assonime

Associazione fra le società italiane per azioni

APPROFONDIMENTI

N. 4 DEL 2023

Raggiunto l'accordo sulla proposta di regolamento UE che istituisce un quadro per un'identità digitale europea

1. Introduzione

Lo scorso 8 novembre, nell'ambito del Trilogo europeo[1], è stato raggiunto l'accordo definitivo sulla proposta di regolamento del Parlamento europeo e del Consiglio, che modifica il regolamento eIDAS[2], istituendo un quadro di regole per un'identità digitale europea. L'accordo segna la tappa decisiva di un iter legislativo iniziato nel giugno 2021 con la presentazione della proposta di regolamento da parte della Commissione europea[3]. Il testo della proposta su cui è stato raggiunto l'accordo è stato approvato il 7 dicembre scorso da parte della commissione ITRE del Parlamento europeo e dovrà ora essere votato dal Parlamento in sessione plenaria. La data per la votazione in plenaria è prevista per il 26 febbraio 2024[4]. In caso di approvazione da parte del Parlamento il testo passerà al Consiglio UE che procederà all'adozione formale del regolamento.

La proposta di regolamento è volta alla creazione di uno strumento europeo di identità digitale armonizzato**,** basato sul concetto di portafoglio europeo di identità digitale "EUDI wallet", che mira a garantire a cittadini e imprese la disponibilità e l'uso di soluzioni di identità digitale, per accedere con un alto livello di sicurezza e tutela della privacy, a servizi pubblici e privati, anche a livello transfrontaliero.

L'iniziativa è diretta a sostenere la trasformazione dell'Unione europea verso un mercato unico digitale riducendo le barriere digitali tra gli Stati membri e potenziando i benefici della digitalizzazione a vantaggio di cittadini e imprese. In questa prospettiva, oltre a introdurre l'EUDI wallet, la proposta di regolamento semplifica anche il processo di notifica dei regimi nazionali di identificazione elettronica, istituiti dal regolamento eIDAS. Inoltre, sono ridefinite le attività rientranti nei "servizi fiduciari" e vengono introdotti nuovi servizi, tra cui in particolare, il rilascio e la convalida di attestati elettronici di attributi, che rilevano per il funzionamento dell'EUDI wallet.

Per garantire un approccio comune nella realizzazione del quadro europeo dell'identità digitale la Commissione ha emanato insieme alla proposta di regolamento una raccomandazione con la quale gli Stati membri sono stati invitati a definire un pacchetto di strumenti che prevede: un'architettura tecnica, standards, orientamenti

[1] Negoziato interistituzionale europeo che riunisce i rappresentanti del Parlamento europeo, del Consiglio UE e della Commissione europea.
[2] Regolamento UE n. 910/2014.
[3] COM (2021) 281 def.
[4] Cfr. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0136(COD)&l=en.

comuni e best practices[5]. Gli esperti dei paesi membri (eIDAS expert group) hanno elaborato, in stretto coordinamento con la Commissione, due documenti: il primo documento "European Digital Identity, Architecture and Reference Framework" è stato pubblicato nel febbraio 2022[6], il secondo "*The common union toolbox for a coordinated approach towards a european digital identity framework*", è stato pubblicato nel gennaio 2023[7]. L'eIDAS expert group sta proseguendo i suoi lavori e sono attese ulteriori pubblicazioni che terranno conto del testo della proposta di regolamento su cui è stato raggiunto l'accordo.

Nel dicembre 2023 la Commissione europea ha assegnato a quattro consorzi internazionali[8] il bando lanciato nel febbraio 2022, per lo sviluppo di progetti pilota destinati a sperimentare il wallet su una serie di *use cases* verticali. La sperimentazione avrà una durata di almeno due anni e riguarda undici casi d'uso prioritari relativi sia a servizi pubblici che privati, con interazioni nazionali e transfrontaliere[9]. I quattro progetti pilota finora avviati collaboreranno strettamente tra loro e con la Commissione, e i loro risultati confluiranno nelle specifiche tecniche per l'EUDI wallet, in corso di elaborazione da parte dell'eIDAS expert group.

In questa nota illustriamo le principali disposizioni relative all'EUDI wallet e agli attestati elettronici di attributi, contenute nel testo della proposta approvato nell'ambito del Trilogo[10], aggiornando l'approfondimento Assonime n. 5/2022, che descriveva il testo su cui era stato adottato l'orientamento generale del Consiglio UE nel dicembre 2022.

