assonime

Associazione fra le società italiane per azioni

APPROFONDIMENTI

N. 5 DEL 2022

La proposta di regolamento UE che istituisce un quadro per un'identità digitale europea

ASSONIME - Riproduzione riservata

1. Introduzione

Nel giugno 2021 la Commissione europea ha presentato una proposta di regolamento[1] che modifica il regolamento eIDAS[2], istituendo un quadro normativo per la creazione di uno strumento europeo di identità digitale armonizzato**,** basato sul concetto di portafoglio europeo di identità digitale "EUDI wallet". Questo strumento è volto ad assicurare il corretto funzionamento del mercato interno garantendo a cittadini e imprese la disponibilità e l'uso di soluzioni di identità digitale, altamente sicure e affidabili, per l'accesso a servizi pubblici e privati, anche a livello transfrontaliero[3].

In particolare, l'EUDI wallet risponde alle esigenze emerse dall'attuale contesto socio-economico in cui è aumentata in maniera considerevole la digitalizzazione di tutti gli aspetti della società, a cui la crisi pandemica ha impresso un'ulteriore accelerazione. Nello specifico, la prestazione di servizi pubblici e privati è diventata sempre più digitale ed è di conseguenza cresciuta la domanda di mezzi per identificarsi e autenticarsi online, così come per scambiare digitalmente informazioni relative all'identità, attributi o qualifiche, in maniera sicura e con un livello elevato di protezione dei dati. Ciò ha innescato un cambiamento di paradigma che sta orientando sia il mondo privato che le PA verso soluzioni avanzate e pratiche, in grado di integrare diversi dati e certificati verificabili dell'utente. Si tratta di wallets basati su app e gestiti attraverso il dispositivo mobile dell'utente che consentono un accesso sicuro e facile a diversi servizi pubblici e privati.

In questo contesto l'EUDI wallet può costituire uno strumento di identità digitale unico a livello europeo, capace di assicurare un alto livello di sicurezza e tutela della privacy nell'accesso ai servizi, pubblici e privati, anche a livello transfrontaliero, in particolare, garantendo all'utente il pieno controllo della condivisione dei propri dati, compresa la possibilità di selezionare quali dati condividere in quanto strettamente funzionali all'accesso ad un determinato servizio.

Per garantire un approccio comune nella realizzazione del quadro europeo dell'identità digitale la Commissione europea insieme alla proposta di regolamento, ha emanato

[1] COM (2021) 281 def.

[2] Regolamento UE n. 910/2014.

[3] Cfr. Comunicazione della Commissione "Plasmare il futuro digitale dell'Europa" (COM (2020) 67 def.), in cui si annunciava la revisione del regolamento eIDAS con l'obiettivo di migliorarne l'efficacia, estenderne i benefici al settore privato e promuovere identità digitali affidabili per tutti gli europei. Cfr. anche la Comunicazione "Bussola per il digitale 2030: il modello europeo per il decennio digitale" (COM (2021) 118 def.), nel quale è fissato l'obiettivo per il 2030 di istituire un quadro europeo che porti ad un'ampia diffusione di un'identità digitale affidabile e controllata dagli utenti, che permetta agli stessi di utilizzare appieno e facilmente i servizi on line in tutta l'UE, preservando al contempo la loro vita privata.

ASSONIME - Riproduzione riservata

anche una raccomandazione con la quale gli Stati membri sono stati invitati a definire un pacchetto di strumenti che comprende: un'architettura tecnica, standards e specifiche tecniche, orientamenti comuni e best practices[4]. Nel febbraio 2022 è stato pubblicato il primo documento elaborato dagli esperti dei paesi membri (eIDAS expert group), in stretto coordinamento con la Commissione: "European Digital Identity, Architecture and Reference Framework". I lavori dell'expert group stanno proseguendo ed è attesa entro l'inizio del 2023 la pubblicazione di un nuovo documento, che terrà conto dello stato dei lavori della proposta e dei commenti da parte degli Stati membri.

Sempre nel febbraio 2022 la Commissione europea ha lanciato anche un bando per lo sviluppo di progetti pilota che sperimenteranno diverse soluzioni di identità digitale basata sull'EUDI wallet, su specifici use cases verticali quali: identificazione online, firme elettroniche qualificate, patente digitale mobile, eHealth, pagamenti digitali. La Commissione dovrebbe assegnare il bando entro la fine di quest'anno affinché i vincitori comincino a lavorare operativamente sulle varie soluzioni di identità digitale dall'inizio del 2023[5].

