dice poco sull'argomento. Deve essere combinato con credenziali verificabili. Le credenziali verificabili sono dichiarazioni sul creatore del DID. Possono essere condivisi e verificati online in modo BYOI e il creatore DID mantiene il controllo completo del processo.

ARCHITETTURA DECENTRALIZED IDENTIFIER (DID)



IL CICLO DI VITA DI UNA CREDENZIALE VERIFICABILE



TECNOLOGIE IMPIEGATE

IOTA's Tangle

La tecnologia Tangle di IOTA verrà impiegata all'interno del processo per le seguenti funzionalità:

- **Public Key Registry:** Tangle abilita un decentralized public keys registry per gli emittenti utilizzando gli standard *DID*. Ciò consente ai verificatori di verificare una firma senza fare affidamento su un file server centralizzato. Lo standard DID aggiunge anche endpoint di servizio, estendendone l'usabilità di identità oltre a un public keys registry, ad esempio per registrare credenziali verificabili standard.

- **Revocation:** Una credenziale verificabile può essere revocata, il che significa che non sarà più in grado di superare una verifica.
La revoca è immutabilmente memorizzata sul Tangle, assicurando che nessun beneficiario utilizzi le proprie credenziali revocate.

LA TECNOLOGIA IOTA

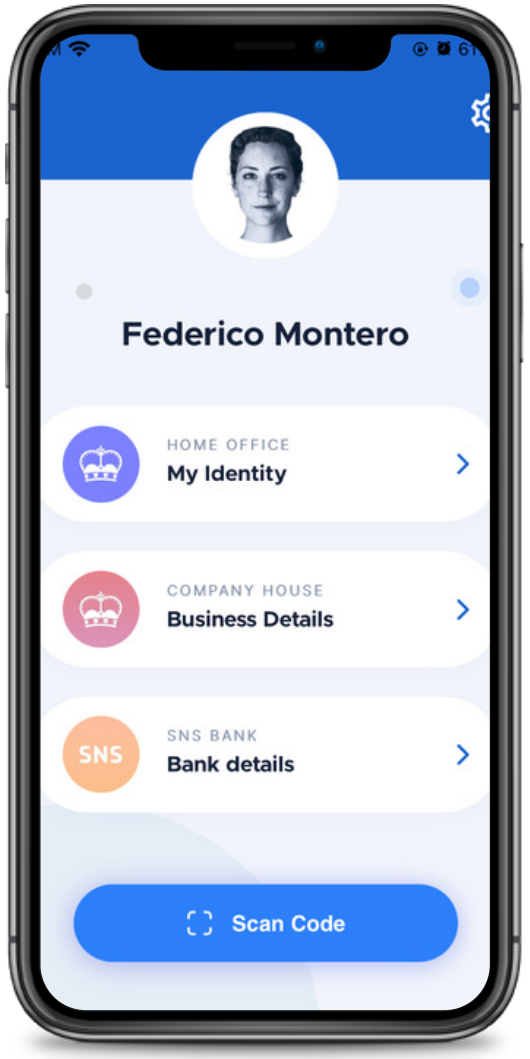
IOTA è una Distribuited Ledger Technology (DLT) unica nel suo genere. La configurazione della rete segue uno schema rivoluzionario nell'ambiente blockchain, offrendo prestazioni straordinarie e framework all'avanguardia, accontentando elevati standard di sicurezza.

IOTA's Tangle

- Nessuna commissione
- Alta scalabilità
- Nessuna attività di mining
- Trasmissione sicura del dato
- Quantum proof

TECNOLOGIE IMPIEGATE

IOTA's Selv



- L'app mobile IOTA SELV utilizza una combinazione di crittografia e DLT che permette di creare un framework per generare e validare credenziali digitali per dati bancari, sanitari e identità personale.

Le credenziali di un individuo vengono archiviate localmente sul proprio dispositivo, consentendo a terze autorità di validarle in modo sicuro.

