AGID | Agenzia per l'Italia Digitale

Regolamento eIDAS e Identity Proofing

Viviana De Paola, funzionario tecnico – Area vigilanza e sicurezza

25/05/2026

Regolamenti eIDAS

Electronic Identification, Authentication and Trust Services, regolamenta a livello comunitario l'identificazione elettronica e i servizi fiduciari per transazioni elettroniche nel mercato interno dell'UE

Regolamento UE 2014/910 – eIDAS 1

Stabilisce regole in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e abroga la direttiva 1999/93/CE.

Regolamento 2024/1183 – eIDAS 2

Modifica il Regolamento 2014/910 e istituisce il quadro europeo relativo a un'identità digitale.

eIDAS 1

Uno degli aspetti fondamentali del Regolamento eIDAS 1 è stato l'istituzione del riconoscimento reciproco per le eID emesse dai paesi UE, lasciando ampio margine ai sistemi nazionali, a condizione del rispetto dei criteri normativi specificati compresa la notifica alla Commissione.

Questo riconoscimento ha consentito transazioni elettroniche sicure assicurando che un eID emesso in uno stato membro fosse valido e riconosciuto in tutti gli altri, ponendo le basi per la fiducia e l'interoperabilità nell'identificazione elettronica.

eIDAS 2 a

- Perfeziona le regole per i fornitori di servizi fiduciari qualificati garantendo una regolamentazione più chiara e armonizzata, introducendo l'attestazione elettronica degli attributi, il certificato di autenticazione di sito web, la gestione di dispositivi qualificati per la creazione di firma elettronica (o sigillo elettronico) a distanza, l'archiviazione elettronica e i registri elettronici.

eIDAS 2 b

- Garantisce a persone e imprese l'accesso a soluzioni di identità digitale sicure e facili da usare che funzionino senza problemi in tutti gli stati membri dell’UE.
- Migliora la sicurezza dei dati e promuove condizioni di parità per i servizi fiduciari qualificati in tutta l’UE.

eIDAS 2 c

Rafforza:

- i principi della privacy by design, offrendo agli utenti un maggiore controllo su quali dati personali vengono condivisi e con chi;
- la conformità allineandosi agli standard ETSI aggiornati per la verifica dell'identità, la gestione dei certificati e l'interoperabilità tra gli Stati membri;
- l’interoperabilità transfrontaliera attraverso il riconoscimento reciproco e globale delle identità digitali.

eIDAS 2 d

- Prevede il Portafoglio Europeo di Identità Digitale EUDI (art. 5-bis), reso accessibile per l'uso da parte delle persone con disabilità, in condizioni di parità con gli altri utenti (co. 21), conformemente alla direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio che consente agli utenti di memorizzare, gestire e condividere i propri dati, credenziali e attributi di identità, accedendo online e offline.

Portafogli europei di identità digitali

Dovrebbero consentire agli utenti di (considerando 19):

- identificarsi e autenticarsi elettronicamente in modalità online e offline a livello transfrontaliero per accedere a un'ampia gamma di servizi pubblici e privati
- creare e utilizzare firme e sigilli elettronici qualificati accettati in tutta l'Unione. Una volta effettuato l'onboarding in un portafoglio europeo di identità digitale, le persone fisiche dovrebbero poterlo utilizzare per firmare con firme elettroniche qualificate **gratuite per tutte le persone fisiche a fini non professionali** (considerando 20), per impostazione predefinita e gratuitamente, senza dover sottostare a ulteriori procedure amministrative. Gli utenti dovrebbero poter apporre firme o sigilli su attributi o dichiarazioni autocertificati.

eIDAS 2

- Introduce nuovi servizi fiduciari: la gestione dei dispositivi per la generazione di firme e sigilli da remoto, il rilascio e la convalida di attestati elettronici di attributi, l'archiviazione elettronica di dati elettronici e di documenti elettronici, la registrazione di dati elettronici in un registro elettronico, la convalida dei dati trasmessi tramite servizi elettronici di recapito certificato.

