

Digital Identity Management and library services access: preparing for the future

Valdo Pasqui^(a)

a) Formerly University of Florence, <https://orcid.org/0000-0002-4105-2208>

Contact: Valdo Pasqui, valdopasqui@tiscali.it

Received: 31 March 2025; Accepted: 02 July 2025; First Published: 15 September 2025

ABSTRACT

Digital identities and their management systems are the core for the next generation ecosystem of trusted digital services. The European Parliament and the European Union Council have set themselves this objective with Regulation 910/2014 (eIDAS), updated in 2024, already transposed by Italy into the Code for Digital Administration (CAD). The architecture and reference framework specification started in 2021 and the ongoing implementations will lead to the adoption by 2026 of the European Digital Identity Wallet (EDIW), whose Italian instance (IT-Wallet) has been released in embryo as recent versions of the App-IO. We are therefore on the eve of a significant transformation from the current way of managing digital identities and access to digital resources and services that will impact on libraries services too. After describing the concepts and methods of access control management and digital identity with some references to current libraries context, the paper describes the new decentralized model and examines some aspects of the transformation process that all stakeholders (decision-makers, operators and users) are called upon to be aware in order to assess the difficulties and seize the opportunities offered.

KEYWORDS

eIDAS2; Digital Identity; Identity and access management; Library services.

La gestione dell'Identità Digitale e l'accesso ai servizi bibliotecari: prepararsi al futuro

ABSTRACT

Le identità digitali e i sistemi per la loro gestione sono il nucleo centrale per lo sviluppo di un ecosistema di servizi digitali affidabili ("trusted"). Il Parlamento Europeo e il Consiglio dell'Unione Europea si è posto questo obiettivo con il Regolamento 910/2014 (eIDAS), aggiornato nel 2024, già recepito dall'Italia nel Codice per l'Amministrazione Digitale (CAD). Fin dal 2021 è stata avviata la specifica dell'architettura e del framework di riferimento che con le implementazioni in corso porteranno entro il 2026 all'adozione del European Digital Identity Wallet (EDIW), Portafoglio Digitale dell'Identità, la cui istanza italiana (IT-Wallet) è stata rilasciata in embrione con le recenti versioni della App-IO. Siamo dunque alla vigilia di una significativa trasformazione rispetto alle attuali modalità di gestione delle identità digitali e dell'accesso alle risorse e ai servizi digitali che impatterà anche sui servizi bibliotecari. L'articolo, dopo aver descritto i concetti e le modalità di gestione del controllo dell'accesso e dell'identità digitale con alcuni riferimenti all'attuale contesto delle biblioteche, descrive il nuovo modello decentralizzato e esamina alcuni aspetti del processo di trasformazione sottolineando che tutti i soggetti coinvolti (decisori, operatori e utenti) sono chiamati a sviluppare la giusta consapevolezza per valutare le difficoltà e per cogliere le opportunità che si presentano.

PAROLE CHIAVE

eIDAS2; Identità Digitale; Controllo dell'accesso; Servizi bibliotecari.

1. Premessa

L'identità di una persona comprende tutto ciò che caratterizza un individuo e presenta molteplici sfaccettature se esaminata da diversi punti di vista come la filosofia, la sociologia, la medicina, la psicologia e il diritto. In psicanalisi si fa riferimento all'identità psicologica intesa come "il senso e la consapevolezza di sé come entità distinta dalle altre".¹ Nella vita di tutti i giorni ci è familiare il concetto di identità come verifica di chi sia una persona attraverso il controllo che le generalità esibite corrispondano a quelle indicate in un documento di riconoscimento valido. L'identità digitale riveste un analogo ruolo nell'ambito dei processi che governano l'accesso alle risorse e ai servizi digitali erogati dalle Pubbliche Amministrazioni (PA) e dalle organizzazioni private. Tutti deteniamo una o più identità digitali, è nostra cura usarle in modo corretto, proteggerle e verificare che i servizi cui accediamo garantiscano adeguati livelli di sicurezza.

Nell'ultimo semestre del 2024 si è parlato molto dell'evoluzione della app dei servizi pubblici (App IO²) che ora consente di memorizzare la versione digitale di alcuni documenti (tessera sanitaria, patente di guida e carta europea della disabilità). Il Sistema Pubblico di Identità Digitale italiano attualmente comprende due tipologie di identità digitale, lo SPID³ e la Carta d'Identità Elettronica (CIE),⁴ con le quali i cittadini possono accedere ai servizi online delle Pubbliche Amministrazioni. App IO diventerà il portafoglio italiano dell'identità digitale (IT-Wallet), lo strumento con il quale l'Italia darà attuazione alla normativa Europea entrata in vigore nel 2024, nota con la sigla eIDAS2 (European Parliament and Council 2014). Il percorso che porterà al suo esercizio è in divenire, ma siamo alla vigilia di un profondo cambiamento rispetto alle modalità di gestione tradizionali che richiede consapevolezza e attenzione.

Anche i Musei, gli Archivi e le Biblioteche sono interessati a questa trasformazione e le biblioteche pubbliche, oltre a facilitare l'accesso ai propri servizi digitali adottando le nuove soluzioni, grazie alla loro diffusione sul territorio possono svolgere anche un importante ruolo di accompagnamento di alcune categorie di cittadini più in difficoltà a causa del *digital divide*. L'articolo richiama i termini, i principi e le modalità di gestione dell'identità digitale, descrive lo scenario attuale e le sue evoluzioni in base alla normativa europea eIDAS2 per poi esaminare alcune criticità e delineare alcune linee d'azione.

2. Gestione dell'identità digitale

2.1. Definizione e attributi

La metadattazione delle risorse bibliografiche si avvale di vari sistemi di codifica degli autori come ISNI, VIAF, ORCID, LCCN e id autore SBN che i cataloghi online propongono sotto forma di link azionabili per recuperare dati sull'autore e le sue pubblicazioni. ORCID, in coppia con una

¹ <https://www.treccani.it/vocabolario/identita/>.

