

Allegato 2 - Estensione dell'utilizzo delle piattaforme nazionali di Identità Digitale (SPID e CIE)

Indice

INTERVENTI FINANZIABILI	2
DIMENSIONE FINANZIARIA E DEFINIZIONE DEL PACCHETTO IDENTITÀ DIGITALE	2
DURATA E TERMINI DI REALIZZAZIONE DEL PROGETTO	3
ADESIONE ALLE PIATTAFORME DI IDENTITÀ DIGITALI SPID E CIE	3
<i>Adesione alla piattaforma di identità digitale SPID</i>	3
<i>Adesione alla piattaforma di identità digitale CIE</i>	3
<i>Raccomandazioni progettuali</i>	4
INTERVENTI COMPLEMENTARI	4
<i>Utilizzo dello standard OpenID Connect</i>	5
<i>Erogazione del piano formativo</i>	5
INTEGRAZIONE NODO ITALIANO EIDAS	6

Interventi finanziabili

Il presente Avviso ha per oggetto la piena adozione delle piattaforme di identità digitale attraverso il raggiungimento dei seguenti **obiettivi**:

- Adesione alla piattaforma di identità digitale SPID.
- Adesione alla piattaforma di identità digitale CIE.
- Erogazione di un piano formativo su disposizioni normative, linee guida e best practices in caso di integrazione a SPID e CIE con protocollo SAML2

È inoltre raccomandata l'integrazione al nodo italiano eIDAS.

Dimensione finanziaria e definizione del pacchetto Identità Digitale

L'importo riconoscibile alle Pubbliche Amministrazioni per l'implementazione del pacchetto per l'Identità Digitale di cui al presente avviso è di 14.000,00 euro.

Il pacchetto è applicabile senza alcuna distinzione ai Soggetti Attuatori di cui all'art. 5 comma 1 dell'Avviso che erogano servizi online ai cittadini e che si trovano in uno degli scenari previsti dalla seguente "Tabella 1" a prescindere dal numero di servizi online erogati e dal bacino di utenza, anche potenziale.

Per servizi online, si intendono i servizi digitali erogati al cittadino dall'amministrazione, cioè l'insieme di interfacce digitali, flussi e procedure, tipicamente a seguito di un login identificativo, il cui scopo è che il cittadino richieda e si veda erogata una prestazione da parte dell'amministrazione, o effettui un adempimento verso l'amministrazione.

In considerazione del fatto che l'amministrazione aderente si può trovare in una situazione di parziale integrazione rispetto alle piattaforme SPID e CIE, sono ammissibili al finanziamento le amministrazioni che si trovano in uno dei seguenti scenari:

#	Scenario di partenza
a	Nessuna integrazione alle piattaforme SPID e CIE
b	Integrazione solo a SPID con protocollo SAML2
c	Integrazione solo a CIE con protocollo SAML2

Tabella 1: Scenari di partenza della Pubblica Amministrazione

Nel rispetto di quanto previsto dall'art. 8 commi 3, 4 e 5 l'obiettivo finale, per ciascuna amministrazione, sarà di assicurare l'adozione di entrambe le piattaforme di identità digitale (SPID e CIE), indifferentemente dal proprio scenario di partenza.

Inoltre, a tutte le amministrazioni che aderiscono alla misura è richiesto l'utilizzo dello standard OpenID Connect, o, in alternativa, l'erogazione di un piano formativo idoneo a costruire le basi per un successivo passaggio tecnologico. Ulteriori dettagli sull'utilizzo di OpenID Connect o sull'erogazione del piano formativo sono disponibili nel paragrafo "Interventi complementari".

Durata e termini di realizzazione del progetto

1. Le attività progettuali devono essere avviate a partire dalla data di notifica del decreto di finanziamento di cui all'art.10 dell'Avviso.
2. L'amministrazione aderente che intende avvalersi di fornitori esterni, soggetti aggregatori e gestori di servizi pubblici deve attivare il relativo contratto entro **12 mesi** dalla data di notifica del decreto di finanziamento; in alternativa deve segnalare la scelta di non ricorrere ad un fornitore esterno. In caso di ritardo l'amministrazione ne dovrà dare comunicazione attraverso apposita funzionalità disponibile nella Piattaforma.
3. Il progetto di integrazione deve essere concluso nel termine perentorio di **10 mesi** dalla data di contrattualizzazione del fornitore.