[5] Raccomandazione (UE) 2021/946 del 3 giugno 2021, relativa a un pacchetto di strumenti comuni dell'Unione per un approccio coordinato verso un quadro europeo relativo a un'identità digitale".

[6] Cfr. file:///C:/Users/aoresta/Downloads/Outline_final_en0ZKkyLuysLYLJtiqqToEokvk_83643.pdf.

[7] Cfr. file:///C:/Users/aoresta/Downloads/0000720132-2023-I078-00041-PR-005.pdf.

[8] I consorzi sono: Potential (Pilots for European Digital Identity Wallet Consortium). A questo riguardo, in Italia, la Provincia autonoma di Trento ha deliberato la propria partecipazione a questo progetto pilota in qualità di partner; EWC (EU Digital Identity Wallet Consortium), NOBID (Nordic-Baltic eID Wallet Consortium), DC4EU (Digital Credentials for Europe Consortium).

[9] Gli undici casi d'uso in fase di sperimentazione sono i seguenti: accesso ai servizi pubblici; apertura di un conto bancario; registrazione di una carta SIM; patente di guida mobile; firme elettroniche; prescrizioni mediche elettroniche; conservazione e visualizzazione delle credenziali di viaggio digitali; organizzazione dei wallet; organizzazione dei pagamenti; uso del wallet per l'autorizzazione dei pagamenti per prodotti e servizi, da parte dell'utente del wallet; uso del wallet nel settore dell'istruzione e della sicurezza sociale. Cfr. EU Digital identity: 4 projects launched to test EUDI Wallet | Shaping Europe's digital future (europa.eu).

[10] Cfr. https://www.europarl.europa.eu/cmsdata/278103/eIDAS-4th-column-extract.pdf.

2. La disciplina dell'EUDI wallet

Definizione e funzionalità

L'EUDI wallet viene definito come uno strumento di identificazione elettronica che consente all'utente di conservare, gestire e convalidare, in modo sicuro, dati di identità e attestati elettronici di attributi, per presentarli alle *relying parties* e agli altri utenti dell'EUDI wallet, e per firmare con firme elettroniche qualificate o sigilli elettronici qualificati. A quest'ultimo riguardo, si evidenzia che la possibilità di sottoscrivere con firme elettroniche qualificate è offerta a tutte le persone fisiche di default e in modo gratuito, ma gli Stati membri devono disporre specifiche misure per assicurare che l'uso gratuito delle firme sia solo per scopi non professionali.

Il wallet darà la possibilità alle persone fisiche e giuridiche di svolgere una numerosa serie di attività. In particolare, esso permetterà di richiedere, ottenere, combinare, conservare, cancellare, condividere e presentare, in modo sicuro e sotto l'esclusivo controllo dell'utente, dati di identificazione personale e attestati elettronici di attributi, per autenticarsi presso le *relying parties*, *on line* e, se appropriato, *off line*, al fine di utilizzare servizi pubblici e privati, assicurando al contempo che sia possibile la *disclosure* selettiva dei dati nel rispetto del principio di minimizzazione del dato a tutela della privacy. In particolare, l'uso *off line* del wallet è importante in molti settori, come quello sanitario, in cui i servizi sono spesso forniti attraverso l'interazione "faccia a faccia" e le prescrizioni elettroniche dovrebbero poter fare affidamento su QR-codes o tecnologie simili per verificare l'autenticità.

Inoltre, attraverso il wallet, si potranno generare pseudonimi e conservarli, sulla base del principio espresso nel testo di compromesso, secondo cui l'uso di pseudonimi scelti dall'utente non è proibito. Sono fatte salve le norme UE o nazionali che richiedono agli utenti di identificare sé stessi e gli effetti legali che gli pseudonimi hanno nelle legislazioni nazionali.

È prevista anche la possibilità di ricevere e scambiare in modo sicuro dati di identità e attesti elettronici di attributi tra due wallets, nonché di autenticare in maniera sicura il wallet di un'altra persona. L'utente avrà traccia di tutte le operazioni effettuate attraverso il wallet e potrà fare il download dei propri dati e degli attestati elettronici di attributi. Infine, viene riconosciuto che il wallet consenta all'utente di esercitare il diritto alla portabilità dei dati, favorendo così la possibilità di passare da un wallet all'altro, laddove lo Stato membro abbia adottato più di una soluzione di wallet.

Gli Stati membri possono anche prevedere, nel rispetto della disciplina nazionale, e conformemente agli specifici requisiti previsti per l'EUDI wallet, ulteriori funzionalità relative al wallet, tra cui, in particolare, l'interoperabilità con gli esistenti sistemi nazionali di identificazione elettronica.