² <https://ioapp.it/>.

³ Un soggetto può avere più identificatori SPID, rilasciati da fornitori diversi tra quelli attivi che sono 12: <https://www.spid.gov.it/cos-e-spid/come-scegliere-tra-gli-idp/>.

⁴ La Carta di Identità Elettronica (CIE) è emessa dal Ministero dell'Interno e prodotta dal Poligrafico e Zecca dello Stato (IPZS) <https://www.cartaidentita.interno.gov.it/la-carta/>.

password, consente anche al soggetto cui è attribuito di accedere alla propria area personale per gestire le pubblicazioni di cui è autore. La pratica corrente può indurre a ritenere che l'identità digitale sia composta da un identificatore (denominato con varie sigle: login, login-id, user, user-id, user name, nome utente, account, sign-in ecc.) accoppiato con una password. In realtà l'identità digitale è un insieme di attributi che descrivono in modo univoco un soggetto o entità in un determinato contesto.⁵ Il Codice per l'Amministrazione Digitale (CAD) (CAD 2005) all'Art.1 la definisce come *“la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale [...]”*.

La Tabella 1 riporta l'elenco degli attributi del Sistema Pubblico di Identità Digitale italiano nelle due varianti SPID e Carta d'Identità Elettronica (CIE).⁶ La Federazione Italiana delle Università e degli Enti di Ricerca per l'Autenticazione e l'Autorizzazione (Federazione IDEM) gestisce attributi mutuati da standard consolidati nei contesti accademici e della ricerca quali LDAPv3 (IETF 2006a) e gli schemi Cosine (IETF 2006b), inetOrgPerson (IETF 2000), eduPerson (REFEDS 2023) e Schac (REFEDS 2022).

2.2. Entità e fasi del controllo dell'accesso

Lo scenario funzionale in cui si esplicita la gestione dell'identità digitale così definita comprende alcune componenti invarianti rispetto ai modelli e alle tecnologie:

- *risorse digitali* (es. articolo di rivista, e-book, pagina web, immagini ad alta risoluzione prodotte dalla digitalizzazione di risorse analogiche, audio, video, documenti di archivio e fascicoli archivistici, dispositivi condivisi come stampanti e scanner, spazio disco in cloud, servizi applicativi ecc.);
- *entità* che richiedono l'accesso a tali risorse e che possono essere persone fisiche ma anche applicazioni, software agent, web services, interfacce programmatiche applicative (API) e dispositivi hardware;
- *sistemi preposti alla gestione dell'identità e dell'accesso* che verificano che l'entità (soggetto) richiedente sia proprio chi dichiara di essere;
- *servizi che rilasciano le identità digitali* e i relativi attributi alle entità.

La ricognizione di diversi OPAC e discovery tool dei sistemi bibliotecari operanti in Italia mostra che molti di essi hanno attivato modalità di accesso controllato ai servizi, previa registrazione. Si tratta di una modalità necessaria per fornire servizi personalizzati (es. area di lavoro in cui salvare query e risultati delle ricerche, scrittura di recensioni, suggerimenti di lettura, funzionalità di tipo social per la taggatura delle risorse bibliografiche, richieste di prestito online sia locale che ILL ecc.) e per gestire l'accesso alle risorse sottoposte a vincoli (es. riviste in formato digitale con abbonamento pagato dalla biblioteca/ateneo/istituzione, visualizzazione e riproduzioni di immagini ad alta definizione, risorse digitali soggette a copyright).

⁵ Cfr. le definizioni riportate in “IT Security and Privacy — A framework for identity management” (standard ISO/IEC 24760-1:2019) e in NIST Special Publication 800-63-4: “An attribute or set of attributes that uniquely describes a subject within a given context”.

⁶ https://docs.italia.it/italia/spid/spid-cie-oidc-docs/it/versions-corrente/attributi_utente.html.

Attributo	Descrizione	Supportato da	Person Identification Data per le persone fisiche (O=Obbligatorio)
spid_code	codice identificativo univoco assegnato dal gestore dell'identità digitale	spid	personal_administrative_number
given_name	Nome	spid, CIEid	given_name (O) given_name_birth
family_name	Cognome	spid, CIEid	family_name (O) family_name_birth
place_of_birth	Luogo di nascita	spid, CIEid	birth_place (O)
birthdate	Data di nascita	spid, CIEid	birth_date (O)
			nationality (O)
gender	Sesso	spid, CIEid	sex
company_name	Ragione o denominazione sociale	spid	per le persone giuridiche (legal person): - current legal name (O) - unique identifier (dello Stato Membro) (O) - una serie di altri attributi opzionali
registered_office	Sede legale	spid	
fiscal_number	Codice fiscale della persona fisica	spid, CIEid	
company_fiscal_number	Codice fiscale Persona Giuridica.	spid	
vat_number	Partita IVA	spid	
document_details	Descrizione del documento d'identità	spid, CIEid	tre metadati obbligatori relativi su chi ha emesso i PID: - issuing_authority - issuing_country - expiry_date (dei PID)
phone_number	Numero di telefono mobile	spid, CIEid	mobile_phone_number
phone_number_verified	Valore booleano che indica se il numero di telefono mobile è stato verificato dal fornitore dell'identità digitale	CIEid	
landline_number	Numero di telefono fisso	CIEid	
email	Indirizzo di posta elettronica	spid, CIEid	email_address
email_verified		CIEid	
e_delivery_service	Domicilio digitale Indirizzo casella PEC	spid, CIEid	
eid_exp_date	Data di scadenza identità	spid	
address		spid, CIEid	- resident_address - resident_country - resident_state - resident_city - resident_postal_code - resident_street - resident_house_number
			Portrait (foto dell'utente del wallet)

Tabella 1. Confronto attributi del Sistema Pubblico di Identità Digitale italiano vs Person Identification Data in Art.3.3 di (European Commission 2024)

La logica di alto livello del controllo dell'accesso può essere descritta esaminando le quattro fasi di cui si compone:

- a) *Registrazione* – è una fase “una tantum” che consente di creare e assegnare un'identità digitale, spesso indicata come “onboarding” di un nuovo utente o “crea il tuo Account” se svolta in autonomia online;
- b) *Identificazione* – la risorsa o il servizio a cui un'entità (es. una persona) vuole accedere le chiede di farsi riconoscere;
- c) *Autenticazione* – l'identità digitale fornita viene verificata, riscontrando che l'entità che l'ha dichiarata sia proprio quella che afferma di essere;
- d) *Autorizzazione* – se l'autenticazione ha avuto esito positivo viene controllato che l'entità abbia i diritti per accedere alla risorsa o al servizio richiesti.

