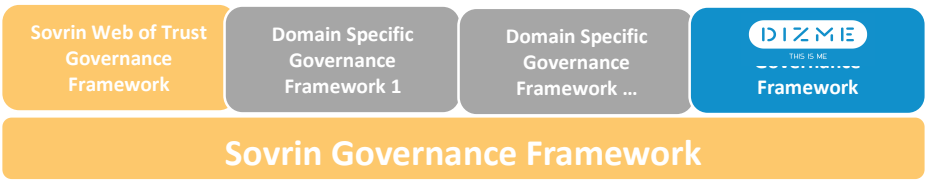
InfoCert S.p.A.

1. Il problema

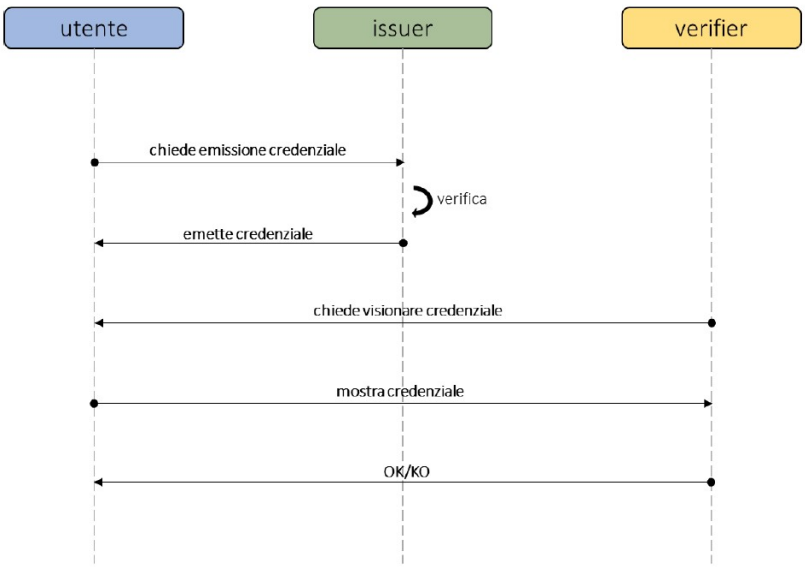
L'identità digitale è uno dei problemi più antichi e più difficili del web. Non c'è ancora modo di usare le credenziali digitali per dimostrare la nostra identità online al pari di come avviene nel mondo fisico.
Questo aspetto è diventato di fondamentale importanza in un contesto in cui l'identificazione *de visu* era preclusa, se non impossibile: la procedura concorsuale per il fallimento di una piattaforma di exchange di cripto-valute.
Una volta incardinatosi il procedimento di fronte l'autorità giudiziaria italiana, la legge applicabile sancisce l'obbligo di identificazione certa dei creditori che si volessero insinuare al passivo.
In questo senso, la curatela ha manifestato la necessità di implementare una soluzione che rendesse possibile l'identificazione dei circa 80.000 creditori, potenzialmente in ogni parte del globo.

2. La soluzione tecnologica

La tecnologia blockchain si pone come traghettatore verso un nuovo modello di identità digitale distribuita e non più nel controllo di pochi grandi fornitori di servizi.
InfoCert svolge un ruolo attivo nella promozione della visione *self-sovereign* sottoscrivendo il programma Sovrin Founding Steward e implementando **DIZME**, un Domain Specific Framework che estende i principi e le definizioni del Sovrin Framework sottostante.



