FONDAZIONE BRUNO KESSLER
MAGAZINE

Onboarding digitale e GDPR: controllo distribuito e fruibilità di dati e documenti

13 Ottobre 2021

Primo di una serie di approfondimenti a cura di CherryChain, realtà imprenditoriale co-locata nella sede FBK di Povo che collabora col centro di ricerca Cybersecurity della Fondazione Bruno Kessler, diretto da Silvio Ranise

Fra i processi che maggiormente hanno subito l'influsso della trasformazione digitale c'è l'identificazione e la certificazione dell'identità di chi si accinge a diventare cliente: la fase chiamata "onboarding".

La pandemia di certo ha enfatizzato e accelerato il tema dell'onboarding digitale, pur non avendo ancora risolto i principali rischi connessi alle tradizionali procedure, quali: l'acquisizione di immagini di documenti cartacei (foto o fotocopie), la trasposizione dei dati (ad es. attività di sportello o back-office), il disallineamento tra documentazione cartacea e digitale, e così via.

Da un lato ci si trova con i rischi dovuti alla manipolazione di dati tra documenti digitalizzati e attributi di identità digitale memorizzati in diverse organizzazioni.

Dall'altro vi è l'opportunità per ogni persona come cittadino, lavoratore, pensionato o studente di poter fare uso di diversi strumenti e soluzioni di identità digitali messe a disposizione.

Questo avviene sia nell'ambito pubblico, con SPID e Carta di Identità Elettronica CIE 3.0, sia in quello privato, con gli strumenti di identificazione usati per l'accesso al Remote Banking (Strong Customer Authentication) o con le firme digitali offerte dalle diverse autorità di certificazione.

Di fatto tutte le soluzioni sopra elencate hanno in comune l'**onboarding**, tramite cui si ottiene l'acquisizione di dati e documenti dell'utente e il suo riconoscimento, ovvero la prova che unisce l'identificazione del soggetto dichiarante e le informazioni raccolte per produrre e associare una identità (l'*identity proofing*).

Possono cambiare le modalità tra canale fisico e canale digitale, ma alla fine devono poter rispettare gli stessi principi di **adeguata verifica** (Know Your Customer o Due Diligence) per dare dimostrazione della coerenza tra la persona e gli attributi (dati e documenti) riferiti all'identità codificata (ad es. anagrafica, numero di rapporto, contratto, utenza, ecc.) e digitalizzata (fattori di

autenticazione).

Perché non ci è possibile accorciare i tempi di onboarding per accedere a servizi on-line della P.A. o aprire nuove utenze sfruttando l'identità digitale fornita dalla propria Banca, o al contrario usare la CIE 3.0 per aderire a un nuovo servizio di pagamento?

Al di là dei limiti tecnici risolvibili come già provato nel caso delle banche con le piattaforme API (API PSD2 o OpenBanking), le diverse identità digitali, pur corrispondenti allo stesso soggetto qualificato, non permettono ancora di essere fruite completamente.

Con questo non si intendono le credenziali di accesso (i due o più fattori di autenticazione), ma la possibilità per la persona di poter avere il controllo di dati e documenti resi disponibili per gli onboarding già eseguiti e poterli riusare e aggiornarli in altri processi di attivazione di nuovi servizi presso operatori diversi.

Se ciò fosse possibile. le eventuali incoerenze dovute ai rischi connessi alle tradizionali procedure come errori, omissioni, manipolazioni o disallineamenti sarebbero man mano meglio individuate e risolte da una sorta di "controllo sociale" o "**catena di custodia**" tra la persona e gli operatori pubblici e privati presso cui essa apre rapporti digitali.

Questa soluzione non necessita di un'entità unica centralizzata, perché si può avvalere di un'architettura distribuita e decentralizzata per effetto della concatenazione degli attributi di identità scambiati nei diversi onboarding. Forse sembra paradossale, ma il GDPR non è di certo un limite a tutto ciò, anzi promuove la fruibilità del dato da parte del proprietario dei dati (il cittadino, lavoratore, pensionato o studente che sia) una volta fissato un livello di consenso al trasferimento tra un operatore e l'altro.

CherryChain è stata fondata nel 2018 da Carlo Rizzi e Marco Sittoni e si occupa di ricerca e sviluppo in ambito Distributed Ledger Technology e Smart Contract. Collabora con il centro di ricerca FBK – Cybersecurity diretto da Silvio Ranise.

LINK

https://magazine.fbk.eu/it/news/onboarding-digitale-e-gdpr-controllo-distribuito-e-fruibilita-di-dati-e-documenti/

TAG

- #certificazione
- #cie 3.0
- #identità digitale
- #onboarding
- #P.A.
- #servizi digitali
- #spid

MEDIA COLLEGATI

- Cherry Chain : https://www.cherrychain.it/
- FBK Cybersecurity : https://www.fbk.eu/it/cybersecurity/

AUTORI

- Redazione interna