2.3 Assegnazione dell'identità digitale

Le modalità di registrazione e assegnazione dell'identità digitale sono un passaggio fondamentale per assicurare l'affidabilità dell'intero ecosistema di servizi basati sull'identità digitale e per minimizzare i rischi di impersonificazione (un soggetto che agisce assumendo l'identità di un altro). È bene sottolineare che le identità digitali rilasciate in modo verificato da organismi appositamente preposti che seguono procedure codificate (es. SPID e CIE) hanno un livello di affidabilità non confrontabile rispetto a quelle (auto)create online dagli utenti stessi. La registrazione e l'attivazione di SPID sono svolte da uno dei gestori attivi (Identity Provider) esibendo un documento italiano in corso di validità o di persona o tramite CIE (online o attraverso app), ma anche da remoto (con o senza operatore⁷). La CIE può essere richiesta presso un qualsiasi Comune e il rilascio comprende la verifica dei dati anagrafici e l'acquisizione delle impronte digitali e, in caso di primo rilascio, l'esibizione di un documento d'identità in corso di validità (altrimenti occorrono due testimoni). Gran parte degli OPAC e dei portali delle biblioteche italiane offrono la registrazione online che comporta l'immissione dell'identificativo utente (di solito indirizzo di posta elettronica) di una password e di alcuni dati anagrafici e di contatto. Solo alcuni sistemi bibliotecari (es. Biblioteche di ROMA, la Rete bibliotecaria di Romagna e San Marino, il Sistema Bibliotecario della Provincia di Reggio Emilia, il Polo Bibliotecario Modenese, il Polo regionale SBN Sardegna, il Polo COBI-RE della Regione Toscana, il Polo MiC Venezia, il Polo bibliotecario regionale del Veneto) hanno colto l'opportunità di avvalersi dell'accesso con SPID/CIE anche per consentire la registrazione recuperando dal Sistema Pubblico d'Identità gli attributi necessari, così rendendo l'operazione completamente automatica per gli utenti e assicurando alle biblioteche il recupero di dati certificati.

⁷ Occorre evitare di far circolare copie dei documenti personali di riconoscimento perché truffatori venuti in possesso di tali copie hanno attivato un secondo SPID intestato a una persona con email e telefono diversi agendo poi per suo conto in modo fraudolento in alcuni servizi (es. INPS).

2.4 Identificazione e autenticazione: password e fattori

Le successive fasi del processo di controllo dell'accesso sono l'identificazione e l'autenticazione che si ripetono in occasione di ogni accesso a un servizio o una risorsa digitali. Questi due momenti si possono rappresentare con la sequenza: “Dimmi chi sei?” – “Sono Paolino Paperino” – “Dimostramelo!”. Al termine di questa interlocazione l'accesso richiesto può essere concesso o negato. Nel primo caso gli attributi che costituiscono l'identità digitale (eventualmente con altri attributi del soggetto/entità registrato) sono utilizzati per effettuare i controlli autorizzativi che determinano il contesto di risorse e funzioni locali abilitate all'utente.

La dimostrazione della identità digitale dichiarata consiste nell'esibizione da parte dell'utente di uno o più fattori (credenziali) classificabili nelle seguenti categorie:

- *Qualcosa che si conosce*: password, PIN;
- *Qualcosa che si possiede*: chiavetta fisica (hardware token), smartcard, codice one-time (OTP) inviato per email o SMS, codice OTP generato da un dispositivo esterno (es. RDS SecurId), codice o richiesta di conferma (es. “Autorizza richiesta”) generati su una APP di un dispositivo mobile (smartphone) associato all'identità digitale e a cui si accede in modo protetto con PIN o controllo biometrico;
- *Qualcosa che si è*: una proprietà biometrica come un'impronta digitale, la scansione della retina, della faccia o della voce (spingendosi fino al DNA in contesti molto sensibili).

L'utilizzo della sola password è la modalità più diffusa ma anche la più debole (un solo fattore) e esposta a molti rischi di compromissione (password facili da scoprire, meccanismi che inducono gli utenti a comunicare le proprie password a soggetti/siti fraudolenti, malware che spiano e catturano le password usate ecc.), pertanto si sta sempre più affermando l'imposizione di due o più fattori. Esistono anche soluzioni che prevedono lo scambio di codici temporanei crittografati (token) mediante coppie di chiavi crittografiche (pubblica e privata) distribuite tramite certificati digitali secondo gli standard della Public Key Infrastructure (PKI).⁸

SPID e CIE prevedono tre livelli di utilizzo, il secondo (due fattori) è lo standard, per SPID consiste nell'invio di un OTP tramite SMS o app e per la CIE prevede l'uso del OTP o la scansione di un QRCode.

3. Modelli e soluzioni un ecosistema di servizi “trusted”

Le identità digitali e i sistemi per la loro gestione sono il nucleo centrale attorno al quale costruire un ecosistema di servizi “trusted” ovvero dei quali gli utenti si fidano, grazie alla combinazione e l'attuazione di standard, tecniche, procedure, regole e comportamenti che assicurano elevati livelli di affidabilità (reliability), verificabilità (accountability) e disponibilità (availability).

