



Realizzato per HACKATHON_THIS IS ME 2021

Ideato da BLOC LawTech Firm

Roma - Reggio Emilia, 13 Aprile 2021

RESUME

Scopo

Conciliare i principi di autodeterminazione e riconoscimento univoco dell'individuo alla spendita delle informazioni sanitarie.

Obiettivo

Il progetto SONO SANO si pone l'obiettivo di realizzare una soluzione tecnologica conforme alla normativa vigente a sostegno dell'autodeterminazione e riconoscimento univoco dell'individuo, in particolare tramite un wallet digitale individuale che racchiuda le credenziali personali in forma autocertificata e le credenziali verificabili (verified credentials) che vengono fornite dai Trusted Service Provider.

Soluzione

Utilizzo della tecnologia blockchain per la creazione di un wallet univoco personale contenente pass vaccinale

Struttura del progetto

1. Self Sovereign Identity ed ambito di applicazione
 - 1.1 Quando si può parlare di Self-Sovereign Identity?
 - 1.2 Pain point allo stato dell'arte
 - 1.3 Cambio di rotta: inversione dei soggetti
 - 1.4 Autodeterminazione: dai principi universali all'autocertificazione amministrativa
2. Progetto Sono Sano
 - 2.1 SSI assoluta
 - 2.2 Soluzione Sono Sano (SSI ibrida)
3. Lo Use Case del Pass Vaccinale SONOSANO per l'Hackathon: proposta generale

4. I dati forniti dal soggetto (ciò che posso dire di me) - la cristallizzazione con NFT del dato personale autocertificato dichiarato dal soggetto per la creazione delle proprie verificable credentials
5. I dati forniti dal TSP
 - 5.1 I dati sanitari: certificato vaccinale + esito del test
6. La sintesi: wallet e token
 - 6.1 il token misto non fungibile e fungibile ERC - 1155
 - 6.2 Dati univoci dell’NFT connessi ai dati interagenti provenienti dall’esterno utilizzando ERC -1155
 - 6.3 Il wallet
7. SONOSANO: criticità
8. Conclusioni

1. Self Sovereign Identity (SSI) ed ambito di applicazione

La sfida di conciliare la necessità di **autodeterminazione** dell'individuo e la capacità dello stesso di mantenere intatta ed immutata la sua **identità** e **riconoscibilità** nel contesto sociale in cui vive è un tema attuale in considerazione dello sviluppo tecnologico e delle contingenze storiche.

La pandemia COVID -19 ha reso più che mai urgente individuare soluzioni che possano consentire all’individuo di disporre delle proprie credenziali identificative in modo autonomo, ma anche di attribuirsele in proprio, senza dover accedere ai servizi di terzi trusted.

E’ un cambio di paradigma necessario per rendere realmente accessibili i molteplici servizi della società dell’informazione nei settori più disparati, tra cui anche quello sanitario di cui ci occuperemo in via esclusiva. Occorre operare in un’ottica di semplificazione e visione congiunta di utilizzo degli strumenti tecnologici a disposizione in uno con il coordinamento normativo rispetto framework frammentario ove esistente e in rapidissima evoluzione.

1.1. Quando si può parlare di Self-Sovereign Identity?

In primo luogo nel momento in cui una persona fisica può determinare autonomamente la propria identità, senza l’intermediazione di un terzo accreditato, dunque esercitando in modo esclusivo ed autonomo il potere di attribuirsi l’identità propria. In secondo luogo quando la persona fisica possiede, può dimostrare e “spendere” detta identità, scegliendo se consentire l’accesso o l’interazione di altri soggetti ai dati ed informazioni che lo qualificano. La sintesi è un’identità “portatile” e dinamica che può essere inequivocabilmente associata a credenziali riconosciute e validate dal soggetto stesso.

Il principio che guida questa tesi consiste nell’ auto attribuzione delle credenziali che identificano la propria persona - una sorta di autocertificazione - per consentire al soggetto di autodeterminarsi con elementi identificativi di sé, come il nome e cognome.

Il punto non è la mera assegnazione a se stessi degli attributi identificativi (ad es. il nome), ma l'opponibilità dell'attribuzione nei confronti di terzi, per dimostrare a chiunque ed in ogni condizione di essere l'effettivo titolare della qualità soggettiva (nell'es. il nome) che ci si è attribuita autonomamente. Viene in rilievo il primo elemento distintivo di una SSI: l'univocità delle credenziali attribuitesi e la loro immutabilità. E' evidente che in un sistema così pensato si richiede che le informazioni identificative del soggetto univocamente determinato non possano essere modificabili né corruttibili.

