Presidenza del Consiglio dei Ministri

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Determina 187/2023

Il Capo del Dipartimento per la trasformazione digitale

Visto il *regolamento (UE) 2014/910* del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, che fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro;

Visto il *regolamento di esecuzione (UE) 2015/1501* della Commissione dell'8 settembre 2015 relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, che stabilisce i requisiti tecnici e operativi del quadro di interoperabilità al fine di garantire l'interoperabilità dei regimi di identificazione elettronica che gli Stati membri notificano alla Commissione;

Visto il *regolamento (UE) 2016/679* del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Visto il *regolamento (UE) 2016/1191* del Parlamento europeo e del Consiglio del 6 luglio 2016, che promuove la libera circolazione dei cittadini semplificando i requisiti per la presentazione di alcuni documenti pubblici nell'Unione europea e che modifica il regolamento (UE) n. 2012/1024;

Visto il *regolamento (UE) 2018/1724* del Parlamento europeo e del Consiglio del 2 ottobre 2018 che istituisce uno sportello digitale unico per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 2012/1024 ed in particolare, l'articolo 6 che prevede che ciascuno Stato membro debba provvedere affinché i cittadini dell'Unione europea nonché le persone fisiche residenti in uno Stato membro possano accedere alle procedure di cui all'allegato II ed espletarle interamente in linea e l'articolo 14 relativo al "Sistema tecnico per lo scambio transfrontaliero automatizzato di prove" tra autorità competenti di diversi Stati Membri, che deve essere utilizzato ai fini dell'eventuale acquisizione presso la competente

amministrazione di altro Stato Membro, di documentazione necessaria al procedimento di iscrizione anagrafica;

Visto il *regolamento di esecuzione (UE) 2022/1463* della Commissione del 5 agosto 2022 che definisce le specifiche tecniche e operative del sistema tecnico per lo scambio transfrontaliero automatizzato di prove e l'applicazione del principio «una tantum» a norma del regolamento (UE) 2018/1724 del Parlamento europeo e del Consiglio ed, in particolare, l'articolo 16 ai fini della determinazione della corrispondenza dell'identità e delle prove, che prevede l'acquisizione di ulteriori attributi oltre a quelli ottenuti dal processo di autenticazione eIDAS (individuato dal Regolamento EU 2018/1724);

Visto il "Piano Nazionale di Ripresa e Resilienza" presentato dall'Italia alla Commissione europea in data 30 giugno 2021 e valutato positivamente con Decisione del Consiglio ECOFIN del 13 luglio 2021, notificata all'Italia dal Segretariato generale del Consiglio con nota LT161/21 del 14 luglio 2021 che individua l'Agenzia per l'Italia Digitale quale soggetto attuatore della Missione 1, Componente 1, Investimento 1.3.2 - *Single Digital Gateway* e, pertanto, soggetto gestore delle componenti nazionali italiane;

Visto il decreto del Presidente della Repubblica 21 ottobre 2022, con il quale l'On. Giorgia Meloni è stata nominata Presidente del Consiglio dei Ministri;

Visto il decreto del Presidente della Repubblica del 31 ottobre 2022 con il quale il Sen. Alessio Butti è stato nominato Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri;

Visto il decreto del Presidente del Consiglio dei Ministri 25 novembre 2022, concernente la delega di funzioni nelle materie dell'innovazione tecnologica e della transizione digitale al Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri Senatore Alessio Butti, che comprendono altresì le funzioni di vigilanza di cui all'articolo 19 del decreto-legge 22 giugno 2012, n. 83, convertito con modificazioni, dalla legge 7 agosto 2012, n. 134, e per lo svolgimento delle quali si avvale del Dipartimento per la trasformazione digitale;

Visto il Decreto del Presidente del Consiglio Ministri del 24 novembre 2022, con il quale al Dott. Angelo Borrelli è stato conferito, ai sensi degli articoli 18 e 28 della legge 23 agosto 1988 n. 400, nonché dell'articolo 19 del decreto legislativo 30 marzo 2001, n. 165, l'incarico di Capo Dipartimento per la Trasformazione Digitale;

Acquisita la nota prot. DTD 5266-A con cui AgID ha trasmesso al Dipartimento per la trasformazione digitale il Regolamento di funzionamento delle componenti nazionali SDG;

Presidenza del Consiglio dei Ministri

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Considerata la necessità di approvare il regolamento di funzionamento nell'ambito delle attività propedeutiche al raggiungimento della Milestone Missione 1, Componente 1, Investimento 1.3.2.