⁸ La FIDO Alliance, l'associazione di industrie ICT che sviluppa standard e soluzioni per l'autenticazione, fonda la soluzione Passkeys, supportata da Google, Amazon, Apple, Microsoft e altre aziende, proprio sulla crittografia a doppia chiave per consentire all'utente di autenticarsi al server senza l'uso di password e l'invio di altri dati: <https://fidoalliance.org/passkeys/>.

3.1 Sicurezza, comportamenti e modelli

Per quanto attiene la sicurezza nel contesto delle biblioteche è bene precisare che oltre a proteggere le risorse bibliografiche e digitali occorre anche tutelare la privacy degli utenti e le loro identità digitali. I sistemi bibliotecari non sono esenti dai rischi di attacchi con effetti rilevanti come dimostra il caso della British Library (BL 2024; Grove 2024). Anche un catalogo online o un discovery tool possono essere obiettivo di attacchi volti a esfiltrare le identità digitali e a violare la privacy degli utenti estrapolando dati sugli interessi di lettura, studio e ricerca e sugli orientamenti politici e sessuali che possono essere usati in modo diretto contro l'utente o indirettamente a fini commerciali (vendita dei dati).

Per limitare questi rischi occorre agire congiuntamente su due livelli: quello comportamentale che ricade sotto la responsabilità degli utenti e quello strutturale che concerne i modelli e le architetture dei sistemi di gestione dell'identità digitale.

Sul primo aspetto si rimanda alla lettura della sezione dedicata alla Cybersecurity del sito del Garante della Privacy che propone un ampio insieme di schede informative⁹ sulle misure di sicurezza, la generazione e la protezione delle password e le modalità per proteggersi dai tentativi di furto d'identità (phishing, smishing, vishing, ransomware) (Clusit 2025). Per mitigare i rischi di sicurezza legati all'uso delle password si sta diffondendo la pratica di utilizzare software che generano password complesse e le memorizzano in modo crittografato (Kime 2024).

La soluzione più datata, ma ancora oggi molto diffusa, per la gestione del controllo dell'accesso prevede funzioni specializzate degli applicativi e tabelle del database per registrare gli attributi degli utenti (password comprese). La maggior parte dei sistemi gestionali installati presso le biblioteche, come si riscontra in un numero molto elevato di cataloghi online e discovery tools bibliotecari, seguono questo approccio perché sono concepiti come soluzioni autonome (verticali) e dunque mettono a disposizione dei propri clienti le funzionalità per registrare gli utenti e per supportare almeno le operazioni base di cambio e recupero password dimenticata.

3.1.1 Il modello di gestione delegata

Per ovviare alla proliferazione di silos contenenti le identità digitali, fin dalla metà degli anni Novanta del secolo scorso sono stati sviluppati sistemi dedicati, denominati Identity and Access Management (IAM), che concentrano tutte le funzionalità e procedure concernenti la gestione delle identità:

- gestire il repository degli attributi delle identità digitali;
- implementare le funzioni di registrazione (self-provisioning), cambio e recupero password dimenticata;
- offrire procedure di provisioning e deprovisioning massivo utili in ambiti aziendali e istituzionali con un rilevante numero di utenti soggetti a ben definite logiche di registrazione e disattivazione (es. studenti di un ateneo, dipendenti di un ente territoriale o di un'azienda multi sede, cittadini residenti in un comune ecc.);
- implementare tecniche di autenticazione a più fattori;
- adottare le policy di sicurezza per la protezione dagli attacchi informatici;

⁹ <https://www.garanteprivacy.it/temi/cybersecurity>.

- abilitare l'autenticazione singola a più servizi, Single Sign-On (SSO);
- implementare i protocolli e gli standard previsti per abilitare la partecipazione a sistemi federati di gestione delle identità, tra cui in Italia SPID e CIE.

Questo approccio ha portato anche alla diffusione del modello di gestione delegata dell'identità digitale, Delegated Identity Management, ormai largamente adottato dalle applicazioni web e dai servizi operanti in Cloud:

- a) un sistema, denominato Identity Provider (IdP), ha in carico la gestione delle identità digitali e gestisce le operazioni necessarie per svolgere le fasi di identificazione e di autenticazione;
- b) le applicazioni e le risorse digitali sono protette da un componente, denominato Service Provider, che quando un'entità (es. utente) ne richiede l'accesso lo reindirizza attraverso un canale sicuro (crittografato) verso l'IdP;
- c) le interazioni per portare a compimento l'identificazione e l'autenticazione avvengono direttamente tra l'entità richiedente e l'IdP;
- d) se l'autenticazione fallisce l'entità richiedente viene rinviata al SP con messaggio d'errore e il SP nega l'accesso, altrimenti il SP riceve un token e degli attributi (detti asserzioni) che permettono al SP di abilitare l'accesso alla risorsa/servizio richiesto.

Le politiche e le modalità (es. autenticazione a più fattori) di controllo dell'accesso sono così centralizzate in un unico sottosistema specializzato e condiviso da più applicazioni e servizi, garantendo una gestione protetta, unificata e coordinata (regole, policy, tecniche di sicurezza ecc.) delle identità digitali degli utenti. Così i singoli software applicativi si svincolano dalle problematiche tecniche e di sicurezza demandando al sottosistema dedicato la gestione delle identità digitali.

