DIGITAL INSIGHTS

Adeguata verifica con SPID e CIE: facciamo chiarezza

Giugno 2024

Intesa

Indice

Adeguata verifica con SPID: facciamo chiarezza

L'adozione di un'identità digitale è oggi una necessità sempre più rilevante per i cittadini, con lo SPID e la CIE che rappresentano le principali soluzioni disponibili.

Istituito dall'art. 64 del Codice dell'Amministrazione Digitale (CAD), lo SPID consente un accesso sicuro ai servizi online delle pubbliche amministrazioni e dei privati. A partire dal "Decreto Semplificazioni", l'utilizzo di identità digitali come SPID e CIE ha contribuito a rendere più efficienti e rapidi i processi aziendali, rispondendo anche alle esigenze normative in ambito Anti Money Laundering (AML). In particolare, queste soluzioni sono ora utilizzabili per l'adeguata verifica del cliente (KYC), garantendo un'identificazione certa e conforme alle normative vigenti.

L'utilizzo di SPID e CIE per l'adeguata verifica è reso possibile grazie alle modifiche introdotte dal Decreto Semplificazioni e ai provider di servizi accreditati da AgID. Facciamo chiarezza

1.

Gli attori delle identità digitali: identity provider, service provider e aggregatori

Innanzitutto, per comprendere come è possibile risolvere l'adeguata verifica con SPID e CIE, bisogna conoscere le **3 tipologie di accreditamento** che i soggetti privati possono ottenere dall'Agenzia per l'Italia Digitale (AgID) per lavorare nell'ambito delle identità digitali: gli identity provider, i service provider e gli aggregatori.

1.1 Gli identity provider, ovvero chi rilascia lo SPID

L'identità digitale SPID può essere rilasciata dai Gestori di Identità Digitale (o identity provider), soggetti privati accreditati da AgID che, nel rispetto delle regole emesse dall'Agenzia stessa, forniscono le identità digitali e garantiscono l'identificazione degli utenti.

A marzo 2025 gli **SPID complessivamente attivati** in Italia hanno raggiunto i **40 milioni**.

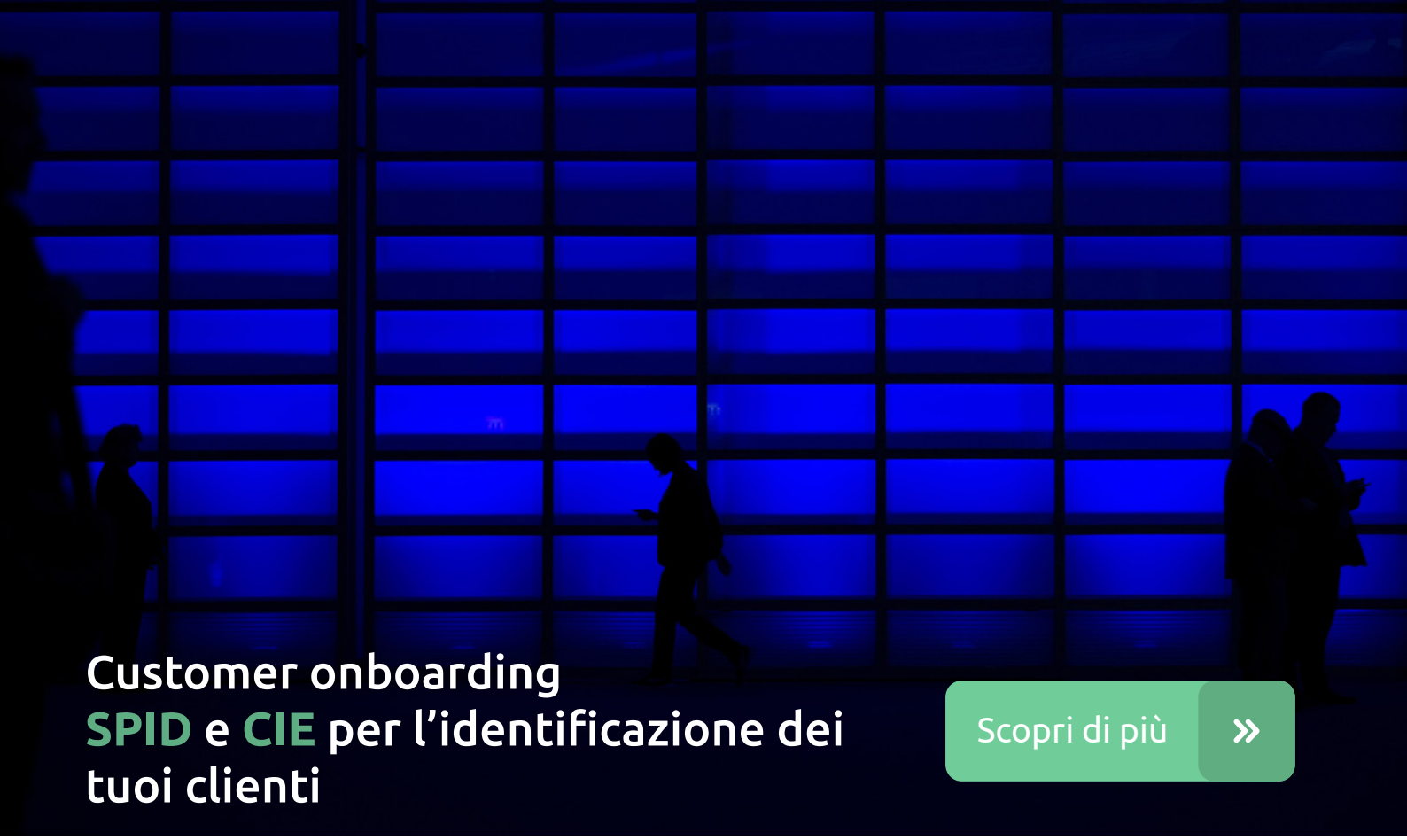
Per tutelare le persone fisiche dal furto d'identità, prima di rilasciare le identità digitali, gli identity provider devono provvedere all'identificazione certa delle persone fisiche per mezzo di appositi processi e strumenti individuati dal AgID, per esempio con video-identificazione o con una richiesta firmata digitalmente con un certificato qualificato emesso da una Certification Authority (Firma Elettronica Qualificata).