Adesione alle piattaforme di identità digitali SPID e CIE

Per l'adesione alle singole piattaforme di identità digitale si rimanda ai paragrafi dedicati e alla lettura delle raccomandazioni progettuali per l'esecuzione tecnica.

Adesione alla piattaforma di identità digitale SPID

Il processo di adesione a SPID prevede una serie di step tecnico amministrativi che portano alla conclusione del processo di onboarding. Per maggiori informazioni si rimanda al sito <https://www.spid.gov.it/cos-e-spid/diventa-fornitore-di-servizi/> e alle [regole tecniche](#) di AgID.

Adesione alla piattaforma di identità digitale CIE

Il processo di integrazione allo schema di autenticazione «Entra con CIE» prevede come prerequisito fondamentale l'onboarding del fornitore di servizi.

L'onboarding deve essere eseguito mediante il [portale di federazione erogatori di servizi](#), messo a disposizione dal Identity Provider e gestito e sviluppato dal Poligrafico che, in qualità di partner tecnologico del Ministero dell'Interno, ne cura tutti gli aspetti tecnici. In particolare il [portale di federazione erogatori di servizi](#) consente al fornitore di servizi di:

- registrarsi ed effettuare facilmente la richiesta di adesione
- federare i metadata e ricevere l'esito della federazione
- verificare in ogni istante lo stato delle attività

Per una lettura esaustiva della procedura di adesione alla piattaforma CIE e diventare fornitori di servizi si rimanda alla lettura del [manuale operativo per CIE](#)

Raccomandazioni progettuali

Anche se non vincolanti per il raggiungimento degli obiettivi di integrazione a SPID e CIE e quindi all'ottenimento del pacchetto di incentivazione, si suggerisce di dare seguito alle seguenti attività progettuali:

- Assessment del progetto di integrazione:
 - identity management assessment: descrizione dei servizi online al cittadino da integrare, delle attività e delle azioni necessarie per l'integrazione
 - analisi comparativa della soluzione tecnologica prescelta per l'integrazione a SPID e CIE, come richiesto dal CAD ([CAD Art. 68¹](#))
- Pianificazione ed esecuzione del progetto:
 - Realizzazione di uno IAM (Identity and Access Management) Proxy SPID/CIE come Service Provider di tipo Public, componente tecnologico che rende possibile l'integrazione a SPID e CIE dei servizi online al cittadino della Pubblica Amministrazione
 - Onboarding amministrativo e tecnico del servizio IAM Proxy a SPID e a CIE

¹ [Codice dell'amministrazione digitale | Art. 68. Analisi comparativa delle soluzioni \(italia.it\)](#)

- Integrazione dei servizi web della PA allo IAM Proxy, e successivo collaudo tecnico (interno alla organizzazione)
- Rilascio a catalogo della soluzione IAM Proxy realizzata. Se invece questa fosse già presente a catalogo, è richiesta l'aggiunta del valore *usedBy*, all'interno del file [publiccode.yaml²](#) relativo alla Amministrazione abilitata.

Si fa presente che il processo di realizzazione dello IAM Proxy potrebbe essere sostituito dalle seguenti soluzioni equivalenti:

- Acquisto da parte della PA di un servizio di aggregazione tramite convenzione con un soggetto aggregatore accreditato da AgID e/o dall'Istituto Poligrafico e Zecca dello Stato in previsione della procedura che regola il ruolo dei soggetti aggregatori anche per la Carta d'Identità Elettronica.
- Integrazione a SPID/CIE mediante Gestore di Pubblico Servizio come da avviso SPID n°6 del 29/07/2016³.
- Integrazione dei singoli servizi online al cittadino e relativa procedura di onboarding con AGID e Interno/IPZS per ciascuno di essi.

Interventi complementari

Obiettivo complementare del presente avviso è incentivare l'evoluzione tecnologica delle piattaforme di identità digitale SPID e CIE attraverso l'adozione dello standard OpenID Connect.

In alternativa è necessaria l'erogazione di un piano formativo, idoneo a costruire le basi per un successivo passaggio tecnologico.