USE CASES

CONDIVIDERE INFORMAZIONI SANITARIE

IMWAllet permette di collezionare e trasferire il proprio certificato medico e record vaccinale

CONDIVIDERE CV E QUALIFICHE

IMWAllet permette di collezionare e traferire certificati scolastici ed accademici

IDENTIFICARE CLIENTI ONLINE

IMWAllet permette di autenticare un utente online e le relative informazioni (es. età, indirizzo, luogo di nascita)

SERVIZI BANCARI

IMWAllet semplifica il processo di KYC e facilita il trasferimento dei dati sensibili tra istituti bancari internamente o esternamente

I TRE ATTORI DEL PROCESSO

Il processo prevede tre attori:

- **Beneficiario** – Rappresenta il soggetto richiedente e possessore dell'identità digitale.
I propri dati personali e le chiavi private sono sotto il suo controllo.

- **Emittente** – Rappresenta il soggetto fidato che provvede al rilascio del certificato firmato digitalmente al Beneficiario.

- **Validatore** – Un Beneficiario condivide il proprio certificato con un Validatore per dimostrare una dichiarazione su se stesso. Il Validatore è in grado di verificare la validità del certificato eseguendo le seguenti operazioni:

- Data Integrity: *Il certificato è firmato dalle parti previste?*
- Issuer Trust: *Il certificato è inalterato?*
- Signature Verification: *Considero attendibile che l'emittente fornisca questo certificato?*
- Validation: *Il certificato è ancora valido?*

I TRE ATTORI DEL PROCESSO

CREARE UN'IDENTITÀ DIGITALE

Il processo di creazione di un'identità digitale è strutturato nel seguente ordine:

1) Quando un beneficiario richiede una credenziale, si identifica presso l'emittente loggandosi e compilando un form all'interno dell'app.

2) Il beneficiario condivide il proprio DID con l'emittente e ne richiede la credenziale.

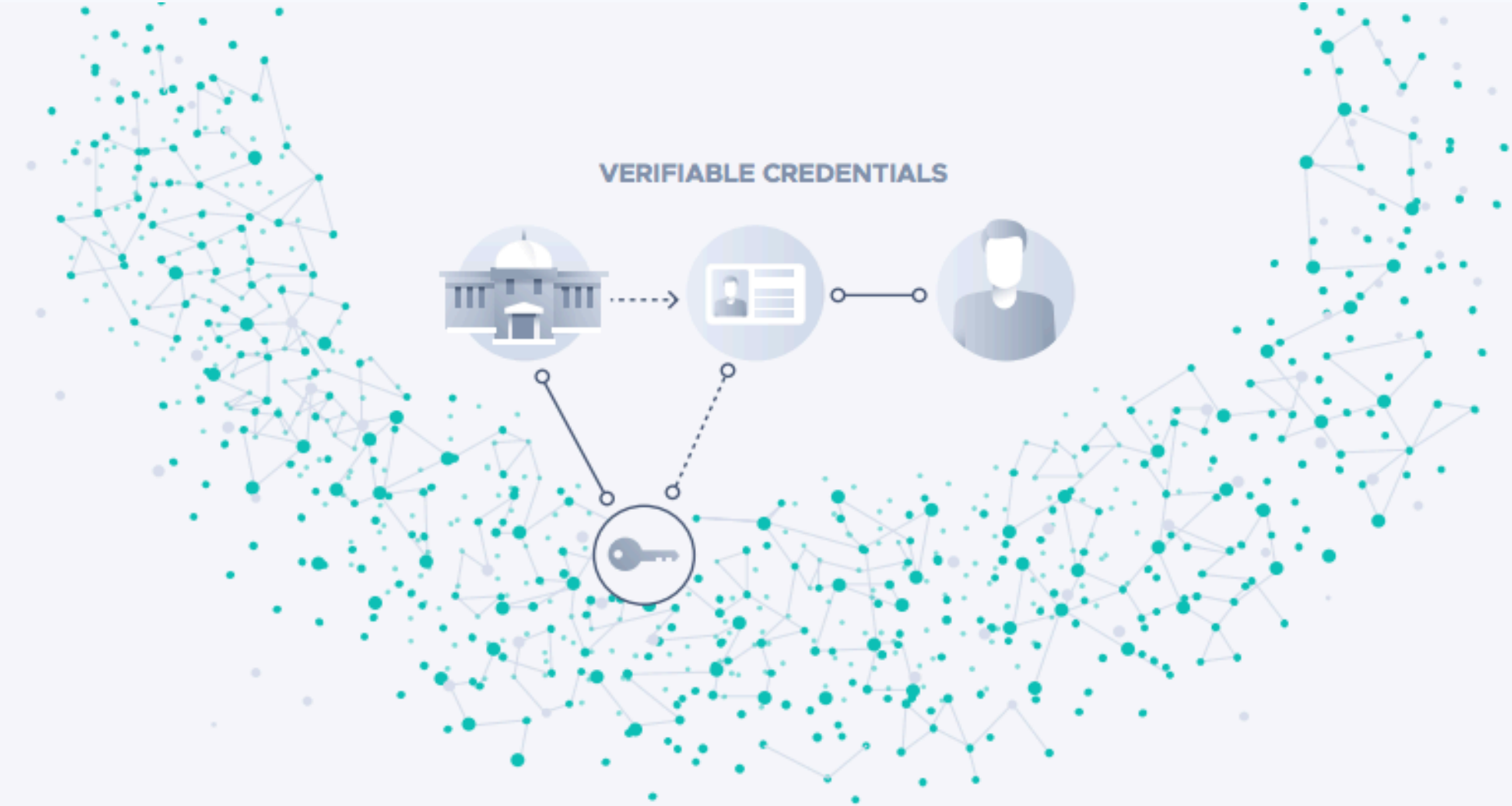
3) L'emittente firma le credenziali e le dichiarazioni allegate relative al beneficiario con una coppia di chiavi crittografiche registrate nel proprio Documento DID.