APPROVA

L'allegato 1 recante il Regolamento di funzionamento delle componenti nazionali SDG.

Angelo Borrelli

BORRELLI
ANGELO
PRESIDENZA
CONSIGLIO
DEI MINISTRI
06.12.2023
16:39:01
GMT+01:00

Progetto Single Digital Gateway (SDG)

Single Digital Gateway

Regolamento di Funzionamento delle componenti nazionali

Versione 1.0.0

Stato del documento: Final

Classificazione del documento: AgID Internal

28/09/2023

(Pagina lasciata intenzionalmente bianca)

INDICE

1 AMBITO ED OBIETTIVO

1.1 PREMESSA

Il **regolamento (UE) 2018/1724 del Parlamento Europeo e del Consiglio (Regolamento SDG)** del 2 ottobre 2018 stabilisce le norme per l'istituzione di uno Sportello Digitale Unico (SDG – Single Digital Gateway) per l'accesso a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi e che modifica il regolamento (UE) n. 1024/2012. L'obiettivo è potenziare la dimensione del mercato interno delle procedure in linea e contribuire in tal modo alla digitalizzazione dello stesso, accogliendo il principio generale di non discriminazione, tra l'altro in relazione all'accesso in linea da parte dei cittadini o delle imprese a procedure già stabilite a livello nazionale sulla base del diritto dell'Unione o nazionale e a quelle che devono essere rese interamente disponibili in linea conformemente al presente regolamento.

Il regolamento detta la base per la messa a punto e l'uso di un "**sistema tecnico" (Once-Only Technical System)** pienamente operativo, **sicuro e protetto** per lo **scambio transfrontaliero e automatizzato di prove** (Evidence) secondo il **principio del Once-Only** ("una tantum") tra i soggetti coinvolti, ovvero tra i Portali della Pubblica Amministrazione, denominati Procedure Portal (PP) e le Pubbliche Amministrazioni che possiedono il dato, denominate Data Service (DS).

Lo scambio di prove può avvenire nel perimetro delle procedure SDG, ove sia richiesto esplicitamente dai cittadini e dalle imprese, offrendo informazioni di alta qualità, procedure efficienti e interamente digitalizzate, in grado di facilitare l'interazione dei cittadini e delle imprese con il mondo delle Pubbliche Amministrazioni, in un'esperienza in grado di arricchire il mercato unico europeo.

1.2 OBIETTIVO

In tale contesto e considerando come input i diversi elaborati dell'Unione Europea in termini di specifiche tecniche per la realizzazione del OOTS, il presente documento ha l'obiettivo di descrivere l'ipotesi di soluzione per le componenti italiane considerando le peculiarità del contesto italiano. La progettazione riportata è coerente con quanto previsto dai documenti tecnici aggiornati all'ultima versione pubblicata.

1.3 CONTESTO DI RIFERIMENTO

L'iniziativa del **Single Digital Gateway** rappresenta un'importante punto di partenza e una opportunità per l'**interoperabilità tra le pubbliche amministrazioni dei diversi stati membri della Unione Europea**, nell'espletamento delle procedure amministrative che richiedono uno scambio transfrontaliero di informazioni già in possesso della PA, seguendo quindi il principio del Once-Only. Secondo quanto specificato nello stesso all'**art. 14 del Regolamento SDG**, il **Once-Only Technical System** dovrà soddisfare i seguenti **requisiti primari**:

a) consentire il trattamento delle richieste di prove su **richiesta esplicita dell'utente**;
b) consentire il trattamento delle richieste di **scambio di prove o di accesso ad esse**;
c) consentire la **trasmissione delle prove tra Amministrazioni competenti**;

d) consentire il **trattamento delle prove da parte dell'Amministrazione competente richiedente**;
e) garantire la **riservatezza e l'integrità delle prove**;
f) prevedere la possibilità per l'utente di **esaminare le prove** che devono essere utilizzate dall'Amministrazione richiedente competente e di **scegliere se procedere o meno al recupero delle prove**;
g) garantire un **adeguato livello di interoperabilità** con altri sistemi pertinenti, nonché un **elevato livello di sicurezza** per la trasmissione e il trattamento delle prove;
h) **non trattare le prove al di là di quanto necessario** sul piano tecnico per lo scambio delle stesse e successivamente solo per la durata necessaria a tal fine.

