AGID academy

AGID | Agenzia per l'Italia Digitale

REGOLAMENTO EIDAS E IDENTITY PROOFING: NUOVI PARADIGMI DI FIDUCIA DIGITALE E CYBERSICUREZZA

Sintesi

Maggio 2026

REGOLAMENTO eIDAS E IDENTITY PROOFING: NUOVI PARADIGMI DI FIDUCIA DIGITALE E CYBERSICUREZZA

Sommario

ABSTRACT

Il presente documento analizza l'evoluzione del quadro normativo europeo in materia di identità digitale, con particolare focus sul passaggio dal Regolamento eIDAS 1.0 al nuovo eIDAS 2.0. Viene approfondito il concetto di *Identity Proofing* da remoto, esaminando le architetture tecnologiche dell'*EUDI Wallet* e dell'*IT-Wallet* italiano. Il paper dedica un'ampia sezione all'analisi delle minacce emergenti, come i *Deepfake* e la *Camera Injection*, e delinea le strategie di mitigazione multilivello raccomandate dalle autorità di vigilanza per garantire la sicurezza delle transazioni digitali.

L'identificazione elettronica sicura rappresenta il pilastro della fiducia digitale nel mercato unico europeo. Il passaggio a eIDAS 2.0 introduce il concetto di EUDI Wallet, superando i limiti del cosiddetto *remote onboarding* asincrono basato su segnali digitali non verificati. Mentre l'*Identity Proofing* si evolve verso modelli basati sulla crittografia e su fonti autentiche statali, la superficie d'attacco si sposta verso la manipolazione dei flussi video tramite l'intelligenza artificiale. Il documento intende dimostrare come solo un approccio olistico, che integri controlli tecnici, ambientali e organizzativi, possa garantire un livello di garanzia elevato (*LoA High*) nelle transazioni transfrontaliere.

INTRODUZIONE

Verificare un'identità a distanza non è più considerato un mero problema tecnologico, bensì una questione di architettura della fiducia. Con la progressiva rimozione della presenza fisica e la completa digitalizzazione dei servizi primari, la distinzione tra realtà fisica e segnale digitale è divenuta critica. Il Regolamento eIDAS-2.0, entrato in vigore nel maggio 2024, mira a standardizzare l'interoperabilità e la sicurezza dei *wallet* nazionali, imponendo a ogni Stato membro di rendere disponibile il proprio portafoglio digitale entro dicembre 2026. In questo contesto, l'Identity Proofing emerge come il processo fondamentale per associare in modo

univoco una persona reale a un'identità digitale, proteggendo l'ecosistema da frodi e furti d'identità sempre più sofisticati e pervasivi.

1. EVOLUZIONE NORMATIVA: DAL REGOLAMENTO EIDAS 1.0 AL QUADRO EIDAS 2.0

Il quadro regolatorio europeo ha subito una trasformazione significativa con il passaggio dal Regolamento (UE) 910/2014 (eIDAS 1.0) al Regolamento (UE) 2024/1183 eIDAS2.0. Mentre il primo si concentrava sul riconoscimento reciproco delle identità digitali nazionali e sui servizi fiduciari (firme, sigilli, marche temporali) eIDAS 2.0 introduce invece una visione più armonizzata basata sul quadro europeo relativo a un'identità digitale comune.
Esso, inoltre, introduce nuovi servizi fiduciari qualificati specifici come ad esempio:

1. l'attestazione elettronica degli attributi e i certificati di autenticazione dei siti web;
2. la gestione di dispositivi qualificati per la firma o sigillo elettronico a distanza;
3. l'archiviazione elettronica e i registri elettronici;
4. la convalida dei dati trasmessi tramite servizi elettronici di recapito certificato.

È opportuno inoltre precisare che l'identificazione elettronica rappresenta una persona fisica o giuridica (o un delegato) attraverso dati in forma elettronica, definendo il mezzo di identificazione come l'unità fisica o digitale che contiene tali dati per l'autenticazione online e offline.
L'obiettivo principale è quindi quello di garantire che i cittadini e le imprese possano identificarsi e autenticarsi elettronicamente in modalità online e offline per accedere a servizi pubblici e privati in tutta l'Unione Europea.
Uno degli aspetti chiave di questa evoluzione è il passaggio da regimi di notifica volontaria a obblighi stringenti per gli Stati membri di fornire portafogli di identità digitale (*EUDI Wallet*).
Sotto eIDAS 1.0, il riconoscimento era basato su notifiche nazionali che potevano avere diversi livelli di garanzia; eIDAS 2.0 punta invece ad un'interoperabilità rafforzata basata su