3.1.2 Single Sign-On e la gestione federata delle identità

Il modello della gestione delegata è al centro del funzionamento del Single Sign-On e dei sistemi di Identity Management Federato. Nel primo scenario, tipicamente aziendale, quando un utente accede a un'applicazione il SP lo reindirizza verso l'IdP che verifica l'esistenza di una sessione di lavoro attiva, creata in occasione della precedente autenticazione di un'altra applicazione. In caso affermativo l'IdP restituisce al SP l'autorizzazione per concedere l'accesso senza ripetere nuovamente le fasi di identificazione e autenticazione (da qui il termine "single"). Nel secondo scenario più organizzazioni si accordano per condividere procedure formali e tecniche attraverso le quali riconoscere reciprocamente le identità digitali emesse da ciascuna di loro. Ogni aderente alla federazione gestisce il proprio IdP che è responsabile dell'assegnazione, della gestione e della verifica (autenticazione) dell'identità digitali delle proprie entità (persone, servizi ecc.). Quando un utente membro della federazione chiede l'accesso ad un servizio/risorsa condiviso/a il relativo SP lo indirizza verso l'IdP della sua organizzazione a cui sono demandate l'identificazione e autenticazione. Se l'autenticazione con il proprio IdP avviene con successo questo restituisce al SP un insieme di attributi che gli consentono di riconoscere l'utente, sbloccare l'accesso e applicare le politiche autorizzative. In tal modo le identità digitali e i fattori usati restano confinati nell'ambito dell'interazione tra l'utente e il sistema di gestione dell'identità dell'istituzione cui afferisce, riducendo il numero di identità digitali usate.

Il Sistema federato IDEM della rete accademica e della ricerca in Italia consente ai docenti, ai ricercatori e agli studenti delle Università e Istituti di ricerca italiani di accedere con la propria identità digitale istituzionale a risorse digitali condivise¹⁰ tra queste istituzioni, tra quelle aderenti alla rete mondiale EDUGain e con editori commerciali come EBSCO Publishing,¹¹ Elsevier,¹² IEEE Xplore,¹³ Casalini Biblioteca Digitale Torrossa¹⁴ e fornitori di servizi come Proquest¹⁵ e Medialibraryonline (Mloll).¹⁶

Il Sistema di Identità Digitale italiano è di fatto una federazione composta dagli attuali 12 fornitori di identità SPID e dal Ministero degli Interni che rilascia e gestisce la CIE.

L'Unione Europea utilizza l'approccio federato per garantire l'interoperabilità transfrontaliera tra gli Stati membri che adottano differenti schemi di identificazione nazionale (eID Building Block¹⁷). Ogni Paese gestisce un "nodo eIDAS" connesso punto a punto con i corrispettivi nodi di altri Stati a formare una maglia che garantisce l'interoperabilità tecnica e la mappatura tra i diversi sistemi di identificazione nazionali.¹⁸ Quando l'utente accede ad un servizio online trova il link/bottone "Login con eIDAS" (es. accesso all'Anagrafe Nazionale della Popolazione Residente – ANPR¹⁹) che gli permette di scegliere il Paese di provenienza e di essere reindirizzato al corrispondente sistema di identificazione (IdP) per poi essere automaticamente riportato al servizio richiesto²⁰ se l'autenticazione avviene con successo.

I messaggi e l'orchestrazione degli scambi tra le componenti di questi modelli si avvalgono di protocolli e linguaggi standardizzati: Security Assertion Markup Language (SAML) (OASIS Open 2008), OpenId Connect (OIDF 2023) e OAuth 2.0 (IETF 2012). Software open source come Shibboleth²¹ e Central Authentication Service (CAS)²² o proprietari come Microsoft Entra ID²³ forniscono i componenti per l'implementazione di queste architetture. OCLC supporta il modello federato attraverso il componente EZproxy²⁴ che permette l'accesso alle risorse digitali della bi-

¹⁰ Risorse della Federazione IDEM <https://www.idem.garr.it/partecipare/risorse-idem>.

¹¹ Users: Start your research => Use my location => scegliere ente/istituzione di appartenenza <https://www.ebsco.com/news-center/press-releases/ebsco-publishing-and-ebsco-information-services-merge>.

¹² Es. Elsevier ScienceDirect <https://www.sciencedirect.com/>: "SignIn" => "Find your organization".

¹³ "Institutional Sign in" <https://ieeexplore.ieee.org/Xplore/home.jsp>.

¹⁴ <https://access.torrossa.com/it/user/access>: "Accesso Istituzionale Federato".

¹⁵ <https://www.proquest.com/>: "Sign into My Research" => "Find your institution now".

¹⁶ <https://www.medialibrary.it/home/index.aspx>: "Accedi" => "Seleziona un Ente"

¹⁷ <https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eID>.

¹⁸ Mappa delle interconnessioni da e verso l'Italia: <https://eid.ec.europa.eu/efda/browse/notification/eid-chapter-contacts/IT>.

¹⁹ <https://www.anagrafenazionale.interno.it/servizi-al-cittadino/> (Attenzione: dopo aver selezionato il paese di provenienza occorre scorrere tutta l'informativa per sbloccare il bottone e proseguire).

²⁰ Questa infrastruttura è uno dei mattoni base per la costruzione dello Sportello digitale unico (Single Digital Gateway) previsto dal PNRR. <https://www.agid.gov.it/it/agenzia/attuazione-misure-pnrr/sportello-digitale-unico-single-digital-gateway>.

²¹ <https://www.shibboleth.net/>.

²² <http://jasig.github.io/cas/4.0.0/index.html>.

²³ Nome assegnato dal marzo 2024 a Azure Active Directory, il servizio di gestione delle identità e degli accessi in cloud (piattaforma SaaS MS Azure, MS 365, il portale di Azure) e a risorse interne (intranet aziendale) <https://learn.microsoft.com/it-it/entra/fundamentals/whatis>.

²⁴ OCLC sta promuovendo attraverso una serie di webinar questa soluzione che consente anche il monitoraggio statistico dell'accesso alle risorse: <https://www.oclc.org/en/ezproxy.html>.

biblioteca integrando (mediante SAML e LDAP) i sistemi di gestione locali in modo da consentire agli utenti di usare le identità digitali delle proprie istituzioni (es. università).