4) La credenziale viene quindi inviata al beneficiario e conservata.

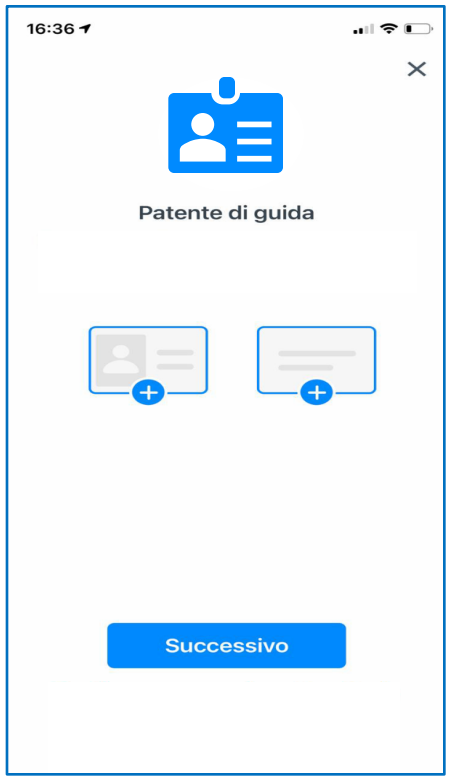
5) Il beneficiario ha ora completa autonomia su come utilizza questa credenziale.

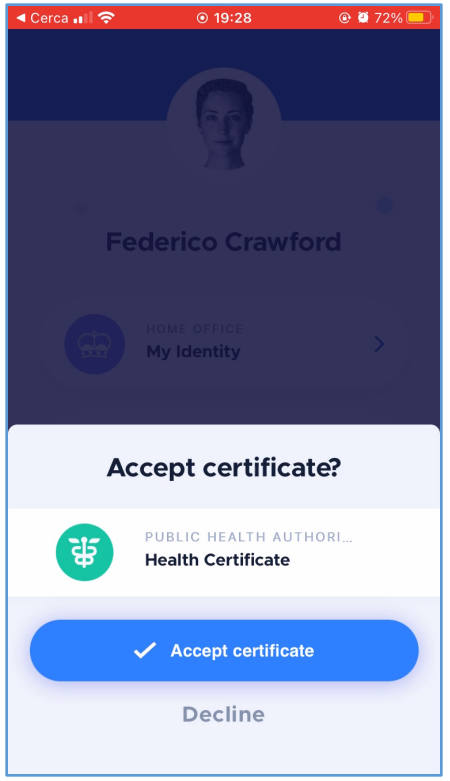
6) L'emittente può successivamente revocare la credenziale, facendo fallire eventuali futuri tentativi da parte del Titolare di utilizzare la credenziale.