È stabilito, infine, che entro sei mesi dall'entrata in vigore del regolamento, la Commissione adotti atti esecutivi che stabiliscono standards di riferimento e, se necessario, specifiche e procedure per l'attuazione dell'EUDI wallet.

I soggetti e le regole per l'emissione del wallet

Ogni Stato membro deve garantire alle persone fisiche e giuridiche la disponibilità almeno di un EUDI wallet, entro 24 mesi dall'entrata in vigore degli atti di esecuzione, per garantire che queste abbiano un accesso sicuro, affidabile e transfrontaliero a servizi pubblici e privati, assicurando al tempo stesso il pieno controllo sui propri dati. In particolare, i wallets possono essere emessi direttamente dallo Stato membro, dai soggetti delegati dagli stessi, o sono emessi a titolo indipendente rispetto ad uno Stato membro, ma devono essere riconosciuti da esso.

L'uso dell'EUDI wallet rimane volontario, senza pregiudizio della possibilità di accedere a servizi pubblici e privati attraverso altri sistemi esistenti di identificazione elettronica. Il rilascio, l'uso e la revoca del wallet saranno gratuiti per tutte le persone fisiche.

Gli Stati membri dovranno fornire in modo gratuito un meccanismo di convalida volto ad assicurare che l'autenticità e la validità del wallet possano essere verificate, e a consentire agli utenti del wallet di verificare l'autenticità e la validità delle identità delle *relying parties* registrate. Inoltre, gli Stati membri dovranno prevedere strumenti per la revoca della validità del wallet nei seguenti casi: esplicita richiesta dell'utente; quando la sicurezza del wallet è stata compromessa; nel caso di morte dell'utente o cessazione dell'attività della persona giuridica.

Resta fermo il principio per cui l'EUDI wallet viene emesso nell'ambito di un regime nazionale di identificazione elettronica notificato, il cui livello di garanzia è elevato. A questo riguardo, è prevista l'emanazione di atti esecutivi da parte della Commissione, volti a facilitare l'*on-boarding* nel wallet con strumenti di identificazione con livello di garanzia significativo, attraverso misure complementari di verifica dell'identità che assicurano il raggiungimento del livello elevato. Questa previsione va incontro alle richieste di alcuni Stati membri, tra cui l'Italia, che hanno già rilasciato un numero considerevole di mezzi nazionali di identificazione elettronica con livello di garanzia

significativo: in Italia vi sono oltre 33 milioni di identità SPID finora rilasciate con questo livello di sicurezza che dovranno "migrare" verso un livello di sicurezza superiore.

Gli aspetti di privacy e la certificazione del wallet

Uno degli aspetti più rilevanti del funzionamento del wallet riguarda la tutela della privacy. In particolare, viene assicurato che l'utente conservi il pieno controllo dell'uso del wallet e dei dati in esso contenuti, compresa la possibilità di selezionare quali dati condividere in quanto strettamente funzionali all'accesso a un determinato servizio.

Restano sostanzialmente invariate le regole previste nelle precedenti bozze di proposta, per il soggetto che emette il wallet. Quest'ultimo è tenuto a non raccogliere informazioni sull'uso dello stesso che non sono necessarie per la prestazione dei servizi del wallet, né combina i dati di identificazione personali e altri dati personali conservati nel wallet o connessi al suo uso, con i dati personali provenienti da altri servizi offerti dallo stesso soggetto emittente o da servizi di terzi, che non sono necessari per la prestazione dei servizi del wallet, a meno che l'utente non lo abbia richiesto espressamente. Inoltre, il soggetto che emette il wallet dovrà tenere i dati personali relativi al wallet separati dagli altri dati dallo stesso detenuti.

Per garantire un livello elevato di sicurezza e protezione dei dati, la proposta di regolamento prevede un sistema di certificazione dell'EUDI wallet. In particolare, la conformità dei wallets e dei regimi di identificazione elettronica in base ai quali essi sono emessi, con gli specifici requisiti previsti nella proposta di regolamento, viene certificata da organismi di valutazione della conformità designati dagli Stati membri. Entro sei mesi dall'entrata in vigore del regolamento la Commissione dovrà emanare atti di esecuzione contenenti standard di riferimento, e se necessario, specifiche e procedure, per la certificazione del wallet.

La certificazione della conformità dei wallets ai requisiti sopra indicati, rilevanti per la cybersecurity è effettuata in conformità ai sistemi di certificazione della cybersecurity adottati ai sensi del regolamento (UE) 2019/881. Per i requisiti non connessi alla cybersecurity e per i requisiti connessi alla cybersecurity ma non coperti dai sistemi di certificazione di cybersecurity, gli Stati membri istituiscono sistemi di certificazione nazionali seguendo le previsioni stabilite negli atti di esecuzione sopra citati.