standard tecnici comuni (come quelli definiti dall'*ETSI*) e su un pieno controllo dell'utente sui propri dati e attributi. Inoltre, il nuovo regolamento introduce nuovi servizi fiduciari qualificati, tra cui l'archiviazione elettronica, i registri elettronici e la gestione di dispositivi qualificati per la creazione della firma elettronica a distanza. Questa armonizzazione è fondamentale per facilitare la circolazione delle persone e assicurare la parità di trattamento nei processi di verifica transfrontaliera.

2. L'ECOSISTEMA EUDI WALLET E L'IMPLEMENTAZIONE NAZIONALE IT-WALLET

L'EUDI *Wallet* (European Digital Identity Wallet) rappresenta lo standard tecnologico e normativo che regola l'interoperabilità, la sicurezza e la portabilità delle identità digitali in Europa. In Italia, questo modello si concretizza nell'IT-*Wallet*, integrato nell'App IO, che fungerà da portafoglio nazionale conforme ai requisiti europei. L'IT-*Wallet* non è concepito come un sistema isolato, ma come un ecosistema che integra credenziali della Pubblica Amministrazione e può ereditare l'identità da fornitori esistenti come SPID e CIE, i quali mantengono il ruolo dei cosiddetti *Identity Provider* fondamentali con un livello di garanzia elevato (*LoA High*).

L'EUDI *Wallet* introduce requisiti di inclusività e nuovi diritti per l'utente, quali:

1. Accessibilità: il portafoglio deve essere utilizzabile dalle persone con disabilità in condizioni di parità, in conformità alla direttiva (UE) 2019/882.

2. Firma elettronica gratuita: una volta effettuato *l'onboarding*, le persone fisiche devono poter apporre firme elettroniche qualificate gratuitamente per scopi non professionali.

3. Controllo dell'utente: viene rafforzato il principio di *privacy by design*, garantendo il pieno controllo su quali dati e attributi condividere e con chi.

Il passaggio all'EUDI *Wallet* segna pertanto un cambio di paradigma: l'identità digitale diventa quindi riutilizzabile, condivisibile e centrale per la vita del cittadino. A differenza dei sistemi precedenti, l'EUDI *Wallet* mira a eliminare la dipendenza da processi di *onboarding* remoto asincroni basati su *selfie* scattati col proprio dispositivo, preferendo un modello in cui i dati personali (contenuti nella patente, nella tessera sanitaria o nei titoli di studio) vengono recuperati direttamente dalle basi dati statali tramite API (*Application Programming Interface* un insieme di regole o protocolli che consentono alle applicazioni software di comunicare tra loro per scambiare dati, caratteristiche e funzionalità) sicure e firmate digitalmente. Questo approccio riduce drasticamente i rischi di manipolazione dei dati alla fonte, poiché il *wallet* si fida dell'identità originaria (SPID/CIE) e comunica direttamente con fonti autentiche come l'ANPR (l'Anagrafe Nazionale) o la Motorizzazione Civile.

3. FONDAMENTI DELL'IDENTITY PROOFING: UNO SGUARDO D'INSIEME SULLE FASI DELLA FIDUCIA

L'*Identity Proofing* è definito come il processo di verifica dell'associazione tra una persona reale (fisica o giuridica) e un'identità dichiarata, operazione che avviene attraverso procedure tecnologiche e controlli rigorosi. Questo processo è essenziale per instaurare un clima di

fiducia nei servizi digitali, riducendo drasticamente il rischio di accessi non autorizzati e di sostituzioni di persona (reato previsto dall'articolo 494 del Codice penale italiano).
L'architettura tipica dell'*Identity Proofing* si articola in quattro fasi sequenziali:

1. Acquisizione
2. Validazione
3. Verifica
4. *Binding*

Sinteticamente, nella fase di acquisizione vengono raccolti dati anagrafici, documenti e, se necessario, elementi biometrici attraverso canali fisici o digitali; segue la validazione, in cui tali informazioni vengono controllate per verificarne correttezza formale, integrità e autenticità mediante verifiche sintattiche, analisi documentale e controlli antifrode; successivamente avviene la verifica, che consiste nel confermare che l'identità dichiarata esista realmente e coincida con la persona che la presenta, attraverso confronti con fonti affidabili, verifiche biometriche o meccanismi di autenticazione aggiuntivi; infine si arriva al *binding*, processo in cui l'identità verificata viene collegata in modo sicuro a credenziali, dispositivi o *account*, creando un legame persistente che consente l'accesso futuro ai servizi garantendo sicurezza, tracciabilità e possibilità di gestione del ciclo di vita dell'identità.
Nella modalità da remoto (*Remote Identity Proofing* o RIPD), l'utente dimostra la propria identità solitamente tramite un dispositivo mobile, inquadrando documenti e fornendo dati biometrici in tempo reale. Tuttavia, esiste una differenza strutturale tra la verifica in presenza e quella remota: mentre la prima si basa sul controllo fisico di una persona e di un documento reale, la seconda dipende interamente da segnali digitali (immagini, *stream* video, bit) che possono essere alterati durante la trasmissione. La sfida dell'*Identity Proofing* moderno consiste quindi nel garantire che l'algoritmo di verifica possa

distinguere tra un utente legittimo e un tentativo di frode automatizzato, mantenendo un equilibrio tra sicurezza ed efficienza dell'esperienza utente. Per comprendere appieno i meccanismi che regolano l'architettura della fiducia digitale è opportuno analizzare nel dettaglio le fasi sequenziali descritte brevemente in precedenza.

4. ACQUISIZIONE E VALIDAZIONE: L'ESTRAZIONE DEI DATI E LA COERENZA DOCUMENTALE

La fase di acquisizione rappresenta il punto d'ingresso dei dati nel sistema.
Attraverso tecnologie note come OCR (*Optical Character Recognition*), il software estrae automaticamente le informazioni testuali dal documento d'identità (nome, cognome, data di nascita, banda MRZ). In questa fase, il sistema deve gestire fonti potenzialmente non affidabili, poiché l'utente potrebbe inquadrare lo schermo di un computer o una riproduzione fotografica invece di un documento fisico. La validazione successiva prevede quindi controlli di coerenza logica, verificando algoritmicamente i *checksum* (l'impronta digitale unica data dall'applicazione di un algoritmo matematico ad un set di dati) presenti nella banda MRZ (*Machine Readable Zone* la striscia inferiore dei documenti d'identità e passaporti in cui i dati del titolare sono codificati in formato alfanumerico).
Tuttavia, la validazione algoritmica basata sulla sola foto è intrinsecamente fragile. Un falsario esperto può generare *checksum* conformi utilizzando calcolatori matematici elementari disponibili online, ingannando i software che non effettuano una verifica hardware. Molti flussi commerciali asincroni omettono la lettura del chip NFC (*Near Field Communication*) presente in CIE o passaporti elettronici, limitandosi all'analisi della superficie del documento, che è facilmente manipolabile tramite software di fotoritocco.
La conformità ai più alti standard di sicurezza richiederebbe invece la verifica dei dati originali firmati dallo Stato all'interno del chip, eliminando alla radice la possibilità di falsificazioni documentali basate su immagini 2D.

5. VERIFICA BIOMETRICA: MATCHING FACCIALE E TECNICHE DI LIVENESS DETECTION

La fase di verifica si concentra sulla biometria per accertare che la persona che richiede l'identità sia il legittimo titolare del documento presentato. Il *Face Matching* utilizza algoritmi di visione artificiale per confrontare i vettori biometrici estratti dalla foto del documento con quelli del *selfie* scattato in tempo reale, calcolando un punteggio di somiglianza probabilistica. Per contrastare l'uso di foto statiche o maschere, vengono implementate tecniche di *Liveness Detection*. La *liveness* attiva richiede all'utente di compiere azioni imprevedibili (come ad esempio ruotare la testa, sorridere, sbattere le palpebre), mentre la *liveness* passiva analizza la texture della pelle e i riflessi della luce sullo schermo.

Nonostante la sofisticazione di questi algoritmi, la biometria remota deve affrontare la sfida dei segnali manipolati. Poiché il sistema analizza *pixel* convinto che arrivino dal sensore fisico della fotocamera, non può facilmente rilevare se sta in realtà analizzando un flusso sintetico iniettato via *software*. La precisione dell'intelligenza artificiale nel riconoscere tentativi di frode è elevata, ma la "corsa agli armamenti" tra difensori e attaccanti rende la rilevazione delle incongruenze biometriche sempre più complessa. L'efficacia della verifica dipende quindi non solo dall'algoritmo di *matching*, ma anche e soprattutto dalla capacità del sistema di garantire l'integrità del canale video utilizzato per l'acquisizione.