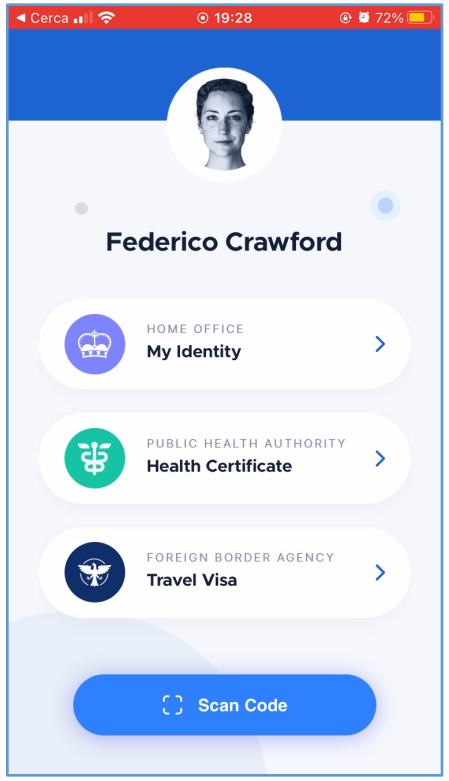
CREARE UN'IDENTITÀ DIGITALE



CREARE UN'IDENTITÀ DIGITALE







USARE UN'IDENTITÀ DIGITALE

Questo processo garantisce che l'emittente sia attendibile, abbia firmato i dati e che i dati non siano stati alterati dopo il processo di firma.

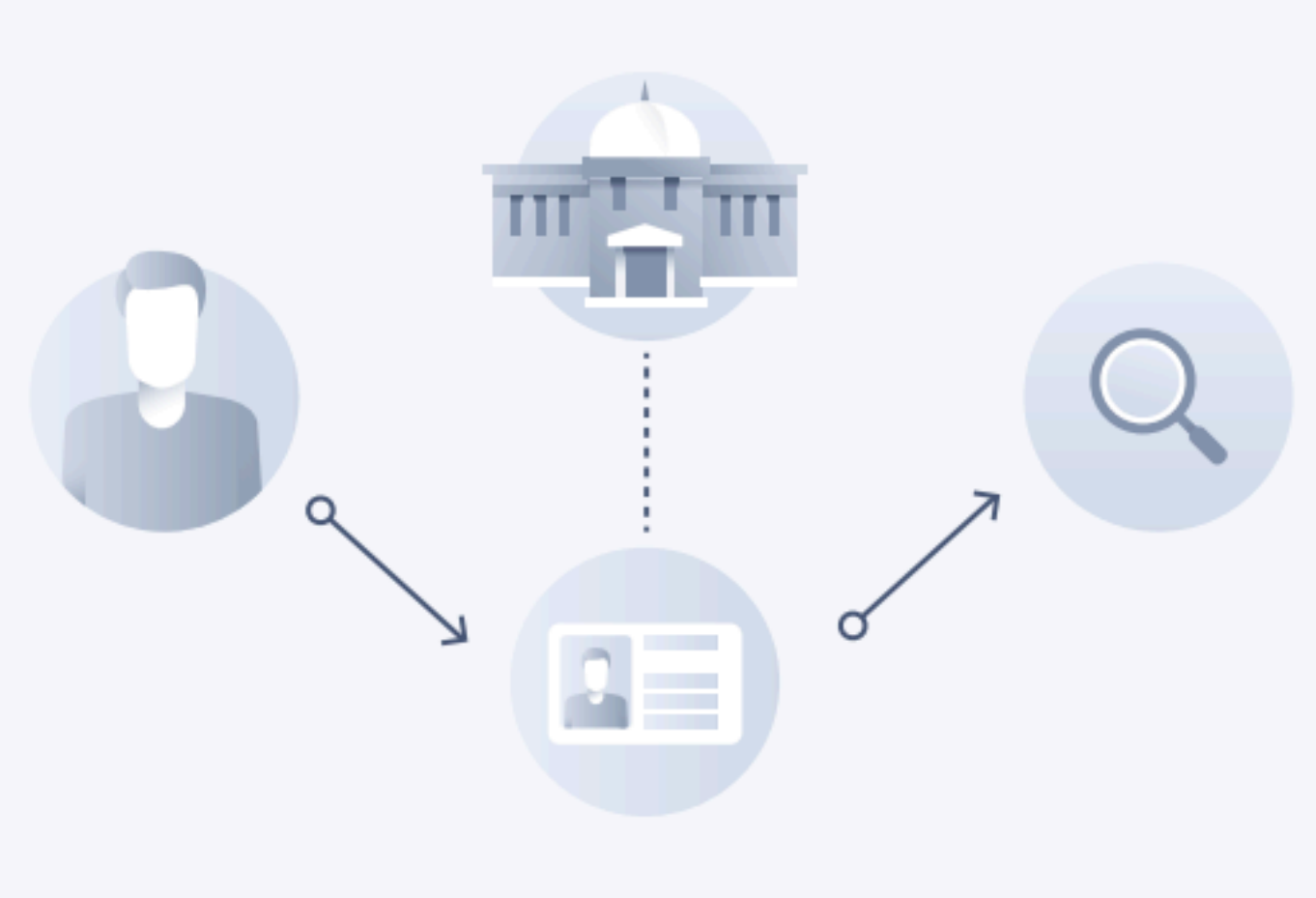
Il processo di impiego di un'identità digitale è strutturato nel seguente ordine:

1) Quando un validatore ha bisogno di conoscere determinate informazioni sul titolare, il beneficiario può scegliere di inviare al validatore attributi specifici.

2) Il validatore ora ha una copia delle informazioni e dei dettagli di cui l'Emittente ha firmato la credenziale.

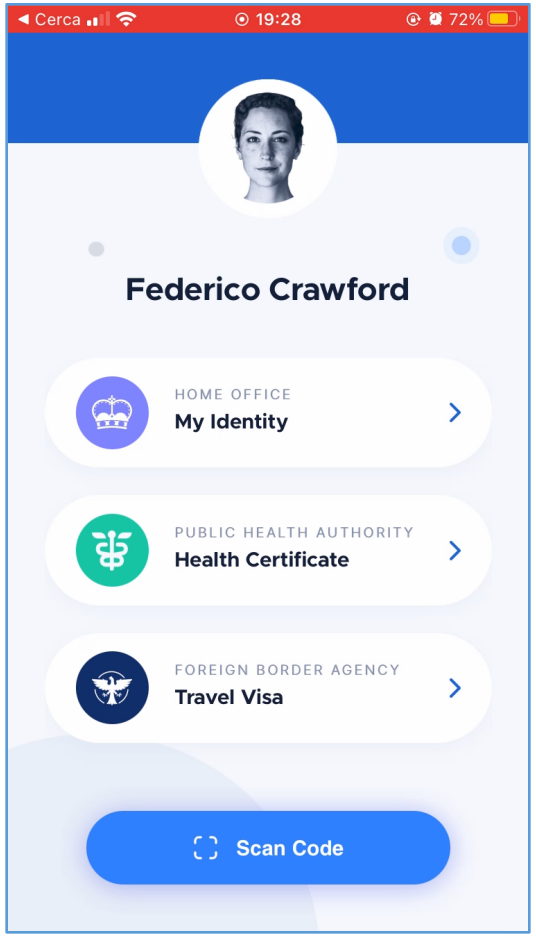
3) Il validatore decide quindi se si fida dell'emittente della credenziale e verifica la loro firma sul Tangle.