3.2 La nuova frontiera: gestione dell'identità decentralizzata

Per superare i rischi di sicurezza a cui sono esposti i repository delle identità digitali sta emergendo il modello di gestione decentralizzata o “self-sovereign identity” che elimina i repository delle identità digitali le quali sono direttamente controllate dal soggetto che le detiene per mezzo di un “digital wallet” (portafoglio digitale), una app installata su un dispositivo mobile (es. smartphone) o un servizio in cloud.²⁵ In questa modalità agiscono i seguenti elementi (W3C 2025):

- *Verifiable Digital Credential (VC)* – un insieme di attributi (asserzioni) relativi a una persona, corredati da alcuni metadati che descrivono l'organizzazione che li emette (issuer), la cui provenienza è resa sicura e verificabile mediante tecniche crittografiche, hanno una data di scadenza e possono essere sospese o revocate.
- *Issuer* – organizzazione (PA, banca, università ecc.) che crea le VC, le firma con la propria chiave privata e le rilascia al proprietario/detentore (holder) dopo averlo identificato.
- *Holder* – il soggetto titolare che riceve le VC, le salva nel proprio digital wallet e le usa (presenta) per accedere a servizi e risorse digitali.
- *Digital Wallet (Portafoglio Digitale)* – lo strumento (es. app per dispositivo mobile) che permette di salvare, memorizzare e gestire le credenziali verificabili.
- *Service Provider o Relying Party* – il componente che protegge l'accesso a una risorsa o servizio digitale e che verifica le credenziali digitali presentate dall'utente per decidere se concedergli l'accesso richiesto.

Rispetto ai modelli descritti in precedenza il controllo dell'accesso non si avvale più degli Identity Provider e l'interazione avviene direttamente tra il servizio (Relying Party) e il Portafoglio digitale (Digital Wallet) che l'utente (Holder) usa per esibire le sue credenziali verificabili (VC).

L'implementazione dell'infrastruttura tecnico-funzionale si avvale della crittografia a chiave pubblica, dei protocolli definiti da OpenId per la gestione delle credenziali verificabili²⁶ e di standard per la loro codifica come JSON Web Tokens (JWTs), CBOR Web Tokens (CWTs), JSON Advanced Electronic Signature (JadES) e ISO-18013-5:2021 for Mobile Driving License(mDLs).

4. Verso un nuovo ecosistema di gestione dell'identità digitale

4.1. eIDAS2, EDIW e IT-Wallet

Dal 20 maggio 2024 è entrato in vigore il Regolamento EU 2024/1183, noto come eIDAS2 che ha aggiornato il precedente 910/2014 (eIDAS) per consolidare lo sviluppo di servizi digitali fiduciari (“trusted”) e avviare il processo di armonizzazione dell'identità digitale con l'obiettivo di ridurre i rischi di sicurezza e i costi gestionali derivanti dalle diverse soluzioni adottate dai Paesi europei

²⁵ Il concetto di digital wallet è mutuato dall'ambito del commercio e dei pagamenti elettronici.

²⁶ <https://openid.net/wg/digital-credentials-protocols/digital-credentials-protocols-dcp-working-group-repository2/>.

(European Parliament and Council 2014). Ancor prima, nel 2021, ha preso il via la definizione della Architettura e del Framework di Riferimento (European Commission 2025) dello European Digital Identity Wallet (EDIW), il portafoglio europeo elettronico dell'identità digitale. EDIW segue il modello decentralizzato ed è "un mezzo di identificazione elettronica che consente all'utente di conservare, gestire e convalidare in modo sicuro dati di identità personale e attestati elettronici di attributi al fine di fornirli alle parti facenti affidamento sulla certificazione digitale".²⁷

Un insieme di undici use case concorre a delineare lo spettro di applicazione molto ampio del portafoglio digitale: memorizzare la patente di guida in formato digitale, aprire un conto corrente bancario da remoto, salvare documenti e biglietti di viaggio, apporre firme digitali, registrare attestati e certificazioni di studio, identificarsi e autenticarsi a servizi digitali pubblici e usare identità digitali che attestano l'appartenenza a organizzazioni, enti, associazioni, aziende, catene commerciali. Per esempio le biblioteche potranno rilasciare l'equivalente digitale delle tessere analogiche di iscrizione dei propri utenti sotto forma di attestazioni elettroniche di attributi. Per ciascuno degli scenari individuati sono in corso sperimentazioni attraverso progetti pilota²⁸ e la roadmap completa delle implementazioni è in liberamente consultabile.²⁹

Il 4 dicembre 2024 la Commissione EU ha pubblicato i primi cinque Atti implementativi (Implementing regulations)³⁰ che definiscono standard, specifiche e procedure relative alla funzionalità tecniche dei wallet e al processo di certificazione necessario per garantire che i wallet siano sicuri e proteggano i dati personali degli utenti.³¹

Per quanto riguarda l'identificazione digitale il Framework di Riferimento prevede che l'accesso ai servizi pubblici e privati avvenga presentando dei Person Identification Data (PID), insiemi di dati identificativi che consentono di stabilire l'identità di una persona fisica o giuridica o di una persona fisica che rappresenta una persona giuridica. I PID sono accompagnati da metadati che identificano il fornitore responsabile dell'emissione e della revoca di questi dati, al quale spetta assicurare che il PID di un utente sia crittograficamente legato al suo wallet. Attribuiti (cfr. Tabella 1), formati e codifiche dei PID sono definiti nel Regolamento EU (European Commission 2024).

Il Regolamento eIDAS2 prescrive che ciascun Stato membro debba fornire almeno un portafoglio europeo di identità digitale entro 24 mesi dal 20 maggio 2024, il cui uso è comunque facoltativo poiché viene mantenuta la possibilità di accedere ai servizi pubblici e privati con altri mezzi di identificazione e autenticazione esistenti. La normativa inoltre stabilisce che l'emissione dei portafogli digitali, l'utilizzo e la revoca devono essere gratuite, che gli Stati Membri devono prevedere meccanismi di convalida gratuiti e che il codice sorgente dei componenti software dei wallet sia rilasciato con licenza open source.