Dal punto di vista tecnologico, DIZME è una piattaforma digitale progettata da InfoCert ma aperta - per una partecipazione attiva - a tutte le parti che desiderano abbracciare la visione di SSI e accelerare il loro percorso di trasformazione digitale. All'interno di DIZME è stata sviluppa la DIZMEwallet APP che è in grado di fornire all'Utente lo strumento tecnologico per gestire le proprie credenziali.
In particolare, DIZME prevede l'emissione di credenziali di identità volte a garantire – attraverso diversi standard tecnologici – la verifica digitale dell'identità fisica dell'utente. In particolare, il flusso di emissione e verifica può essere così descritto:



I ruoli di ciascun attore sono i seguenti:
a) Issuer, il soggetto che rilascia una Credenziale ad un Utente.
b) Utente, il soggetto a cui è stata rilasciata una credenziale a seguito di una procedura di verifica.
c) Verifier, soggetto che verifica la credenziale contenuta nel wallet dell'Utente. In questa fase, l'Utente stesso fornisce una prova (proof) della propria identità, attraverso la credenziale stessa.

2.1 Flusso di verifica dell'identità per il fallimento Bitgrail

Per il fallimento BitGrail la verifica dell'identità dell'Utente avviene secondo diversi gradi di fiducia (c.d. Level of Assurance LoA) a cui corrispondono quattro diversi livelli di sicurezza:

a) ***Self Identification***: identità auto dichiarata, arricchita dalla presenza fisica, Liveness detection. (Issuer 1)
   L'utente conferma il proprio indirizzo email con un codice OTP ricevuto sulla mail dichiarata e gira un breve video selfie.
b) ***Identity Proofing***: *Self Identification* e verifica delle foto dell'Utente attraverso strumenti di face matching. (Issuer 1)
   L'utente aggiunge una foto del proprio documento di identità in cui sia presente una foto del volto. Le due foto sono confrontate.
c) ***Document Proofing***: *Identity Proofing* e verifica del documento attraverso strumenti di Document recognition. (Issuer 2)
   In questa fase sono verificati i dati identificativi riportati sul documento.
d) ***Video Identification***: *Identity Proofing* e verifica attraverso un video sincrono con Operatore. (Issuer2)
   L'utente effettua una video-sessione di riconoscimento con un operatore.

In questo contesto, i ruoli della piattaforma DIZME sono così ripartiti:
a) Issuer 1: DIZMEwallet.
b) Issuer 2: InfoCert.
c) Verifier: Curatela fallimentare.

Il processo di verifica dell'identità dell'utente inizia con l'invio all'utente da parte della curatela una mail contenente le indicazioni per scaricare il DIZMEwallet e proseguire con gli step -di cui sopra- proposti per l'identificazione, facendo di volta in volta l'"upgrade" delle proprie credenziali fino ad ottenere il livello con il massimo grado di fiducia (lett. d).

2.2 Accesso alla piattaforma

Terminato il processo di verifica dell'identità, l'Utente si collega alla piattaforma della Curatela, spende le proprie credenziali e condivide i propri documenti d'identità, a seconda del livello di sicurezza richiesto dal Verifier.

3. Elementi distintivi del progetto e benefici raggiunti dal cliente

Il progetto ha visto una fase di definizione dei requisiti negli ultimi mesi del 2019, poi lo sviluppo e il lancio nel gennaio 2020 e infine la prima udienza di comparizione si terrà a giugno 2020.

Il caso è senz'altro unico nel suo genere: poter identificare in maniera certa utenti in ogni parte del mondo per consentirgli l'esercizio di un diritto in un luogo probabilmente lontano dalla propria sfera di interessi è rivoluzionario e allo stesso tempo necessario. Non era mai stato applicato questo paradigma in un contesto di procedura fallimentare.

Il mondo della DLT (distributed ledger technology) si sta certamente affacciando a casi d'uso molto più eterogenei rispetto alla generazione di cripto valute (la tecnologia è divenuta nota con l'esplosione di Bitcoin): il tema dell'identità è centrale e InfoCert stessa ha lanciato l'applicazione di questa tecnologia al servizio di problematiche come la necessità di provare una qualifica o l'appartenenza ad una organizzazione, arricchite da una informazione sullo stato di salute (come la temperatura corporea entro una certa soglia) in un certo luogo e in un certo momento. Quest'ultima implementazione è indubbiamente frutto di una esigenza attuale e impellente come la possibilità di garantire l'accesso a luoghi pubblici o di lavoro in sicurezza.