Ecco dunque che l'utilizzo di un sistema basato su un protocollo blockchain può risolvere questo primo punto, consentendo la creazione di una SSI che si svincoli dal concetto di intermediazione quale garanzia delle informazioni immesse.

È l'issuer stesso a trascrivere i propri attributi identificativi su blockchain, sfruttandone le potenzialità in termini di data certa (time stamping), immodificabilità (hashing) e sicurezza di verifica di ogni transazione relativa ai quel dato. Inoltre, sempre l'issuer, a mezzo della propria chiave privata, può accedere in via esclusiva al dato a lui riconducibile ed utilizzarlo a sua discrezione, senza dover avviare procedure difficoltose, né rischiare di perderne la disponibilità in quanto detto dato è a lui univocamente riconducibile senza limitazioni.

1.2 Pain Point

Attualmente lato legale, non è prevista la possibilità di generare un'identità digitale senza fare affidamento ad un provider accreditato e rispondente a determinate caratteristiche.

Se, per iperbole, il provider cessasse di esistere seguirebbero la sua fine anche le identità digitali ad esso collegate, un po' come se il registro anagrafe andasse in fumo.

Citando Ferdous: *“questo sconfigge tutte le proprietà fondamentali di un'identità auto-sovrana, come l'esistenza, l'autonomia, la proprietà e l'accesso, e il principio che l'utente e solo l'utente, deve avere il pieno controllo sui propri dati di identità in una struttura di gestione dei dati controllata dallo stesso”*. Pertanto occorre un cambio di rotta che inverta il processo che vede le identità calate dall'alto e ponga il soggetto trusted al servizio della persona fisica unica sovrana della propria identità.

1.3 Cambio di rotta: inversione dei soggetti

Citando Wagner: *“lo scenario attuale di gestione dell'identità tradizionale è quello in cui l'identità di un soggetto/utente del servizio è definita **dal punto di vista del provider per uno scopo specifico**”*. Le persone possiedono (forse) ed utilizzano i tipi di identità conferite loro in varie forme (carte d'identità, passaporti, etc) e da diverse terze parti, che operano come fonti di autorità (ad esempio, enti credenziali o TSP).

Nessuna di queste forme può screditare il fatto che gli individui sono la fonte unica di dati concernenti se stessi: l'identità di un cittadino preesiste prima del conferimento di un'identità da parte di terzi.

In un ecosistema autosufficiente, le persone fisiche dovrebbero essere in grado di

controllare ogni aspetto delle proprie credenziali: rilascio, verifica, accettazione, archiviazione, scambio. Ogni persona fisica dovrebbe quindi possedere, gestire e scegliere se condividere le proprie credenziali e in che misura (in tutto o in parte) senza la necessità di ricorrere costantemente a terze parti intermedie e garanti che convalidino l'identità.

In un contesto di applicazione di Self Sovereign Identity gli individui certificano la propria identità sovvertendo il concetto di fiducia.

Se in un sistema di fiducia tradizione, diciamo "pubblico" i dati sono certificati da un terzo riconosciuto e generano un legittimo affidamento nel contesto in cui operano; in un sistema di fiducia "di matrice privata", i dati della persona fisica vengono generati dall'individuo che dovrebbe poterne disporre in autonomia. Tuttavia oggi la persona fisica non può generare automaticamente le proprie credenziali ma si deve rivolgere ad un TSP, il quale conferisce la sola gestione esclusiva in capo ad esso, una mera "self governable identity", senza possibilità di auto attribuzione delle credenziali.

In un contesto di applicazione di Self Sovereign Identity gli individui certificano la propria identità sovvertendo il concetto di quadro di fiducia pubblico in quello di fiducia privata, utilizzando il TSP solo per l'utilizzo delle stesse in una sorta di self governable identity.

Questo è il presupposto del progetto SONOSANO, supportato dal protocollo blockchain.