²⁷ Cfr. punto 42) aggiunto dal Regolamento EU 2024/1183 al regolamento (UE) n. 910/2014.

²⁸ <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects>.

²⁹ <https://github.com/eu-digital-identity-wallet/eudi-wallet-reference-implementation-roadmap>.

³⁰ <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+milestone+reached+as+Commission+adopts+implementing+regulations>.

³¹ Il 26 giugno 2025 sono stati rilasciati in pubblica consultazione fino al 15 luglio ulteriori 3 Atti: <https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/New+batch+of+Implementing+Acts+published+for+feedback>.

A livello normativo l'Italia ha recepito il regolamento eIDAS2 con la Legge 29 aprile 2024 che ha aggiunto al CAD il nuovo l'Art. 64-quater "Sistema di portafoglio digitale italiano – Sistema IT-Wallet". Al livello pratico la versione corrente della AppIO consente di scaricare e memorizzare la versione digitale della patente di guida, della tessera sanitaria e la Carta Europea della Disabilità³² e rappresenta la prima istanza dell'IT-Wallet. Al 28 giugno 2025 gli utenti di AppIO attivi negli ultimi 12 mesi erano 12 milioni (con 4.4 milioni di patenti di guida digitali, 4.8 milioni di tessere sanitarie e 0.1 milioni di Disability Card scaricate).³³ In tempi successivi sono pianificati il caricamento della CIE, del passaporto, della tessera elettorale, del certificato di nascita e di titoli di studio. Entro il 2026 (scadenza del PNRR) è pianificata l'integrazione con EDIW.³⁴

4.2 Prepararsi al cambiamento tra luci e ombre

Il percorso per lo sviluppo e l'avvio di EDIW e di IT-Wallet è in itinere. Le Linee Guida AgID³⁵ per "disciplinare gli standard tecnologici e le soluzioni tecniche ed organizzative" la cui pubblicazione secondo l'Art. 64-quater comma 3 del CAD doveva avvenire entro sessanta giorni dall'entrata in vigore (1 Maggio 2024) ancora non sono state pubblicate. Questo ritardo avrà un impatto sul processo di attuazione soprattutto per quanto riguarda il coinvolgimento del settore privato per la produzione di portafogli digitali (wallet) e per la fornitura/emissione di attestati elettronici di attributi. Gli operatori economici devono infatti disporre di un quadro di riferimento chiaro (regole e procedure) dal momento che queste attività, sempre in base all'Art. 64-quater, sono sottoposte a accreditamento.³⁶

Predisporre alla trasformazione implica che tutti i soggetti coinvolti (privati cittadini, PA centrali e locali, operatori commerciali) acquisiscano la consapevolezza delle opportunità e delle complessità che questa evoluzione comporta.

Il principale vantaggio del Sistema IT-Wallet è la riduzione delle criticità di sicurezza e degli oneri di protezione degli attuali sistemi di gestione delle identità digitali basati sulle password. Per il momento è prematuro prevedere per quanto tempo, dopo il 2026, l'ecosistema di gestione delle identità digitali manterrà operative tutte e tre le modalità SPID, CIE, IT-Wallet. L'autenticazione tramite CIE confluirà nel IT-Wallet che tuttavia non è uno strumento obbligatorio. La sostenibilità economica avrà un peso significativo sull'assestamento degli scenari futuri.³⁷

L'adozione e la diffusione dell'IT-Wallet dovrà essere accompagnata da un efficace e ampia attività

³² <https://ioapp.it/documenti-su-io/>.

³³ <https://ioapp.it/numeri>.

³⁴ I soggetti attuatori sono PagoPA e IPZS, di concerto con AgID e l'Autorità Nazionale per la Cybersicurezza (ACN).

³⁵ <https://www.agid.gov.it/it/piattaforme/it-wallet>.

³⁶ Una prima versione delle Specifiche Tecniche è disponibile a: <https://italia.github.io/eid-wallet-it-docs/versione-corrente/en/index.html>. Queste forniscono raccomandazioni, requisiti e risorse relative al sistema IT-Wallet e quando saranno formalmente adottate insieme alle Linee Guida costituiranno il quadro di riferimento che regolerà il Sistema IT-Wallet.

³⁷ Con il comunicato del 5 marzo 2025 (<https://innovazione.gov.it/notizie/comunicati-stampa/identita-digitale-firmato-il-decreto-che-assegna-40-milioni-di-euro-ai-gestori-spid>) il Sottosegretario alla Presidenza del Consiglio con delega all'Innovazione, Alessio Butti, ha annunciato la firma del Decreto che assegna 40 milioni di euro agli operatori impegnati nell'erogazione di SPID per garantirne "continuità e sostenibilità, comunque due di loro (Aruba e InfoCert) per lo SPID ad uso personale, dopo il primo anno gratuito, hanno introdotto un costo dal secondo anno.

di informazione, sensibilizzazione e promozione delle politiche di adozione. I decisori politici delle PA locali dovranno percepire questa trasformazione non come un mero adempimento da attuare al livello minimo indispensabile, ma come una scelta strategica per la costruzione dell'ecosistema di servizi digitali affidabili che è la finalità ultima di eIDAS2. IT-Wallet, evoluzione di App IO, sarà il portafoglio digitale conforme a EDIW rilasciato dallo Stato italiano come previsto dalla normativa italiana, ma gli operatori commerciali dovranno essere stimolati e agevolati per sostenere gli investimenti necessari affinché l'adozione del portafoglio non resti confinata al solo ambito dei servizi delle PA. A tal fine sarà necessario individuare e fissare criteri che consentano lo sviluppo di un modello commerciale per il rilascio dei portafogli digitali conformi a EDIW e che rispetti le prescrizioni del Regolamento eIDAS2 sulla gratuità di alcuni servizi. Questa non è un'incongruenza poiché la normativa circoscrive il contesto assegnando agli Stati il compito di fornire strumenti gratuiti per verificare la validità e l'autenticità degli EDIW, per verificare l'autenticità e la validità delle identità digitali delle "relying parties", stabilisce che per le persone fisiche ("natural person") le firme digitali e le operazioni di emissione, uso e revoca degli EDIW siano gratuite. Si tratterà dunque di disegnare uno scenario che da un lato non comporti costi per i privati cittadini (persone fisiche) e dall'altro assicuri la sostenibilità economica dell'intero sistema attraverso modalità di tariffazione da applicare all'utilizzo da parte dei professionisti e delle aziende, differenziando tra l'uso di attestazioni qualificate e non qualificate e tenendo conto della tipologia dei soggetti che le emettono e dei servizi cui si vuole accedere.