Riguardo allo stato di avanzamento della proposta, lo scorso 6 dicembre il Consiglio UE ha adottato un orientamento generale sulla quinta proposta di compromesso, in vista dell'avvio dei negoziati interistituzionali con il Parlamento europeo, che voterà in seduta plenaria il 13 marzo 2023.

Questa nota analizza lo stato attuale della proposta che potrebbe ancora subire alcune variazioni in seguito all'esito del trilogo nel nuovo confronto fra Consiglio e Parlamento europeo. Essa parte da una breve analisi dei limiti presentati dal regolamento eIDAS per illustrare le principali disposizioni sull'EUDI wallet e sugli attestati elettronici di attributi, contenute nel testo della proposta su cui è stato adottato l'orientamento generale.

2. I limiti del regolamento eIDAS

Il regolamento eIDAS, che ha istituito il primo quadro europeo per l'identificazione elettronica, consente il riconoscimento transfrontaliero dei mezzi di identificazione

[4] 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".

[5] Da fonti non ufficiali risulta che i consorzi in gara sono quattro: Potential (di cui fa parte la società Namirial), che investirà in applicazioni dell'identità digitale in ambito bancario e sanitario; Nobid (di cui fanno parte Banca d'Italia, PagoPA, Abilab e Intesa Sanpaolo. Sono coinvolte a livello tecnico anche Poste italiane, Istituto poligrafico e zecca dello Stato, Intesi group e Infocert), che si concentrerà sui pagamenti digitali; Consorzio European digital wallet (di cui fanno parte Infocert, Intesi ed eWitness); Digital credential 4 Europe, che si occuperà dei settori della scuola, formazione e sicurezza sociale.

ASSONIME - Riproduzione riservata

elettronica nazionali e dei servizi fiduciari, ma la sua applicazione nel corso del tempo ha evidenziato molti limiti. Anzitutto, nel regolamento eIDAS non è previsto un obbligo di notifica dei regimi nazionali di identificazione elettronica e questo ha comportato che, fino ad ora, solo 18 Stati membri hanno notificato un regime di identificazione. Inoltre, ad oggi l'accesso transfrontaliero ai servizi è limitato a causa di nodi tecnici non risolti, relativi all'infrastruttura di interoperabilità per il riconoscimento reciproco dei regimi nazionali. In secondo luogo, il regolamento eIDAS si concentra solo sull'accesso transfrontaliero ai servizi pubblici e non sono indicati incentivi chiari che incoraggiano i soggetti privati a utilizzare i mezzi di identificazione elettronica nazionale. A questo proposito, nella valutazione ex post della Commissione sul regolamento eIDAS, si evidenza come la maggior parte delle esigenze in materia di identità e autenticazione elettroniche si riscontra nel settore privato e, in particolare, nel settore bancario, delle telecomunicazioni e degli operatori di piattaforme, che sono tenuti per legge a verificare l'identità dei loro clienti. In terzo luogo, il regolamento eIDAS non si applica alla fornitura di attributi elettronici, rendendo difficile assicurare il loro riconoscimento giuridico a livello transfrontaliero. Infine, esso non prevede la minimizzazione del trattamento dei dati personali, non consentendo agli utenti di limitare la condivisione dei dati di identità a ciò che è strettamente necessario per la prestazione di un servizio.

3. La disciplina dell'EUDI wallet

L'EUDI wallet è definito nella proposta di regolamento (art. 6-bis) come un mezzo di identificazione elettronica che permette all'utente, in modo trasparente e tracciabile dallo stesso, di:

a) richiedere, selezionare, combinare, conservare, cancellare gli attestati elettronici di attributi e i dati di identificazione personale e presentarli in modo sicuro alle relying parties[6], anche per l'autenticazione online e, se del caso, offline[7], per utilizzare servizi pubblici e privati, garantendo al contempo che sia possibile la disclosure selettiva[8];

[6] Le relying parties sono definite dal regolamento eIDAS come persone fisiche o giuridiche che fanno affidamento su un'identificazione elettronica o su un servizio fiduciario.

[7] L'uso offline presuppone un'interazione tra un utente e una relying party in un luogo fisico, dove il wallet non è tenuto ad accedere a sistemi a distanza tramite reti di comunicazione elettronica ai fini dell'interazione. L'uso offline è importante in molti settori, tra cui quello sanitario nel quale i servizi sono spesso forniti mediante interazione face to face (considerando 9 della proposta di regolamento).

[8] Il considerando 29 della proposta di regolamento chiarisce che la disclosure selettiva conferisce al proprietario dei dati il potere di divulgare solo alcune parti di un insieme di dati più ampio.