1.4 Autodeterminazione: da principi universali all' autocertificazione amministrativa

Chi sono io? Chi sono io per dire che io sono io? Il principio di "autodeterminazione" ricomprende i diritti fondamentali dell'uomo: il diritto al riconoscimento di sé come individuo, l'espressione del proprio libero arbitrio, la capacità di assumere decisioni e responsabilità in capo alle proprie azioni. L'affermazione del sé e il riconoscimento giuridico di tale principio trova espressione nel diritto naturale ed in particolare modo nei principi costituzionali. In particolare in Italia il Decreto del Presidente della Repubblica n. 445 del 2000 stabilisce i parametri di riferimento in materia di "espressione del sé" all'interno degli atti amministrativi. La Pubblica Amministrazione regola i rapporti con il cittadino, ponendosi come autorità naturalmente preposta alla validazione dei dati afferenti i singoli utenti (si pensi, ad esempio, all'Anagrafe). Particolare rilevanza però rivestono gli istituti della "dichiarazione sostitutiva di certificazione" di cui all'art. 46 e della "dichiarazione sostitutiva dell'atto di notorietà" di cui all'art. 47. Quest'ultimo evidenzia che il vaglio esercitato dalla PA può essere in taluni casi sostituito dal soggetto interessato nella misura in cui: *"L'atto di notorietà concernente stati, qualità personali o fatti che siano a diretta conoscenza dell'interessato è sostituito da dichiarazione resa e sottoscritta dal medesimo ..."* pertanto al cittadino viene fornita l'opportunità di sostituirsi alla funzione della PA per ciò che riguarda la certificazione di dati relativi a se stesso. L'autodeterminazione dell'individuo nel mondo contemporaneo si veste di una nuova forma, facendosi nuovo paradigma al passo con la rivoluzione digitale in corso: l'Identità Digitale: le informazioni legate alla propria persona creano un insieme di attributi che definiscono una qualsiasi identità. Allo stato attuale, questo insieme di informazioni facenti capo ad un unico individuo è posto al centro di un sistema di controllo e validazione facente capo ad un ente

esterno al quale di demandano la validazione nonché la verifica di tali informazioni. A questo proposito, le tecnologie di Distributed Ledger rappresentano lo strumento principe per dare concretezza al principio di autodeterminazione che da sempre si cerca di cristallizzare dal punto di vista normativo in maniera sempre più precisa. Grazie a questo nuovo paradigma tecnologico ogni individuo ha la possibilità di generare un proprio insieme di informazioni univoche che permettono di disegnare la sua Identità Digitale, alle quali sarà possibile associare credenziali verificabili da parte di un'autorità esterna *trusted*. In questo senso, la soluzione che qui si propone un progressivo appello al principio di autodeterminazione che porterà ad una totale assenza di autorità intermedie dei processi di validazione dei dati dell'individuo. Strumento importante della rivoluzione digitale in corso è la blockchain, che permette di costruire un perimetro entro il quale conservare tutte le identità appartenenti a un singolo individuo, portando alla costituzione della c.d. "identità sovrana decentralizzata (SSI)". Tali sistemi consegnano all'individuo la sovranità sui dati che ha diffuso nel web per costruire un identificativo univoco. Autorità riconosciute, quali ad esempio i Governi nazionali, possono rilasciare credenziali caratterizzate dall'imprescindibile requisito della verificabilità, che conferiscono ai singoli individui il potere di controllo sulla circolazione dei propri dati in rete, nel nostro caso: un certificato vaccinale. Il modello attualmente in essere si fonda sulla presenza di enti certificatori che svolgono la funzione di Identity Provider. La restituzione al singolo individuo del potere di autodeterminarsi, in favore della diminuzione del potere in capo ad un'autorità certificante, rappresenta un nuovo paradigma che permette di superare schemi che appaiono ormai obsoleti. La c.d. "Self Sovereign Identity" trova nella Blockchain lo strumento principe per dare vita ad un registro distribuito, disponibile e permanente sul quale registrare certificati ed informazioni facenti capo ad un unico soggetto grazie all'impiego della crittografia dei dati.

Il progetto SonoSano si propone come modello di SSI eterogenea ed "ibrida" preferito nel caso di specie ad una forma di SSI assoluta, senza alcun tipo di intermediazione ed in segno di rottura con il passato, fungendo così da ponte nel passaggio dal vecchio sistema gestito dal service provider al nuovo sistema interamente autonomo.