Relying parties

La "*relying party*" è definita come una persona fisica o giuridica che fa affidamento su un'identificazione elettronica, sull'EUDI wallet o altro strumento di identificazione elettronica, o su un servizio fiduciario.

Nel caso in cui le *relying parties* vogliano fare affidamento sull'EUDI wallet per fornire servizi pubblici o privati, devono registrarsi nello Stato membro in cui sono stabilite. La procedura di registrazione deve essere economicamente vantaggiosa e proporzionata al rischio e garantire che le *relying parties* forniscano almeno i seguenti dati: informazioni necessarie per autenticarsi nell'EUDI wallet; informazioni di contatto; la destinazione d'uso del wallet e i dati da richiedere. Restano impregiudicati ulteriori requisiti previsti dalla normativa UE o nazionale, per la fornitura di specifici servizi.

Quando intendono fare affidamento sul wallet, le *relying parties* devono identificare sé stesse all'utente del wallet. Inoltre, esse sono responsabili per lo svolgimento delle procedure di autenticazione e validazione dei dati di identificazione personale e delle attestazioni elettroniche di attributi, richieste dai wallets. Le *relying parties* non possono rifiutare l'uso di pseudonimi quando l'identificazione dell'utente non è richiesta dalla normativa UE o nazionale. Viene specificato che gli intermediari che agiscono per conto delle *relying parties* devono essere considerati anch'essi come *relying parties*.

Entro sei mesi dall'entrata in vigore del regolamento, la Commissione stabilirà attraverso atti esecutivi le specifiche tecniche e operative riguardo alle previsioni relative alle *relying parties.*

Utilizzo transfrontaliero

Riguardo all'utilizzo transfrontaliero degli EUDI wallets, è previsto che, quando gli Stati membri richiedono l'identificazione e l'autenticazione elettronica per accedere ai servizi *on line* prestati da un organismo del settore pubblico, essi accettano anche gli EUDI wallets.

Per essere ampiamente disponibili e utilizzabili, gli EUDI wallets devono essere accettati dai prestatori di servizi privati. In questo senso la proposta di regolamento dispone che le *relying parties* private che forniscono servizi, ad eccezione delle microimprese e delle piccole imprese, accettano anche l'EUDI wallet, esclusivamente su richiesta volontaria dell'utente, nei casi in cui la normativa UE o nazionale o gli obblighi contrattuali, impongono un'autenticazione forte dell'utente per l'identificazione

on line. Questa disposizione riguarda, in particolare, i servizi nei seguenti settori: trasporti, energia, banche, servizi finanziari, sicurezza sociale, sanità, acqua potabile, servizi postali, infrastruttura digitale, istruzione, telecomunicazioni. A questo riguardo, nei considerando della proposta viene specificato che per agevolare l'uso e l'accettazione del wallet è opportuno tener conto delle norme e delle specifiche tecniche settoriali.

Viene, infine, stabilito che nei casi in cui le piattaforme *on line* di dimensioni molto grandi, come definite nel "Digital Services Act"[11], impongono agli utenti di autenticarsi per accedere ai servizi *on line*, esse devono accettare e facilitare anche l'uso dell'EUDI wallet per l'autenticazione dell'utente, esclusivamente su richiesta volontaria dell'utente e nel rispetto del principio di minimizzazione dei dati necessari per lo specifico servizio *on line* per cui è richiesta l'autenticazione.

3. Attestati elettronici di attributi

La proposta di regolamento amplia il novero delle attività che rientrano nella definizione di "servizi fiduciari" [12], prevedendo, tra gli altri, il rilascio e la convalida di attestati elettronici di attributi, che rilevano per il funzionamento dell'EUDI wallet[13].

L'attributo è definito come la caratteristica, la qualità, il diritto o l'autorizzazione di una persona fisica o giuridica o di un oggetto. L'attestato elettronico di attributi è definito come un attestato in forma elettronica che consente l'autenticazione di attributi, a cui non sono negati gli effetti giuridici e l'ammissibilità come prova nei procedimenti giudiziali per il solo motivo della sua forma elettronica.

Gli attestati elettronici di attributi possono essere rilasciati da prestatori di servizi fiduciari non qualificati[14]. A questo proposito nel framework elaborato dall'eIDAS expert

[11] Regolamento (UE) 2022/2065, articolo 33. Per un commento al regolamento cfr. circolare Assonime n. 17/2023.