ASSONIME - Riproduzione riservata

b) firmare con firme elettroniche qualificate e apporre sigilli attraverso sigilli elettronici qualificati[9].

I soggetti e le regole per l'emissione del wallet

Ogni Stato membro deve garantire la disponibilità dell'EUDI wallet alle persone fisiche e giuridiche entro 24 mesi dall'entrata in vigore dei relativi atti di esecuzione, per garantire che queste abbiano un accesso sicuro, affidabile e transfrontaliero a servizi pubblici e privati. In particolare, i wallets sono emessi dagli Stati membri, o dai soggetti delegati dagli stessi, o sono emessi a titolo indipendente e riconosciuti dagli Stati membri.

Viene specificato che il soggetto che emette il wallet non raccoglie informazioni sull'uso dello stesso che non sono necessarie per la prestazione dei servizi del wallet, né combina i dati di identificazione personale e gli altri dati personali conservati nel wallet o relativi 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. Viene in questo modo assicurato uno strumento che permette di condividere in sicurezza i dati relativi all'identità, che restano sotto il controllo esclusivo dell'utente, e consente, secondo un principio di minimizzazione, di condividere solo e unicamente le informazioni necessarie ad accedere ad uno specifico servizio.

L'EUDI wallet viene emesso nell'ambito di un regime nazionale di identificazione elettronica notificato il cui livello di garanzia è elevato. Per questo, viene posto l'obbligo per gli Stati membri che non l'abbiano ancora fatto, di notificare un regime di identificazione elettronica di livello di garanzia elevato e comprendente almeno un mezzo di identificazione elettronica di livello di garanzia elevato. A tale proposito, per rispondere alle preoccupazioni di alcuni Stati membri, tra cui in particolare l'Italia, che hanno già rilasciato un numero considerevole di mezzi nazionali di identificazione elettronica di livello di garanzia "significativo" (in Italia oltre 33 milioni di SPID finora rilasciate), sono state previste misure complementari di verifica dell'identità che permetteranno comunque di "inizializzare" il wallet anche attraverso questi mezzi e nel caso Italiano con SPID, attivando alcuni accorgimenti tecnici per soddisfare il requisito di garanzia elevato per attivare il wallet.

[9] Nel framework dell'eIDAS expert group viene specificato che l'obiettivo di consentire di firmare con firma elettronica qualificata o sigillo qualificati attraverso l'EUDI wallet può essere raggiunto in diversi modi: il wallet può includere un certificato qualificato per la creazione di firme/sigilli, o il wallet costituisce uno strumento di autenticazione sicuro per l'emissione di certificato qualificato per la creazione di firme/sigilli.

ASSONIME - Riproduzione riservata

L'emissione, l'uso per l'autenticazione e la revoca degli EUDI wallets sono gratuiti per le persone fisiche, mentre i servizi che si basano sull'uso del wallet possono comportare costi connessi, ad esempio, al rilascio degli attestati elettronici di attributi (considerando 9).

La certificazione del wallet

Per garantire un livello elevato di sicurezza e protezione dei dati, la proposta di regolamento prevede che la conformità relativa alla cybersecurity dei requisiti e delle specifiche tecniche previste per l'EUDI wallet vengano certificate da organismi di valutazione della conformità, accreditati ai sensi del cybersecurity act[10] e designati dagli Stati membri. Sulla base delle informazioni provenienti dagli Stati membri, la Commissione redige, pubblica e aggiorna un elenco degli EUDI wallets certificati.

Relying parties (art. 6-ter)

In linea generale, se le relying parties che forniscono servizi pubblici o privati, vogliono avvalersi dell'EUDI wallet, devono effettuare una notifica allo Stato membro in cui sono stabilite. La procedura di notifica deve essere economicamente vantaggiosa e proporzionata al rischio e garantire che le relying parties forniscano almeno le informazioni necessarie per autenticarsi nell'EUDI wallet. Restano impregiudicati ulteriori obblighi di notifica, in conformità del diritto dell'Unione o nazionale, per specifiche categorie di dati, come quelli sensibili.

Le relying parties notificanti assicurano l'attuazione di meccanismi di autenticazione delle stesse nel wallet e sono responsabili della procedura di autenticazione delle persone e della convalida degli attestati di attributi elettronici derivanti dal wallet.

Gli Stati membri possono esentare le relying parties dall'obbligo di notifica quando il diritto dell'Unione o il diritto nazionale non prevedono specifici obblighi di notifica o registrazione per accedere alle informazioni fornite attraverso il wallet. Si tratta ad esempio di casi in cui il diritto di verificare specifici attributi non richiede l'autenticazione o consente l'autenticazione mediante mezzi elettronici delle relying parties.