2.1 SSI assoluta

Nel caso di SSI assoluta, l'issuer trascriverebbe il proprio nome a titolo definitivo su blockchain fornendo time stamp della creazione e hash del dato. E' il caso ad esempio di chi, al raggiungimento della capacità conseguita con la maggiore età, possa attribuirsi un'identificativo e determinare la sua SSI. La chiave crittografica asimmetrica privata consente all'issuer di avere univocamente accesso al dato da lui generato ed a lui riconducibile e spenderlo on demand. In tal modo si può ipotizzare il possesso, o meglio diritto di accesso, ad un wallet che invece di detenere valore, detiene una identità. Ciò che un processo di SSI deve garantire è in realtà l'immutabilità del dato generato e soprattutto la sua spendibilità in ogni transazione relativa a dati che rappresentino appunto identità, documenti o valore. Poter dimostrare a chiunque ed in ogni condizione di essere il titolare della informazione "nome" autoattribuita rende l'identità spendibile. In sostanza gli elementi fondamentali sono quindi l'univocità del collegamento al soggetto definito "portatore" della propria identità (prima caratteristica necessaria per la costruzione della SSI) e (seconda caratteristica) l'immutabilità della stessa informazione autoattribuita.

Un caso di SSI assoluta si potrebbe ipotizzare per i nati, i cui nomi alla data XX

verrebbero registrati dai genitori alla presenza di due testimoni (ostetrica e infermiere) su un wallet digitale, con trascrizione su blockchain pubblica. Come per la registrazione tradizionale in anagrafe, anche essa si basa su autocertificazione/dichiarazione dei genitori circa il nome attribuito e farà fede X la nascita come data di nascita la data di registrazione. **(Timestamp ex art. 8 ter D.L. 135/2018 – convertito in L.12/2019)**. Questa soluzione elimina l'utilizzo di TSP.

Prima i genitori per i figli poi questi ultimi, al compimento della maggiore età, avranno il possesso della chiave privata per accedere univocamente ai propri dati ed essere a loro collegati univocamente, oltre che una chiave pubblica per permettere a tutti i soggetti ingaggiati la verifica degli stessi dati ad ogni occasione necessaria, come uno spid “diverso” decentralized.

2.2 Soluzione Sono Sano (SSI Ibrida)

Il cambio di paradigma culturale che conduce ad una SSI assoluta e svincolata dai TSP richiede un passaggio intermedio: un sistema ibrido che regolamenti le identità delle persone fisiche. **Pertanto ai fini del progetto SONOSANO si ipotizzerà una la soluzione ibrida: Me + Trusted Service Provider (TSP).**

Per conferire agli individui il potere di autocertificazione e di autodeterminazione, si utilizzerà il TSP per permettere la transizione da data base centralizzato (quello del TSP che fornisce la firma elettronica e garantisce identità) ad uno distribuito che elimina l'intermediario TSP. Il processo prevederà il collegamento dei dati personali contenuti nel wallet ai dati allocati nel sistema centralizzato dell'Ente o TSP, in un ideale passaggio di consegne.

L'autoattribuzione e l'opponibilità dell'identità possono essere garantite dall'utilizzo di un protocollo blockchain.

Collochiamo la SSI ibrida su un data base distribuito e pubblico anche in considerazione di quanto previsto dall'art. 8 ter del Decreto legge 14.12.2018, n. 135 in tema di riconoscimento dell'esistenza e della validità delle DLT, quali strumenti di garanzia di trasparenza, immutabilità del dato e verificabilità.

3. Lo Use Case del Pass Vaccinale SONOSANO per l'Hackathon: proposta generale

Il COVID-19 potrebbe essere il momento di svolta nel settore della autocertificazione per accelerare la spinta verso un sistema di credenziali auto-sovrane, onnipresenti, convenienti e verificabili alimentato dalla tecnologia blockchain.

L'associazione della SSI ai dati sanitari e ad un certificato vaccinale emesso da un soggetto medico trusted rafforza e cristallizza il legame, rendendolo definitivo, tra l'autocertificazione di sé ed il dato certificato emesso in favore di soggetto identificato tradizionalmente dal TSP, secondo la logica di transizione già proposta.