1.2 I service provider, ovvero chi può erogare servizi utilizzando SPID e CIE

Oltre agli identity provider, ricoprono un ruolo altrettanto importante nella gestione di SPID i service provider (SP).

I service provider sono quei soggetti che, per mezzo di apposita convenzione con AgID, **possono erogare i propri servizi (e solo i propri servizi) a tutti coloro che sono in possesso di un'identità digitale SPID o CIEid,** verificando le credenziali degli utenti che richiedono l'accesso ai servizi attraverso una "chiamata" all'identity provider che ha rilasciato lo SPID.

FIGURA:
*Secondo la determina relativa allo schema per l'adesione dei fornitori di servizi privati al Sistema Pubblico per l'Identità Digitale i dati non potrebbero essere comunicati a terzi.



Customer onboarding SPID e CIE per l'identificazione dei tuoi clienti

Scopri di più »

DATI OSSERVATORIO DIGITAL IDENTITY 2024

216

SERVICE PROVIDER PRIVATI PER **SPID**

53

SERVICE PROVIDER PRIVATI PER **CIE**

Precisiamo che gli utenti in possesso dell'identità digitale SPID potranno usufruire del predetto servizio indipendentemente dall'identity provider che ha rilasciato SPID, come disposto dall'art. 1 lett. i) DPCM 24 ottobre 2014. Il service provider, dunque, dovrà accettare le credenziali emesse da qualsiasi identity provider.

Infine, i service provider si possono distinguere in pubblici e privati. I primi sono enti pubblici quali ad es. INPS e Agenzia delle Entrate che erogano servizi ai cittadini. I secondi, invece, sono provider privati che erogano servizi alla propria clientela, per esempio una Certification Authority che voglia rilasciare una firma digitale ai propri clienti.

Diventare service provider: un iter lungo e complesso

Tutti i soggetti privati possono accreditarsi come service provider. Tuttavia, dovendo garantire una costante sicurezza e affidabilità dell'intero ecosistema, l**a procedura di accreditamento prevede un iter** di qualificazione tecnica e amministrativa **particolarmente complesso e lungo**. Lo scopo di questo iter è quello di presentare ad AgID le motivazioni e le finalità per cui il soggetto intende diventare service provider, come prevede di utilizzare le credenziali e quali sono le caratteristiche di affidabilità da lui garantite.
Non tutte le aziende, quindi, possono ritenersi by default in possesso dei requisiti, delle risorse o delle capacità necessarie per intraprendere la procedura di accreditamento e quindi erogare i propri servizi all'interno della federazione secondo gli standard previsti.