Utilizzo transfrontaliero (art. 6 quinquies-ter)

Per quanto riguarda il ricorso transfrontaliero agli EUDI wallets è previsto che quando gli Stati membri richiedono l'identificazione elettronica mediante un mezzo di identificazione elettronica e un'autenticazione per accedere ai servizi on line prestati da

[10] Cfr. articolo 60 del regolamento (UE) 2019/881.

ASSONIME - Riproduzione riservata

un organismo del settore pubblico, essi accettano anche gli EUDI wallets per l'autenticazione dell'utente.

Per essere ampiamente disponibili e utilizzabili, gli EUDI wallets devono essere accettati dai prestatori di servizi privati. Perciò la proposta dispone che 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 settori dei: trasporti, energia, banche, servizi finanziari, sicurezza sociale, sanità, acqua potabile, servizi postali, infrastruttura digitale, istruzione, telecomunicazioni. Per agevolare l'uso e l'accettazione del wallet è opportuno tener conto delle norme e delle specifiche tecniche settoriali (considerando 28).

È previsto anche che nei casi in cui le piattaforme on line di dimensioni molto grandi, come definite nel regolamento europeo sui servizi digitali[11], impongono agli utenti di autenticarsi per accedere ai servizi on line, esse devono accettare anche l'uso dell'EUDI wallet per l'autenticazione, esclusivamente su richiesta volontaria dell'utente e nel rispetto dei dati minimi necessari per lo specifico servizio on line per cui è richiesta l'autenticazione.

Entro 24 mesi dall'introduzione degli EUDI wallets la Commissione può valutare se sia opportuno imporre ad altri prestatori privati di servizi on line di accettare l'uso del wallet, sempre esclusivamente su richiesta dell'utente.

4. Attestati elettronici di attributi (artt. 45-bis e ss.)

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

[11] Regolamento (UE) 2022/2065.

[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 e più chiara formulazione di tutti i servizi ricompresi nella definizione di servizi fiduciari, sono introdotti i nuovi servizi di: gestione di disposizioni qualificati 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.

ASSONIME - Riproduzione riservata

fisica o giuridica o di un oggetto. La proposta disciplina tre tipologie di attestati elettronici di attributi. L'attestato elettronico di attributi è definito come un attestato in forma elettronica che consente l'autenticazione di attributi, a cui vengono riconosciuti effetti giuridici e l'ammissibilità come prova nei procedimenti giudiziali. 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 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 degli attestati, in ambiti come quello delle patenti di guida, titoli di studio, pagamenti digitali. Anche se non previsto nella proposta di regolamento, il framework specifica che questi prestatori, per consentire agli utenti di richiedere e ottenere gli attestati, devono essere tecnicamente conformi alle specifiche tecniche dell'interfaccia dell'EUDI wallet.

L'attestato elettronico di attributi qualificato è un attestato rilasciato da un prestatore di servizi fiduciari qualificato[15], che soddisfa specifici requisiti e ha gli stessi effetti giuridici degli attestati in formato cartaceo rilasciati legalmente. Quando viene rilasciato in uno Stato membro è riconosciuto come attestato qualificato anche in tutti gli altri Stati membri. Per determinati attributi che fanno affidamento su fonti autentiche all'interno del settore pubblico, gli Stati membri devono consentire ai fornitori qualificati di attestati elettronici di attributi di verificare questi attributi rispetto alle fonti autentiche mediante mezzi elettronici. L'attestato 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 degli attestati in formato cartaceo rilasciati legalmente ed è riconosciuto come tale in tutti gli Stati membri. Sia i fornitori di attestati elettronici di attributi qualificati che gli organismi del settore pubblico devono 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

[14] Oltre ai requisiti di sicurezza già previsti dal regolamento eIDAS per i prestatori di servizi fiduciari qualificati e non qualificati, la proposta di regolamento introduce una nuova disposizione che disciplina specifici requisiti per i prestatori di servizi fiduciari non qualificati.

[15] Ai sensi del regolamento eIDAS, il prestatore di servizi fiduciari qualificato è un prestatore di servizi fiduciari 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 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.

ASSONIME - Riproduzione riservata

non combinare i dati personali relativi alla prestazione di questi servizi con i dati personali provenienti da qualsiasi altro servizio prestato da loro o dai loro partner commerciali.

19 Dicembre 2022

ASSONIME - Riproduzione riservata