Identificazione elettronica

Processo che utilizza dati di identificazione personale in forma elettronica per rappresentare una persona fisica o giuridica o un’unica persona fisica **che rappresenta un’altra persona fisica** (art. 3 eIDAS 2) o persona giuridica.

Il mezzo di identificazione elettronica è l'unità (fisica o digitale) che contiene tali dati e viene usata per autenticarsi online **o, se del caso, per un servizio offline** (eIDAS 2).

Requisiti per i prestatori di servizi fiduciari qualificati (art. 24, co. 1, eIDAS 1)

Per ottenere un certificato elettronico qualificato (come la firma digitale), un prestatore di servizi fiduciari qualificati (QTSP) doveva verificare l'identità del richiedente:

- **Presenza fisica**: Identificazione di persona (de visu) della persona fisica o del rappresentante legale della persona giuridica.
- **A distanza, mediante mezzi di identificazione elettronica**: Utilizzo di un'identità digitale precedentemente rilasciata in presenza fisica, che soddisfacesse i livelli di garanzia *significativo* o *elevato.*

eIDAS 1 - Requisiti per i prestatori di servizi fiduciari qualificati (art. 24, co. 1, eIDAS 1)

- **Mediante un certificato qualificato preesistente**: Utilizzo di una firma digitale o di un sigillo elettronico qualificato ancora validi, emessi in precedenza secondo una delle altre modalità conformi.
- **Mediante altri metodi di identificazione a distanza equivalenti**: Metodi alternativi (come il video-riconoscimento con operatore o il self-video con bonifico bancario) riconosciuti a livello nazionale, le cui condizioni di sicurezza fossero certificate da un organismo di valutazione della conformità.

eIDAS 2 - Requisiti per i prestatori di servizi fiduciari qualificati (art. 24, co. 1-bis, eIDAS 2)

Il prestatore di servizi fiduciari qualificato, per il rilascio di un certificato qualificato o un attestato elettronico di attributi qualificato, verifica l'identità con mezzi adeguati direttamente o tramite un terzo, sulla base di uno dei metodi seguenti o, ove necessario, di una combinazione degli stessi:

a) **mediante il portafoglio europeo di identità digitale o un mezzo di identificazione elettronica notificato che rispetta i requisiti di cui all'articolo 8 per quanto riguarda il livello di garanzia elevato**; (nuovo rispetto ad eIDAS 1)

Art. 8 eIDAS 2 livello di garanzia elevato

Il livello di garanzia elevato si riferisce a un mezzo di identificazione elettronica più elevato dei mezzi di identificazione elettronica aventi un livello di **garanzia significativo**, nel contesto di un regime di identificazione elettronica che fornisce riguardo all'identità pretesa o dichiarata di una persona un grado di sicurezza, ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, **il cui scopo è quello di impedire l'uso abusivo o l'alterazione dell'identità.**

Forum of European di Supervisory Authorities FESA

L’art. 24, par. 1 **richiede l'uso di un portafoglio o di un mezzo di identificazione elettronica con un elevato livello di garanzia (precedentemente “sostanziale”).**

Partendo dal presupposto che tutti questi metodi di verifica dell'identità debbano raggiungere un livello di affidabilità simile, FESA, nel proprio position paper del 2024 , ritiene che i metodi che devono soddisfare un “elevato livello di affidabilità” dovranno soddisfare requisiti simili a quelli applicabili al livello di garanzia elevato per i mezzi di identificazione elettronica, come definito **nell’art. 8 e specificato nel regolamento di esecuzione (UE) 2015/1502 della Commissione dell'8 settembre 2015.**

Altri requisiti per i prestatori di servizi fiduciari qualificati art. 24 co. 1-bis, eIDAS 2

b) mediante un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato rilasciato conformemente alla lettera a), c) o d);

c) mediante altri metodi di identificazione che garantiscono l'identificazione della persona **con un elevato livello di sicurezza,** la conformità dei quali è confermata da un organismo di valutazione della conformità;)a differenza della lettera d) di eIDAS 1 relativamente all'affidabilità della presenza fisica)

d) **mediante la presenza concreta della persona fisica** (lettera a di eIDAS 1) o di un rappresentante autorizzato della persona giuridica, sulla base di adeguate prove e procedure, conformemente al diritto nazionale.