1.3 I soggetti aggregatori, un nuovo capitolo

I soggetti aggregatori sono pubbliche amministrazioni o privati che **offrono a terzi** (cosiddetti "soggetti aggregati") **la possibilità di rendere accessibili con SPID e CIE i rispettivi servizi**, e rappresentano una grande opportunità per tutte quelle aziende che, per i motivi più svariati, non sono in grado di ottenere l'accreditamento AgID come service provider privati.

Gli aggregatori si possono distinguere in aggregatori di servizi pubblici e aggregatori di servizi privati. I primi, in particolare, si pongono al servizio di quelle pubbliche amministrazioni che vogliono erogare i propri servizi digitali senza doversi accreditare o abilitare come service provider.
I secondi, i soggetti aggregatori privati, possono supportare aziende private rendendo possibile l'utilizzo di SPID e CIE anche per accedere a servizi di fornitura (energy & utilities), leasing e telco.

Dopo grande attesa da parte delle aziende (in particolare dei settori energy & utilities, leasing e telco) il **31 marzo 2022 è stata emanata la convenzione anche per i soggetti aggregatori privati**, aprendo un nuovo capitolo per l'utilizzo dell'identità digitale SPID per l'accesso ai servizi da remoto.

2.

SPID, CIE e adeguata verifica del cliente

Come già riportato, in riferimento all'utilizzo di SPID o CIEid in ambito bancario è fondamentale riferirsi al cosiddetto Decreto Semplificazioni (d.l. n. 76/2020), che ha introdotto importanti novità nella disciplina antiriciclaggio, soprattutto per quanto riguarda le procedure di identificazione della clientela per l'accesso ai servizi bancari, finanziari e assicurativi.