Il certificato vaccinale risulta essere trusted di default in quanto emesso da soggetto

fiduciario. Si tratta, ora, di trasferirlo dal data base centralizzato ove è ospitato verso uno pubblico e distribuito, collegandolo ad una identità sovrana autonoma (come detto verificata in fase ibrida di transizione dal TSP) e già residente su blockchain pubblica, su cui è stata trascritta in modo immutabile, sempre verificabile, inequivocabile ed incorruttibile.

La soluzione SONOSANO applica questo principio ed il predetto algoritmo di concatenazione logica. La persona fisica si autodetermina e convalida la propria identità, facendo il match con l'identità fornita dal TSP. L'identità risiede univocamente su un wallet personale, l'utilizzo del token e del protocollo blockchain consentono l'identificazione univoca e la verificabilità delle identità e delle informazioni fornite dal TSP. I dati forniti dal TSP vengono ospitati all'interno del token ERC - 1155 che interagisce con l'esterno, collegando le informazioni sanitarie alla SSI.

4 I dati forniti dal soggetto (ciò che posso dire di me) - La cristallizzazione con NFT del dato personale autocertificato dichiarato dal soggetto per la creazione delle proprie verificable credentials)

Il possessore del wallet di identità può soddisfare l'univocità dell'attribuzione delle qualità personali con la creazione di un **Self Sovereign Identity Token** da depositare nel proprio wallet. Gli NFT possono rendere univoca l'identità dell'individuo oltre che essere essi stessi richiamati ogni qual volta si necessita di verificare la stessa identità. Possono quindi rappresentare certificati di nascita. Nel caso in esame rappresentano dati di identità. Ovviamente questi token possono essere tenuti al sicuro in forma digitale e preservati da contraffazioni. Nasce in tal modo una **NFI (Non fungibile identity)** in cui i dati autocertificati risulteranno sempre collegati al soggetto emittente e mai modificabili in seguito.

Il tal modo si ottiene il superamento del concetto di verificable credentials fornite esclusivamente dal TSP con la creazione di un **NFT univoco collegato ad uno smart contract più complesso, richiamabile per ogni verifica**. Il sistema si completa implementandolo con certificati prodotti dal TSP o Ente che gestisce il dato sanitario (certificato vaccinale).

5 I dati forniti dal TSP (ciò che devono dire altri di me)

5.1 dati sanitari: certificato vaccinale

La composizione del dato sanitario relativo al pass vaccinale impegna professionalità mediche che necessariamente non possono ricadere sotto l'arbitrio dell'individuo che ne beneficia. La creazione del certificato non può prescindere quindi dalla competenza ed attività di un soggetto trusted appartenente ad un profilo medico accreditato presso struttura sanitaria che lo legittimi ed un Ente preposto che ne gestisca il rilascio. Tale dato risiede inizialmente in un Data Base centralizzato di dominio dell'Ente o del TSP. La proposta di SONOSANO è di scollegare il certificato dal Data Base centralizzato del TSP e collegarlo alla **NFI** dell'individuo, all'interno di un token complesso risiedente su blockchain pubblica (decentralizzata e distribuita) e richiamabile per ogni verifica

necessaria.

6. La sintesi: wallet e token

Perché il sistema funzioni correttamente, esso deve soddisfare, a questo punto, i tre principi fondamentali: il **controllo individuale**, la **sicurezza** e la piena **portabilità**. Il sistema proposto lo permette contemporaneamente.

6.1 Il token misto non fungibile e fungibile ERC- 1155

Lo Use Case **SONOSANO** prevede la realizzazione ed attribuzione a ciascun individuo di un **token ERC-1155 su blockchain di Ethereum** che presenta congiuntamente le caratteristiche di un **token non fungibile** ma anche di un **token fungibile**.

6.2 dati univoci dell'NFT connessi ai dati interagenti provenienti dall'esterno utilizzando ERC-1155

Il token presenta le caratteristiche di univocità dell'NFT, legate alla SSI dell'individuo, ma permette la sua implementazione attraverso l'invio allo smart contract di risorse esterne che non sarebbero implementabili in un mero NFT ERC-721. L'altra caratteristica dello standard ERC-1155 è la spiccata interoperabilità tra blockchain, aspetto importante quando si accostano ambiti di utilizzo differenti.

La collocazione all'interno del medesimo token di una SSI e di un certificato vaccinale proveniente da terze parti TSP, con possibilità di aggiornamento additivo, crea un PASS individuale, portatile, dinamico e sicuro che può essere custodito in un Wallet, il Wallet documentale di **SONOSANO**.