Regolamento di esecuzione (UE) 2025/1566

Emanato ai sensi dell’art. 24 co. 1 quater, si applicherà a decorrere dal 19/08/2027 e stabilisce la verifica dell'identità e degli attributi della persona fisica o giuridica a cui deve essere rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato.

In particolare, per garantire la parità di trattamento e la possibilità di fidarsi dell'esito dei processi di verifica, le verifiche dovrebbero essere effettuate in modo equivalente da tutti i prestatori di servizi fiduciari qualificati (considerando 2).

Sono state, quindi, selezionate diverse norme per soddisfare tali requisiti specifici che, da una parte, rispecchiano le prassi consolidate, dall'altra, sono state adattate per includere controlli supplementari che garantiscano la sicurezza e l'affidabilità del servizio fiduciario qualificato.

AGID | Agenzia per l’Italia Digitale

Regolamento di esecuzione (UE) 2025/1569

Il regolamento è entrato in vigore il 19/08/2025 e stabilisce le norme di riferimento, le specifiche e le procedure relative: agli attestati elettronici qualificati di attributi; agli attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto; all'elenco di fornitori di attestati di elettronici rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto; al catalogo di attributi e al catalogo di regimi per gli attestati di attributi; alla verifica degli attributi rispetto a fonti autentiche o intermediari designati.

2025/1569 Regolamento di esecuzione (UE)

A decorrere dal 19 agosto di questo anno si applicano le disposizioni relative alla:

- pubblicazione da parte della CE dell'elenco dei fornitori di attestati elettronici di attributi rilasciati da un organismo del settore pubblico (art. 6);
- redazione e pubblicazione da parte della CE di un catalogo di attributi ed uno di regimi; la CE istituisce un sistema sicuro che consente la presentazione di richieste di inclusione di attributi e di regimi nel catalogo di attributi e di regimi per gli attestati di attributi o di modifica degli attributi in esso registrati (artt. 7 e 8);

Regolamento di esecuzione 2025/1569

- Meccanismo di verifica degli attributi rispetto a fonti autentiche o intermediari designati (art. 9).

Il risultato della verifica indica esclusivamente se l'attributo è stato verificato o no e specifica l'organismo del settore pubblico responsabile della fonte autentica o, se del caso, l'organismo del settore pubblico designato per agire per conto della fonte autentica rispetto alla quale è stato verificato l'attributo.

Identity Proofing

Processo di verifica e di associazione di una persona fisica o giuridica a una persona reale con procedure e controlli tecnologici tramite documenti, biometria e mezzi elettronici, fondamentale per servizi digitali.

In ambito di sicurezza digitale permette di ridurre frodi, accessi non autorizzati e furti di identità instaurando un clima di fiducia nei servizi digitali.

AGID | Agenzia per l'Italia Digitale

Remote Identity Proofing

Il processo di verifica dell’identità a distanza, attraverso il quale un utente online dimostra di essere il titolare dell'identità dichiarata, viene solitamente effettuato tramite webcam o dispositivo mobile, dove gli utenti mostrano il proprio volto e presentano i documenti rilasciati dalle Autorità – carte d'identità o passaporti. La verifica dell'identità è un elemento fondamentale per le transazioni elettroniche e lo sviluppo del mercato unico digitale in tutta l’Unione Europea.

ENISA REMOTE ID PROOFING 2021 - ENISA Report - Remote Identity Proofing - Attacks & Countermeasures.pdf 2022 e REMOTE ID PROOFING GOOD PRACTICES 2024.

AGID | Agenzia per l’Italia Digitale

Fasi di Identity Proofing

Raccolta dei dati personali: l’utente fornisce dati personali come nome, data di nascita, indirizzo e documento di identità per iniziare il processo.

Verifica dei documenti: si controlla l’autenticità e la validità dei documenti attraverso elementi di sicurezza e coerenza dei dati.

Autenticazione dell’utente: include controlli come codici OTP o riconoscimento biometrico per confermare l’identità dell’utente.