6. ANALISI DELLA SUPERFICIE D'ATTACCO: DEVICE, DATI E VETTORI DI AGGRESSIONE

La superficie d'attacco digitale nell'*Identity Proofing* moderno si poggia su tre pilastri critici:

1. il Device
2. i Dati
3. il Vettore

Il primo pilastro riguarda l'ambiente di esecuzione: se il *software* gira su un telefono compromesso l'attaccante ottiene il controllo totale sulla memoria RAM e sui processi dell'applicazione di verifica, potendo bypassare i controlli di sicurezza interni. Anche se le applicazioni installate nel dispositivo cercano di rilevare il suo stato di compromissione, queste difese possono essere eluse attraverso tecniche di *reverse engineering* o modifiche del codice dell'applicazione stessa.

Il secondo pilastro riguarda i dati: con l'avvento dell'IA generativa, la barriera d'ingresso per creare volti falsi o calcolare *checksum* MRZ si è azzerata, trasformando foto e video in sequenze di bit facilmente manipolabili. Il terzo pilastro è il vettore d'attacco: l'attaccante non si limita più a mostrare un display davanti alla telecamera (*Presentation Attack*) ma utilizza strumenti di *Camera Injection* al fine di modificare il sistema operativo intercettando la richiesta dell'applicazione di accendere la fotocamera e rispondendo con l'invio di un file video sintetico (*Deepfake,* appunto) iniettato direttamente nel software, rendendo inutili i tradizionali controlli fisici di *liveness*.

7. INJECTION ATTACKS: LA SFIDA DEI DEEPFAKE E DEL BYPASS DELLA FOTOCAMERA

Vediamo nel dettaglio cosa sono esattamente i cosiddetti *Injection Attacks.*

Essi rappresentano la minaccia più grave per i sistemi di verifica remota, poiché agiscono a livello digitale scavalcando l'intera *pipeline* hardware. Mentre un attacco di presentazione fisico (come, ad esempio, le maschere di silicone o i video riprodotti su un tablet) può essere rilevato da un occhio umano o da un algoritmo attento a segnali come il colore del collo o il movimento innaturale delle palpebre, l'iniezione software è virtualmente invisibile a livello fisico. L'attaccante, infatti, può programmare il video sintetico affinché risponda esattamente alle richieste di *liveness* attiva dell'app, muovendo gli occhi o ruotando il volto in tempo reale.

L'intelligenza artificiale rende queste simulazioni estremamente realistiche, permettendo di alterare movimenti, espressioni e comportamenti in modo fluido e privo di artefatti visibili. Il software di verifica, ingannato alla radice, analizza *pixel* apparentemente perfetti convinto della loro autenticità. La sfida è aggravata dal fatto che molti modelli di intelligenza artificiale utilizzati per la verifica risiedono su server esterni, spesso fuori dall'Europa, ponendo ulteriori questioni sulla gestione dei dati e sulla sovranità tecnologica nel rilevamento dei falsi.

In questo scenario, l'unica difesa efficace sembra essere il passaggio da un concetto di fiducia basata sull'immagine ad un paradigma basato sulla crittografia hardware.

8. IDENTITY BINDING: MECCANISMI DI LEGAME CRITTOGRAFICO E PROTEZIONE HARDWARE

Una volta accertata l'identità, il sistema deve creare un legame indissolubile tra l'identità digitale e il dispositivo fisico dell'utente, processo noto come *Identity Binding*. Questo legame avviene tramite la generazione di una coppia di chiavi asimmetriche (pubblica e privata). La chiave privata viene sigillata all'interno di chip di sicurezza dedicati dello smartphone, come la *Secure Enclave* su iOS o lo *StrongBox* sui sistemi Android, che impediscono l'esportazione della chiave anche da parte del sistema operativo. L'uso della chiave è subordinato alla biometria locale a cui fa riferimento il dispositivo (*FaceID/ TouchID*).