Infine, i cittadini dovranno essere accompagnati affinché il portafoglio di identità digitale non sia destinato solo agli utenti tecnicamente più evoluti. Per questo sarà necessario dedicare una particolare cura all'usabilità dei wallet, alla formazione e al supporto agli utenti prevedendo "punti di facilitazione digitale" diffusi sul territorio³⁸.

Le biblioteche possono cogliere l'opportunità di inserirsi in questo percorso evolutivo con più ruoli: avvalersi delle attestazioni digitali e dei PID per aggiornare i propri sistemi di controllo dell'accesso al fine di ridurre il rischio di attacchi informatici, rilasciare attestazioni digitali dell'iscrizione ai propri utenti fruibili in vari circuiti (es. eventi culturali, spettacoli, librerie ecc.), svolgere funzioni di reference per i cittadini. Le biblioteche che hanno già integrato i servizi digitali con SPID e CIE sono avvantaggiate nel cambiamento poiché in gran parte si sono avvalse di sistemi federati di ambito territoriale (es. FedERa per l'Emilia Romagna, le analoghe infrastrutture della Regione Toscana e della Regione Veneto o di alcuni Comuni) che potrebbero adeguare le loro funzioni di gateway al fine di semplificare l'integrazione con i servizi di emissione e verifica delle attestazioni di attributi digitali. Altresì le biblioteche pubbliche potrebbero estendere le loro funzioni di reference desk assumendo il ruolo di facilitatori digitali (informazioni, assistenza operativa ecc.) verso i cittadini nella fase di accompagnamento post rilascio dell'IT-Wallet e dei portafogli accreditati.

La trasformazione è appena avviata, il percorso non è breve e presenta degli ostacoli, ma occorre predisporre per affrontarlo senza precondizionamenti, seguendone le evoluzioni e valutando strada facendo le opportunità offerte da questa innovazione.

³⁸ Il progetto "Rete dei servizi di facilitazione digitale" (Misura 1.7.2 del PNRR) prevede la costituzione di tremila presidi "Digitale facile" per accrescere le competenze e l'inclusione digitale di oltre 2 milioni di cittadini entro il 2026: <https://repubblicadigitale.gov.it/portale/progetti-del-dipartimento/rete-dei-servizi-di-facilitazione-digitale>.

Riferimenti bibliografici*

BL (British Library). 2024. *Learning lessons from the cyber-attack*. British Library cyber incident review, 8 marzo. <https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf/>.

Clusit (Clusit - Associazione Italiana per la Sicurezza Informatica). 2025. *Rapporto Clusit sulla Cybersecurity in Italia e nel mondo 2025*. Astrea. https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_03-2025_web.pdf.

Codice per l'amministrazione digitale. D.Lgs. 7 marzo 2005, n. 82 e successive modifiche. <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82>.

European Commission. 2024. *CIR 2024/2977, Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards person identification data and electronic attestations of attributes issued to European Digital Identity Wallets*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402977.

European Commission. 2025. *European Digital Identity Wallet Architecture and Reference Framework*. <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/>.

European Parliament and Council. 2014. *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02014R0910-20241018>.

Grove, Jack. 2024. "How the British Library cyberattack disrupted research." *Times Higher Education*, 21 novembre. <https://www.timeshighereducation.com/depth/how-british-library-cyberattack-disrupted-research>.

IETF (Internet Engineering Task Force). 2000. *RFC 2798 Definition of the inetOrgPerson LDAP Object Class*. <http://tools.ietf.org/html/rfc2798>.

IETF (Internet Engineering Task Force). 2006a. *RFC 4519 Lightweight Directory Access Protocol (LDAP): Schema for User Applications*. <http://tools.ietf.org/html/rfc4519>.

IETF (Internet Engineering Task Force). 2006b. *RFC 4524 COSINE LDAP/X.500 Schema*. <http://tools.ietf.org/html/rfc4524>.

IETF (Internet Engineering Task Force). 2012. *The OAuth 2.0 Authorization Framework*. Internet Engineering Task Force (IETF) Request for Comments 6749. <https://datatracker.ietf.org/doc/html/rfc6749>.

Kime, Chad. 2024. *6 Best Enterprise Password Managers for 2024*. *eSecurity Planet*. <https://www.esecurityplanet.com/products/best-password-managers/>.

OASIS Open. 2008. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, OASIS Security Services TC Draft 02. <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html>.

* Ultimo accesso di tutti i riferimenti online, compresi quelli citati nelle note, il 31 marzo 2025.

OIDF (OpenID Foundation). 2023. *OpenID Connect Core 1.0 incorporating errata set 2*. https://openid.net/specs/openid-connect-core-1_0.html.

REFEDS (Research and Education FEDerations). 2022. *SCHAC – SCHEMA for Academia*. <https://wiki.refeds.org/display/STAN/SCHAC>.

REFEDS (Research and Education FEDerations). 2023. *EduPerson Object Class Specification*. <https://wiki.refeds.org/display/STAN/eduPerson>

W3C (World Wide Web Consortium). 2025. *Verifiable Credentials Data Model v2.0*. W3C Proposed Recommendation. <https://www.w3.org/TR/vc-data-model-2.0/>.