Validazione e revisione finale: il sistema o un operatore conferma l’esito del processo, con possibile revisione manuale in contesti ad alto rischio.

Verifica

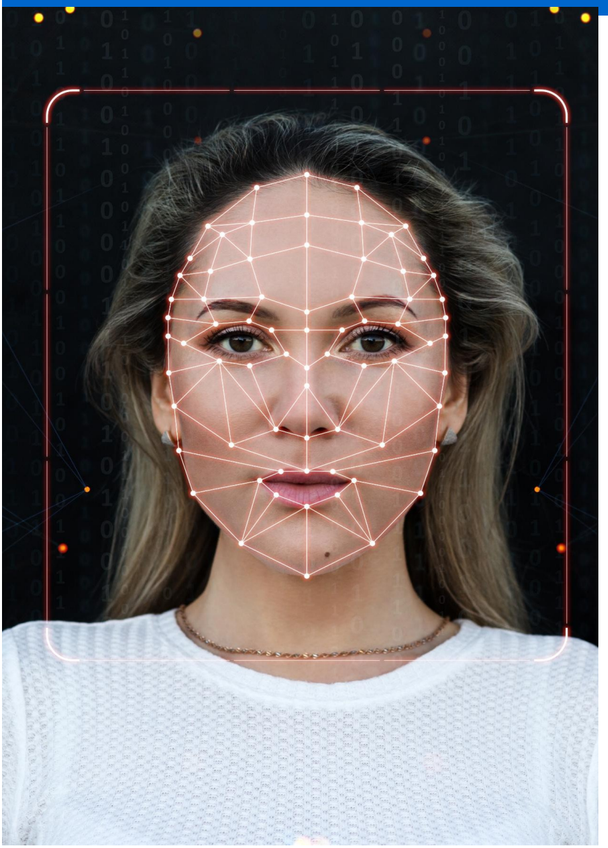
In presenza: controllo fisico dei documenti da parte di un operatore, garantendo alta affidabilità.

Da remoto: utilizzo di strumenti digitali come app e videochiamate per autenticare l’identità online.

Approccio ibrido: Molte organizzazioni combinano controlli automatici e umani per bilanciare sicurezza ed efficienza.

Fattori decisionali: la scelta del metodo dipende dal rischio, dal contesto normativo e dall’esperienza utente desiderata.

Autenticazione forte e biometria



Autenticazione forte: utilizza più fattori come password, dispositivi e dati biometrici per aumentare la sicurezza.

Tecnologie biometriche principali: riconoscimento facciale, impronte digitali e riconoscimento vocale per identificare in modo univoco l'utente.

Sicurezza e sfide della privacy: l'uso della biometria aumenta la sicurezza ma richiede maggiore protezione dei dati personali.

Strumenti

Intelligenza Artificiale e Machine Learning: analizzano documenti e riconoscono volti, identificando tentativi di frode con precisione elevata.

Tecnologia OCR per estrazione dati: automatizza l'estrazione di dati dai documenti di identità, migliorando velocità e riducendo errori manuali.

Riconoscimento facciale e controlli di liveness: confrontano immagini in tempo reale e usano controlli di liveness per prevenire frodi con immagini statiche o deepfake.

Integrazione con database esterni: le piattaforme si collegano a database affidabili per validare documenti e migliorare la sicurezza del processo di verifica.

Sintesi

Aspetto	eIDAS 1 (2014)	eIDAS 2 (2024)
Identity proofing	Verifica tramite presenza fisica o mezzi elettronici equivalenti; livelli di garanzia definiti	Procedure armonizzate, uso di portafoglio digitale, verifica remota avanzata, standard UE
Strumenti	Mezzi di identificazione elettronica notificati	Portafoglio europeo di identità digitale (EUDI Wallet)
Obbligatorietà	Notifica volontaria dei regimi, riconoscimento reciproco	Obbligo per ogni Stato membro di offrire almeno un portafoglio digitale
Controllo utente	Limitato, dipende dal sistema nazionale	Pieno controllo su dati e attributi condivisi
Interoperabilità	Basata su notifica e livelli di garanzia	Rafforzata, standard tecnici comuni