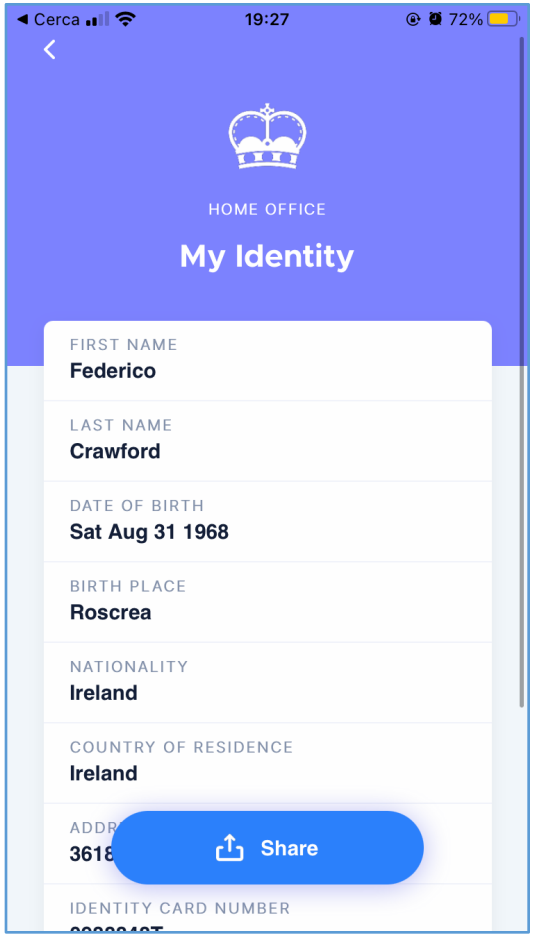
USARE UN'IDENTITÀ DIGITALE

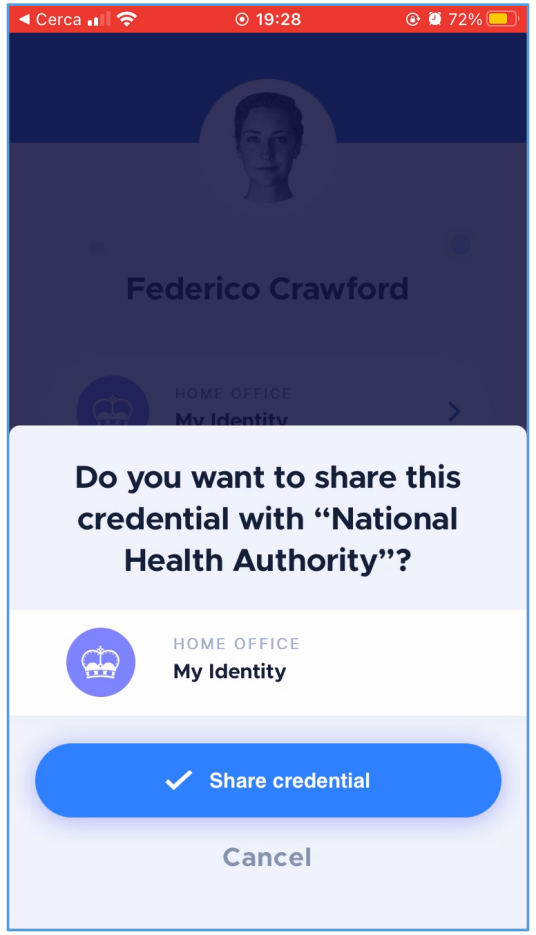


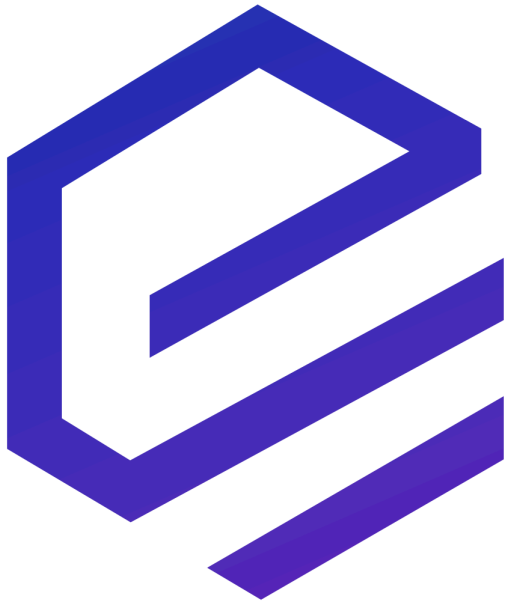
USARE UN'IDENTITÀ DIGITALE

Selv









GRAZIE DELL'ATTENZIONE

Email: federico.grilli@ethlabora.com

Cell: +39 3314652876

Ethlabora S.r.l.
Codice fiscale: 15534021009

Roma Head Office:
Via Marco e Marcelliano, 45 - 00147