2.1 I riferimenti normativi e gli estremi del documento di identità

DATI OSSERVATORIO DIGITAL IDENTITY 2024

862 mln

accessi con SPID effettuati tra gennaio e ottobre 2024

48,2 mln

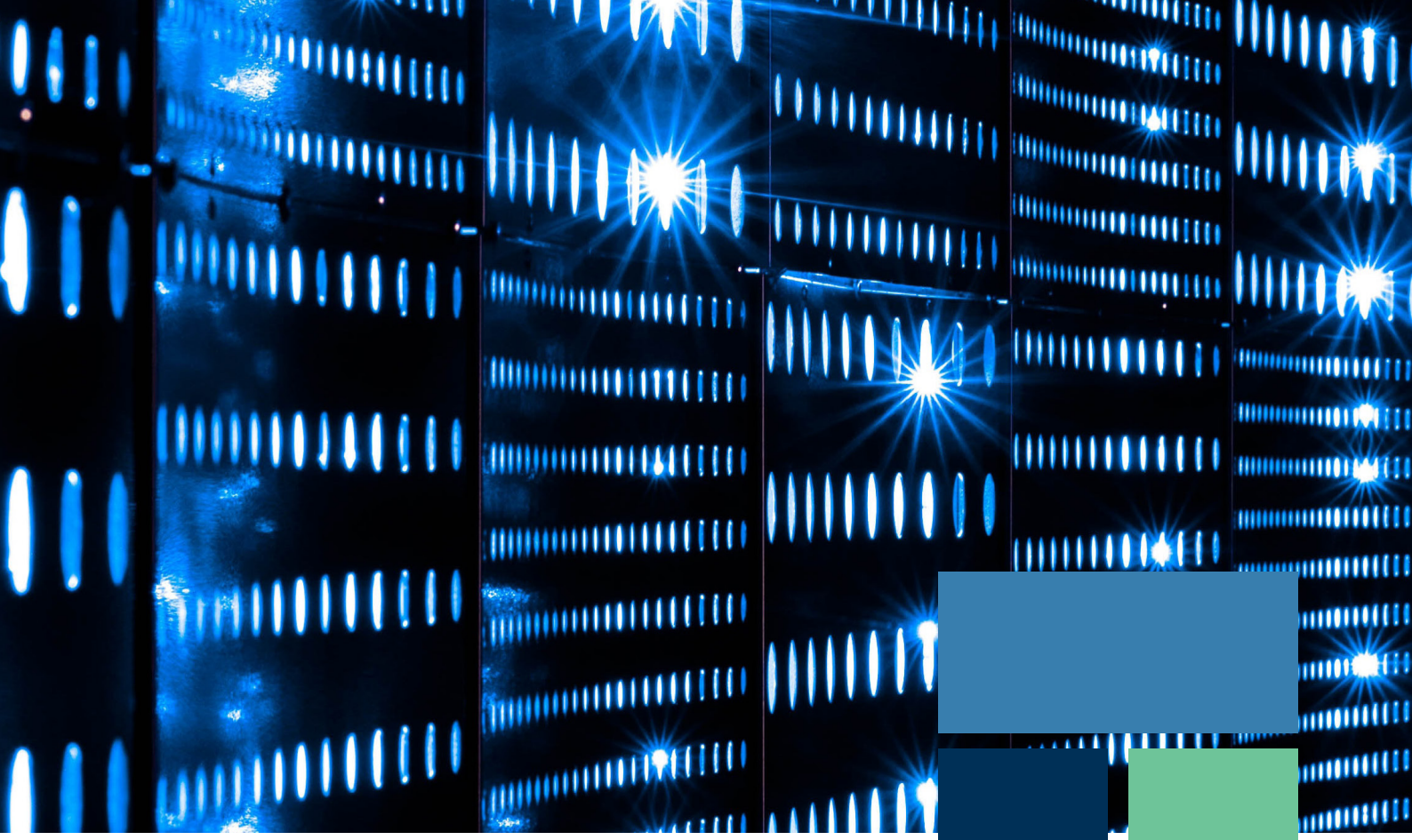
CIE rilasciate fino a gennaio 2024

Nello specifico, l'articolo 27 del Decreto Semplificazioni (d.l. n. 76/2020) **modifica gli art. 1 comma 2 e 19 comma 1 del D.lgs. n. 231/2007 riguardanti la disciplina AML** (Anti Money Laundering).

Queste modifiche prevedono:

- che non sia più obbligatorio acquisire i documenti di identità in fase di identificazione forte del cliente: *«le parole "gli estremi del documento di identificazione" sono soppresse»*;

- che l'obbligo di identificazione nell'ambito dell'adeguata verifica possa considerarsi assolto attraverso determinati strumen-



ti digitali tra cui, appunto: *«per i clienti in possesso di un'identità digitale, con livello di garanzia almeno significativo, nell'ambito del Sistema di cui all'articolo 64 del predetto decreto legislativo n. 82 del 2005 (c.d. "CAD", ndr), e della relativa normativa regolamentare di attuazione, nonche' di un'identita' digitale con livello di garanzia almeno significativo, rilasciata nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione europea a norma dell'articolo 9 del regolamento UE n. 910/2014, o di un certificato per la generazione di firma elettronica qualificata o, infine, identificati per mezzo di procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale».*

Sarà quindi possibile considerare l'obbligo di identificazione assolto, senza necessità di raccogliere gli estremi del documento,* laddove i clienti siano in possesso di un'identità digitale SPID o CIE.

*** Solo nel caso di identificazione da remoto. Gli estremi del documento di identità dovranno comunque essere acquisiti nel caso di identificazione in presenza.**

Tuttavia, ciò non significa che banche, assicurazioni e istituti finanziari possono richiedere semplicemente un'identificazione con SPID o CIE per concludere la prima parte dell'adeguata verifica: il lettore attento infatti si ricorderà che solo *"i service provider possono erogare i propri servizi (e solo i propri servizi) a tutti coloro che sono in possesso di un'identità digitale SPID, verificando le credenziali degli utenti"*.

L'utilizzo di SPID e CIE per identificare gli utenti può avvenire solo nel rapporto tra il service provider e la propria clientela

2.2 FEQ e trusted services per la condivisione dei dati

Quindi, per utilizzare SPID e CIE nell'Adeguata Verifica, tutti gli istituti finanziari devono ottenere l'accreditamento come service provider privati? Non necessariamente: è possibile infatti che sia un altro service provider, già accreditato AgID, a effettuare l'identificazione e la raccolta dei dati per rilasciare i propri servizi. Per esempio, nel caso di un service provider che sia anche un Qualified Trust Service Provider, **il service provider potrà effettuare l'identificazione per rilasciare un certificato di firma qualificato. Lo stesso certificato di firma qualificata verrà poi utilizzata per portare a termine l'identificazione a distanza ai sensi AML**, come previsto dalla norma di settore.

Naturalmente, l'utente finale dovrà utilizzare, previa autorizzazione, lo stesso certificato di firma qualificata rilasciato dal service provider e QTSP per sottoscrivere il documento con cui l'istituto bancario, assicurativo o di credito potrà effettuare l'identificazione certa.

Nel caso di Intesa, service provider SPID e CIE accreditato AgID, la raccolta dei dati e l'identificazione avverrà con lo scopo di **emettere un certificato di firma elettronica qualificata (servizio di Intesa), con cui il cliente firmerà un modulo di *data privacy***. Tale modulo potrà poi essere utilizzato dal servizio principale (per esempio l'istituto bancario) per accertarsi dell'identità dell'utente che ha effettivamente apposto la firma elettronica qualificata.