Tuttavia, anche questo meccanismo presenta vulnerabilità logiche. In un sistema operativo compromesso da *malware*, infatti, l'attaccante pur non potendo estrarre la chiave privata, può manipolare l'applicazione che la utilizza. Il *malware* può intercettare la domanda dell'applicazione al chip *hardware* (es.: "la biometria è corretta?") e alterare la risposta *software* convertendola in un "SÌ" artificiale, firmando operazioni all'insaputa dell'utente e bypassando il *FaceID* fisico. Inoltre, eventuali attacchi di *phishing* (tentativi di

truffa informatica in cui criminali inviano messaggi ingannevoli via e-mail, SMS o social fingendosi enti affidabili) durante la fase di *onboarding* possono indurre la vittima a cedere le proprie credenziali primarie (SPID/CIE), permettendo al criminale di avviare il processo sul proprio dispositivo modificato e legando legalmente l'identità della vittima allo smartphone dell'attaccante.

9. VETTORI DI ATTACCO SOCIALE: PHISHING, SMISHING E RISCHI DI SICUREZZA NEI FLUSSI DI ONBOARDING

Il fattore umano rimane l'anello debole della catena di sicurezza. Campagne massive di *smishing* (SMS *phishing*) utilizzano domini creati ad hoc che imitano istituzioni come l'INPS o l'AgID per rubare documenti e credenziali. Gli utenti, convinti di aggiornare i propri dati per non perdere prestazioni assistenziali, caricano volontariamente foto di carta d'identità, patente, tessera sanitaria e persino selfie, alimentando il mercato nero dei dati digitali. Questi documenti non sono solo venduti, ma riutilizzati per creare profili SPID fraudolenti con cui i criminali possono, ad esempio, modificare l'IBAN per l'accredito di stipendi o pensioni.

Un altro vettore insidioso riguarda i cosiddetti verificatori malevoli. Un finto addetto alla sicurezza o un sito web malevolo può mostrare un QR Code da inquadrare con il *Wallet*. Invece di richiedere solo l'attributo necessario (es.: "maggiore di 18 anni"), il codice richiede surrettiziamente l'intero pacchetto di dati certificati dell'utente. Se l'utente approva la richiesta senza leggere attentamente l'elenco dei dati condivisi, trasferisce al criminale un pacchetto di informazioni autenticate dallo Stato, perfette per creare truffe finanziarie o furti d'identità mirati. L'educazione dell'utente e la trasparenza delle interfacce di autorizzazione sono quindi componenti critiche quanto la robustezza del codice.

10. STRATEGIE DI MITIGAZIONE MULTI-LAYER E CONFORMITÀ AI CONTROLLI TECNICI

Per mitigare i rischi del *Remote Identity Proofing*, l'ENISA (l'Agenzia dell'Unione Europea per la Cybersicurezza) propone un approccio *multi-layer*, e cioè multilivello, poiché nessun controllo singolo è considerato sufficiente.

Le strategie d'intervento si dividono pertanto in quattro categorie principali:

1. Tecniche ambientali
2. Tecniche procedurali
3. Tecniche Organizzative.

Nello specifico, le tecniche ambientali si concentrano sull'analisi del contesto operativo in cui avviene la verifica dell'identità, includendo controlli sul dispositivo utilizzato tramite device *fingerprinting*, analisi della rete e della geolocalizzazione per individuare l'uso di VPN o proxy, rilevazione di ambienti sospetti come emulatori o macchine virtuali e monitoraggio dei comportamenti durante la sessione per identificare pattern anomali o non umani, contribuendo così a contrastare attacchi automatizzati e tentativi di frode su larga scala.

Le tecniche procedurali, invece, riguardano invece la progettazione del processo di identificazione, prevedendo flussi strutturati e multi-step che includono acquisizione del documento, verifica biometrica tramite selfie o video, utilizzo di sistemi di *liveness detection* sia passiva che attiva, controlli avanzati sui documenti come analisi OCR, verifica degli elementi di sicurezza e confronto con database affidabili, gestione delle eccezioni con escalation verso operatori umani e separazione delle fasi critiche del processo per evitare punti singoli di compromissione, riducendo il rischio legato a *deepfake* e documenti falsificati.

In ultima analisi le tecniche organizzative si focalizzano sulla governance interna, prevedendo soprattutto una formazione continua del personale per il riconoscimento

delle frodi, ed in secondo luogo alcuni accorgimenti importanti come la segregazione dei ruoli in azienda per limitare i rischi di abuso interno, l'implementazione di audit e sistemi di *logging* per garantire tracciabilità e verificabilità delle operazioni, la gestione e il controllo dei fornitori terzi coinvolti nei processi di identificazione e l'adozione di pratiche di risk management dinamico, mirate ad aggiornare continuamente le difese in base all'evoluzione delle minacce.