Citando ancora Ferdous: *“La blockchain e le caratteristiche della tecnologia sono conformi alle proprietà chiave dell'a Self Sovereign Identity. La blockchain fornisce un dominio decentralizzato che non è controllato da nessuna singola entità ed in cui i dati archiviati sono resi prontamente disponibili a qualsiasi entità autorizzata, come "asset personale di disponibilità o accesso”.*

6.3 Il Wallet

Attraverso la realizzazione e l'utilizzo del Wallet documentale SONOSANO, il proprietario di un dato possiede il pieno controllo su di esso sin dalla sua creazione e determina come tali dati possono essere condivisi con altri utenti all'interno della blockchain, soddisfacendo così la possibilità di divulgazione richiesta dall'esigenza di un pass vaccinale.

SONOSANO prevede la creazione di portafogli digitali e garantisce ai loro univoci proprietari la facoltà di comunicare e scambiare credenziali verificabili in modo sicuro ed incorruttibile oltre che resistente ad attacchi informatici, permettendo ad essi di **esibire il passaporto vaccinale in favore dei soggetti richiedenti**.

Il tipo di blockchain selezionato per le credenziali digitali ha molto a che fare con la fiducia che si ripone nel sistema utilizzato. La blockchain che intende utilizzare SONOSANO si baserà principalmente sull'utilizzo di blockchain pubblica permissionless ossia una blockchain senza autorizzazione ove quindi chiunque è in

grado di scrivere / aggiornare dati.

Ma tale infrastruttura sarà collegata attraverso gli smart contract ibridi residenti ai data base centralizzati o, ancora in seguito, alle blockchain degli Enti TSP.

L'uso del protocollo blockchain permette di soddisfare il requisito della firma elettronica avanzata secondo quanto previsto per lo stesso dal Regolamento UE 2014/910 (Reg. eIDAS art. 25). Esso è sufficiente per la gestione del passaporto vaccinale.

7. SONOSANO: riflessioni ulteriori

Nel progetto SONOSANO la qualificazione soggettiva ai fini del trattamento dei dati sanitari viene identificata alla luce della struttura che abbiamo immaginato. Il soggetto che si autodetermina agisce in qualità di interessato e al contempo di titolare del trattamento in quanto determina finalità e mezzi: è l'interessato stesso che determina chi possa accedere ed in che misura alle proprie informazioni tramite il wallet personale abbinato al token in cui è contenuta la NFI.

Il dato sanitario dell'individuo risiede sul proprio wallet ed è protetto dal sistema di crittografia asimmetrica che utilizza chiave pubblica e chiave privata. Su blockchain sarà possibile verificarne, attraverso la funzione di HASH, l'univocità ed il collegamento al soggetto che ne permetterà l'accesso. Il documento medico sarà anche esso custodito all'interno del wallet a cui è collegato e sempre verificabile dai soggetti autorizzati dal possessore del wallet.

La circolazione del dato è completamente in capo al soggetto proprietario del wallet che decide di renderlo disponibile per le verifiche

Non abbiamo approfondito il tema GDPR in questa sede in quanto ai fini dell'hackthon il presente progetto si propone di offrire solo un'idea concettuale, la quale andrebbe declinata con operatori tecnici per trovare la sua compiuta definizione in un'architettura di privacy by design in relazione ai principi di cui all'art. 5 GDPR e ai diritti degli interessati.

8. Conclusioni

Il quadro normativo attuale è frammentario e carente ed in rapida evoluzione. Da ultimo l'Autorità Garante della privacy ha enunciato la necessità della redazione di una legge per disciplinare il tema dei passi vaccinali ed in sede europea è in corso di discussione il Digital Green Pass. Il presente paper si propone solo di offrire una prima interpretazione possibile del tema SSI applicato al passaporto vaccinale. SONOSANO è un wallet documentale in cui risiede un combinato di una Self sovereign identity non fungibile NFI ed un documento proveniente da un provider definito Trusted che fornisce il certificato vaccinale. L'utilizzo combinato di NFT, Smart contract, e blockchain ambisce, in misura più possibilmente compliant alle norme vigenti, a garantire all'individuo possessore dell'accesso al proprio wallet di creare, spendere e circolarizzare secondo la propria volontà i propri dati in relazione all'esigenza che si manifesta.