Il divieto di divulgazione dei dati

Secondo la determina la determina ***"relativa allo schema di convenzione per l'adesione dei fornitori di servizi privati al sistema pubblico per le identità digitali"***, per il service provider è vietato mettere a disposizione di terzi le informazioni e i dati acquisiti in fase di identificazione. Per quanto questo divieto di divulgazione dei dati personali, in linea teorica, potrebbe essere ritenuto conforme ai dettami normativi in termini di privacy, è anche vero che la comunicazione dei dati personali ad un terzo soggetto potrebbe rispondere a un'esigenza propria dell'utente (cfr. art. 6 Regolamento UE 2016/679: ***"Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità"***). L'utente potrebbe infatti avere tutto l'interesse a vedersi riconosciuto, con una sola autenticazione, sia l'identificazione per accedere al servizio del service provider sia l'identificazione ai fini dell'onboarding presso un terzo.

Banca

Intesa

1.
l'utente vuole accedere al servizio

2.
la procedura si sposta su piattaforma Intesa: accesso con SPID o CIE (senza cambiare UX)

3.
Intesa emette certificato FEQ

4.
L'utente firma documenti con firma EQ

5.
Intesa condivide il documento con istituto regolato (ad es. banca)

6.
Istituto ha identificato l'utente, che può concludere la procedura

3.

Identificazione e autenticazione: una differenza importante

Si è parlato, all'interno di questo documento, esclusivamente di identificazione con SPID e CIE, che può essere effettuata solo dai service provider.

E per quanto riguarda l'autenticazione con SPID?
Qual è la differenza?

3.1 Identificazione e autenticazione: una differenza importante

Tutto dipende da quante informazioni si ha necessità di ottenere, e se si è già in possesso di alcune di queste. L'identificazione, infatti, avviene nel momento in cui l'onboarding del cliente non è ancora stato effettuato e nessuno dei suoi dati è già presente nel database. Una volta effettuata l'identificazione, l'erogatore del servizio potrà scegliere se richiedere l'utilizzo delle credenziali SPID o CIE anche in fase di autenticazione al portale, oppure fornire altre credenziali (come, per esempio, quelle bancarie).

L'autenticazione, invece, avviene nel momento in cui l'onboarding del cliente è già stato effettuato, e quindi molti dei suoi dati sono già presenti all'interno di un database. In questo caso, infatti, l'autenticazione potrà avvenire con le credenziali SPID, ma l'identity provider condividerà solo le informazioni strettamente necessarie a ricollegare le credenziali con i dati già in possesso di chi eroga il servizio (ad esempio il codice fiscale).

4.

La rivoluzione dell'EUDI Wallet

Il 29 febbraio 2024 il Parlamento Europeo ha approvato la revisione del regolamento eIDAS, il regolamento europeo sui servizi fiduciari e sulle identità digitali, che porta con sé l'istituzione dell'European Digital Identity Wallet, l'identità digitale europea che sarà valida obbligatoriamente in tutta l'UE.

Intorno all'EUDI Wallet c'è molta attesa da parte delle aziende private e delle istituzioni, principalmente per la sua struttura a "portafoglio" digitale. All'interno dell'EUDI Wallet, infatti, si troveranno non solo i dati anagrafici ma potranno anche essere raccolte certificazioni e documenti verificabili e verificati – i cosiddetti "attributi" – quali estremi di passaporto, certificato di nascita, patente e tessera elettorale.

I vari use case del wallet sono oggi al vaglio dei Large Scale Pilot, e prima di comprendere effettivamente l'impatto che potrà avere il wallet sulle procedure di adeguata verifica bisognerà attendere almeno il primo rilascio di Implementing Acts. Tuttavia la possibilità di inserire, all'interno dell'identità digitale europea, anche informazioni che vanno oltre le informazioni di base apre nuove interessantissime possibilità per i servizi privati, finanziari e non, e per la verifica dell'affidabilità creditizia.

Intesa, a Kyndryl Company

Intesa, a Kyndryl Company è un Digital Solution Provider nell'ambito della digitalizzazione dei processi aziendali e dei servizi fiduciari e una società Benefit.
Da oltre 35 anni offriamo soluzioni modulari e adattabili alle esigenze di ogni mercato su scala globale. I nostri servizi rispettano i requisiti della normativa digitale e assicurano stabilità e sicurezza tecnologica, tenendo in considerazione la sostenibilità del business.

TORINO | MILANO | ROMA

Intesa.it

Intesa