Nel complesso, quindi, l'approccio ENISA si basa su di un tipo di difesa a strati o livelli, in cui quindi la sicurezza non è affidata a un singolo meccanismo ma a un ecosistema integrato di controlli che operano congiuntamente per prevenire, rilevare e mitigare i tentativi di frode in scenari sempre più complessi e caratterizzati dall'uso crescente di tecnologie sofisticate come l'intelligenza artificiale generativa.

Evoluzione del Regolamento eIDAS

Confronto tra eIDAS 1 (2014) e il nuovo regolamento eIDAS 2 (2024)

Aspetto	eIDAS 1 (2014)	eIDAS 2 (2024)
Identity Proofing	Presenza fisica o mezzi elettronici equivalenti.	Procedure armonizzate, EUDI Wallet, verifica remota avanzata.
Strumenti	Mezzi eID notificati.	Portafoglio Europeo (EUDI Wallet).
Obbligatorietà	Notifica volontaria dei regimi.	Obbligo per gli Stati di offrire il Wallet.
Controllo Utente	Limitato dal sistema nazionale.	Pieno controllo su dati e attributi.
Interoperabilità	Basata su livelli di garanzia.	Rafforzata tramite standard ETSI comuni.

11. CONCLUSIONI: IL FUTURO DELLA SOVRANITA' DIGITALE E LA RESILIENZA DEL SISTEMA

Il rafforzamento del quadro normativo eIDAS 2.0, unitamente alla progressiva introduzione dell'IT-Wallet, rappresenta un elemento strutturale per l'evoluzione della resilienza digitale a livello nazionale ed europeo. In tale contesto, la sicurezza sistemica non può essere ricondotta esclusivamente alla solidità degli algoritmi crittografici

adottati, ma deve essere inquadrata in un modello architetturale più ampio, fondato su un approccio *security-by-design* e su una integrazione coerente tra componenti *software*, *hardware* e processi di *governance*.

In particolare, risulta imprescindibile privilegiare l'impiego di ancoraggi crittografici di tipo *hardware*, rispetto a soluzioni basate unicamente sull'analisi di segnali video o biometrici, intrinsecamente più esposti a vulnerabilità derivanti da tecniche avanzate di manipolazione, tra cui *deepfake* e attacchi di *spoofing* basati sul ricorso all'intelligenza artificiale.

La costruzione della fiducia digitale deve essere concepita pertanto come un'infrastruttura complessa e multilivello, non riducibile a una variabile opzionale o a una caratteristica accessoria del sistema. Essa richiede la definizione di un modello di identità digitale interoperabile, riutilizzabile e conforme ai principi di *self-sovereign identity*, in cui cioè l'utente mantenga il pieno controllo sui propri attributi identificativi e sulle modalità di condivisione degli stessi.

La continuità operativa e la robustezza dell'ecosistema digitale dipendono dalla capacità di integrare in modo sinergico fonti autentiche primarie con meccanismi di verifica crittografica avanzata, inclusi schemi di firma digitale qualificata, attestazioni verificabili e protocolli di autenticazione forte basati su chiavi asimmetriche. Parallelamente, è necessario implementare un modello di *governance* distribuito, caratterizzato da una chiara definizione dei ruoli e delle responsabilità tra autorità pubbliche, *provider* tecnologici e soggetti privati, al fine di garantire trasparenza, auditabilità e gestione efficace del rischio lungo l'intero ciclo di vita dell'identità digitale.

In tale prospettiva, l'interoperabilità transfrontaliera costituisce un requisito imprescindibile per il funzionamento del mercato unico digitale europeo, imponendo l'adozione di *standard* aperti e di *framework* tecnologici condivisi che consentano il

riconoscimento reciproco delle identità e delle credenziali elettroniche tra Stati membri. Solo attraverso una convergenza tra componenti normative, tecniche e organizzative sarà possibile costruire un ecosistema affidabile, resiliente e scalabile, in grado di sostenere la trasformazione digitale e di contrastare efficacemente le minacce emergenti, incluse quelle derivanti dall'evoluzione delle tecnologie di intelligenza artificiale.

In questo scenario, l'Agenzia per l'Italia Digitale svolge una funzione essenziale di coordinamento, indirizzo e certificazione, agendo quale autorità di riferimento nella definizione degli standard tecnici, nella supervisione dei fornitori di servizi fiduciari e nella garanzia di conformità ai requisiti normativi europei.