[12] Ai sensi del regolamento eIDAS, i servizi fiduciari sono definiti come servizi forniti normalmente dietro remunerazione e relativi alla: creazione di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi di recapito certificato e certificati relativi a questi servizi; creazione, verifica e convalida di certificati di autenticazione di siti web; conservazione di firme, sigilli o certificati elettronici relativi a questi servizi.

[13] Oltra ad una nuova formulazione di tutti i servizi ricompresi nella definizione di servizi fiduciari, sono introdotti i seguenti nuovi servizi: gestione di dispositivi per la creazione di una firma elettronica a distanza o per la creazione di un sigillo a distanza; archiviazione elettronica di dati elettronici; registrazione di dati elettronici in un registro elettronico.

[14] La proposta di regolamento introduce una nuova disposizione che prevede specifici adempimenti per i prestatori di servizi fiduciari non qualificati.

group, pur mantenendo la supervisione di questi prestatori nell'ambito del regolamento eIDAS, viene avanzata l'ipotesi che si possa far riferimento anche ad altri quadri normativi o accordi contrattuali riguardo alle regole per la fornitura, l'uso e il riconoscimento di questi attestati, in ambiti come quello delle patenti di guida, dei titoli di studio e dei pagamenti digitali.

L'attestato elettronico di attributi qualificato è un attestato rilasciato da un prestatore di servizi fiduciari qualificato[15], che soddisfa specifici requisiti. Quando viene rilasciato in uno Stato membro è riconosciuto come attestato qualificato anche in tutti gli altri Stati membri. Un attestato elettronico di attributi qualificato ha gli stessi effetti giuridici degli attestati in formato cartaceo rilasciati legalmente.

L'attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica[16], o per suo conto, che rispetta determinati requisiti, come previsto per gli attestati di attributi qualificati, ha gli stessi effetti giuridici dell'attestato in formato cartaceo rilasciato legalmente ed è riconosciuto come tale in tutti gli Stati membri.

Per determinati attributi che si basano su fonti autentiche all'interno del settore pubblico, gli Stati membri devono consentire ai prestatori qualificati di attestati elettronici di attributi di verificare questi attributi rispetto alle fonti autentiche mediante mezzi elettronici, su richiesta dell'utente e in conformità con il diritto nazionale o dell'Unione.

Quando una norma nazionale richiede l'identificazione elettronica attraverso strumenti di identificazione elettronica e autenticazione per accedere ai servizi pubblici, i dati di identificazione personale contenuti nell'attestazione elettronica di attributi non sostituiscono la specifica identificazione elettronica richiesta, a meno che sia permesso in modo esplicito dallo Stato membro.

[15] Ai sensi del regolamento eIDAS, il prestatore di servizi fiduciari qualificato è un prestatore che fornisce uno o più servizi fiduciari qualificati e la cui qualifica come prestatore qualificato è assegnata da un organismo di vigilanza. La disciplina di questi prestatori è oggetto di molte modifiche da parte della proposta di regolamento.

[16] La fonte autentica è definita nella proposta di regolamento come un archivio o un sistema, tenuto sotto la responsabilità di un organismo del settore pubblico o di un soggetto privato, che contiene e fornisce gli attributi relativi ad una persona fisica o giuridica ed è considerato una fonte primaria di tali informazioni, o la cui autenticità è riconosciuta conformemente al diritto dell'Unione o nazionale, inclusa la prassi amministrativa.

Gli attestati elettronici di attributi rilasciati per il wallet

I prestatori di attestati elettronici di attributi danno la possibilità agli utenti dell’EUDI wallet di chiedere, ottenere, conservare e gestire gli attestati elettronici indipendentemente dagli Stati membri in cui il wallet è stato emesso. I prestatori di attestati elettronici di attributi qualificati, così come disposto per gli organismi del settore pubblico responsabili di una fonte autentica, sono tenuti a fornire un’interfaccia con gli EUDI wallets.

A tutela dei dati personali relativi agli attestati elettronici è disposto che i prestatori di servizi di attestazione elettronica di attributi qualificati e non qualificati sono tenuti a non combinare i dati personali relativi alla prestazione di questi servizi con i dati personali provenienti da qualsiasi altro servizio offerto da loro o dai loro partner commerciali. Infine, è previsto che i dati personali relativi alla fornitura di servizi di attestazione elettronica degli attributi devono essere mantenuti separati dagli altri dati detenuti dal prestatore del servizio elettronico di attestazione di attributi.