Il presente avviso stimola questo avanzamento attraverso il riconoscimento di una somma forfettaria di 3.000,00 euro (già compresa nella misura complessiva dell'intervento), volti a coprire il passaggio tecnologico ad OpenID Connect, o, in alternativa, l'erogazione del piano formativo per il successivo passaggio tecnologico.

Utilizzo dello standard OpenID Connect

OpenID Connect (OIDC) è lo standard di autenticazione attualmente utilizzato dalla quasi totalità delle moderne applicazioni web e mobile nel mondo privato (Google, Microsoft, PayPal e molti

² standard di metadati ideato per essere inserito in repository contenenti software della Pubblica Amministrazione con lo scopo di renderli facilmente individuabili e, di conseguenza, riutilizzabili da altri enti.

³https://www.agid.gov.it/sites/default/files/repository_files/documentazione/spid-avviso-n6-note-sul-dispiegamento-di-spido-preso-i-gestori-di-servizi-v1.pdf

altri). Le caratteristiche di OpenID Connect rispetto al protocollo SAML2, precedentemente usato nell'integrazione a SPID e CIE, sono:

- maggiore sicurezza;
- maggiore facilità di integrazione in sistemi eterogenei (single-page app, web, backend, mobile, IoT);
- migliore integrazione di componenti di terze parti in modalità sicura, interoperabile e scalabile.

Tra gli altri vantaggi, OpenID Connect consente: di evitare potenziali attacchi attuati mediante l'intercettazione delle comunicazioni tra i vari attori coinvolti, soprattutto nel caso di applicazioni per dispositivi mobili. Inoltre, di evitare continui inserimenti di password e migliorare la user experience nelle applicazioni mobili attraverso l'utilizzo delle cosiddette sessioni lunghe revocabili. In virtù delle suddette considerazioni e del fatto che il passaggio al protocollo OpenID Connect rientra nel percorso di evoluzione strategica delle Identità Digitali, la misura al presente avviso rappresenta un'importante occasione per fare evolvere i sistemi informativi delle amministrazioni nella direzione auspicata. Pertanto seppur non è obbligatorio, il passaggio a OpenID Connect per SPID e CIE è fortemente raccomandato. Qualora le integrazioni coperte dal corrente avviso siano effettuate con protocollo OpenID Connect, non è necessaria l'erogazione del piano formativo.

Erogazione del piano formativo

L'erogazione di un piano formativo di almeno 25 ore è vincolante al completamento con esito positivo del progetto nel caso in cui l'integrazione ad una o entrambe le piattaforme avvenga con il protocollo SAML2 ed in ottica di garantire all'amministrazione le competenze interne necessarie per la successiva migrazione al protocollo OIDC.

Il piano formativo deve articolarsi su due livelli:

- il primo, di carattere normativo, riguarda la gestione dell'identità elettronica da un punto di vista normativo, e può comprendere i seguenti aspetti:
 - Regolamento UE 1502/2015 relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014..
 - Regolamento UE 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.
 - Legge N. 120 del 11/09/2020, «Misure urgenti per la semplificazione e l'innovazione digitali» (Decreto Semplificazioni) con particolare attenzione al Capo 1, articoli 24, 25 e 26 comma 8.
 - DPCM del 24 ottobre 2014 che definisce le caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi



e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.

- il secondo, di natura tecnica, può comprendere i seguenti aspetti:
 - Overview su OpenID Connect Core Specification
 - Overview su OpenID Connect Federation 1.0 Specification
 - Linee guida per OpenID Connect in SPID
 - Regole tecniche OpenID Connect per CIE
 - Conservazione dei logs, buone pratiche e trasferimento di know-how necessario per l'utilizzo della nuova tecnologia e per l'implementazione dei servizi con SPID e CIE.

Integrazione nodo italiano eIDAS

Al fine di promuovere la cooperazione transfrontaliera e l'interoperabilità dei sistemi nazionali di identificazione elettronica (eID) e facilitare l'accesso dei cittadini e delle imprese ai servizi online ai cittadini nei diversi Stati membri⁴, è fortemente suggerita l'integrazione delle proprie soluzioni informatiche al nodo italiano eIDAS nello sforzo di affermare la diffusione e l'utilizzo delle identità digitali.

Sul sito <https://www.eid.gov.it/> è possibile trovare tutte le informazioni necessarie per procedere con l'integrazione.

⁴ in cui tale accesso è consentito tramite l'autenticazione eID