Nella visione del regolamento, un ruolo fondamentale è rivestito dal **portale unico europeo** (https://europa.eu/youreurope/), come punto di snodo per trovare informazioni su diritti e doveri dei cittadini europei ma anche per poter accedere ai servizi con procedure completamente online offerte dai diversi Portali Amministrativi esposti dagli Stati Membri. Il network di cooperazione amministrativa è garantito dalla realizzazione per ogni Stato Membro di un **gateway SDG**, composto da componenti e strutture in grado di garantire l'interoperabilità semantica, che metterà in collegamento i **Portali della Pubblica Amministrazione** (PP)ed i diversi **Soggetti Erogatori** di prove (DS) con i vicendevoli presenti negli altri Stati Membri, attraverso gli **eDelivery Access Point** ed un **gateway SDG centrale** a livello EU.

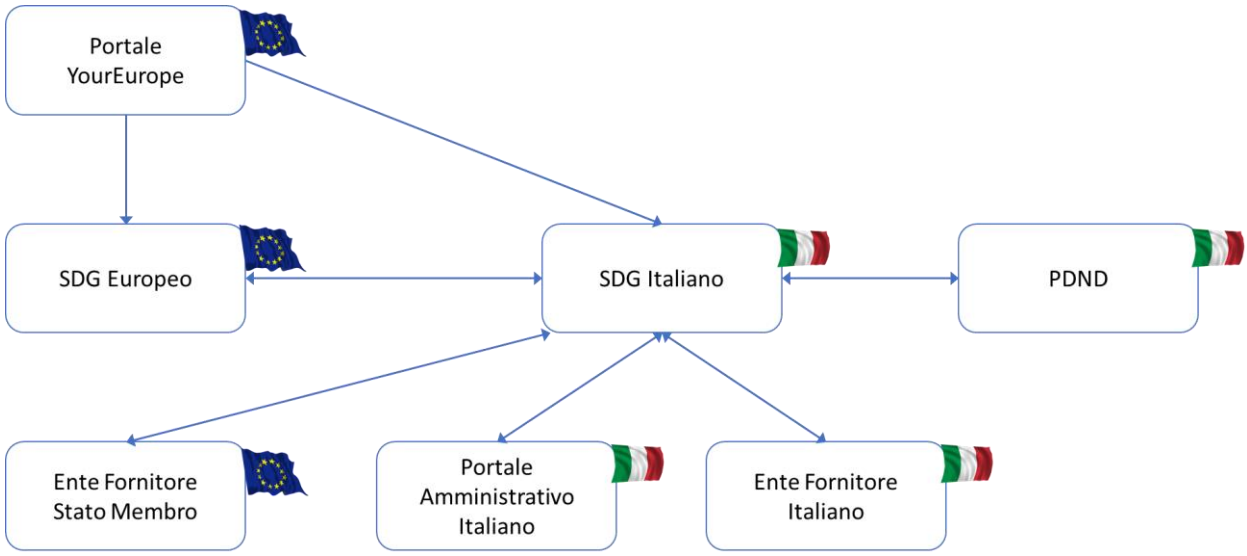

Figura 1 – Disegno alto livello delle interazioni SDG

Per ogni stato membro, la soluzione SDG prevede le seguenti componenti logiche, le cui specifiche tecniche sono allegate al presente documento:

A. **Catalogo dei servizi** – Componente nazionale utile a censire e descrivere i procedimenti amministrativi delle Pubbliche Amministrazioni coinvolte nel progetto SDG;

B. **Componente per l'eDelivery** (Access Point) – Componente necessaria ad abilitare lo scambio di dati tra Procedure Portal e Data Service, secondo il protocollo definito nel Regolamento SDG ed in particolare nel Technical Design Document (allegato all'Implenting Act di cui all'art. 14 comma 9) nel quale sono regolamentate le modalità di scambio di dati (Exchange Data Model). Lo scambio di dati è abilitato attraverso il nodo dell'Infrastruttura nazionale denominato Access Point, basato sullo standard OASIS ebXML RegRep versione 4.0;

C. **eID** – Il Regolamento SDG prevede all'art. 13 la realizzazione di un componente di autenticazione, basato sul Regolamento UE 2014/910 (Regolamento eIDAS), per l'accesso alle procedure in linea da parte di utenti transfrontalieri. Per quanto concerne il livello di sicurezza garantito in fase di autenticazione mediante eIDAS, si evidenzia quanto segue: Il livello di sicurezza è indicato nella "*authentication response*" fornita dall'Identity Provider (IDP) in risposta alla "*authentication request*" inviata dal Service Provider (SP) al momento della richiesta di autenticazione da parte dell'utente transfrontaliero. Il livello di sicurezza, come definito all'art. 6 lettera b del Regolamento UE n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 e nelle relative specifiche tecniche, potrà essere soltanto maggiore o uguale al livello indicato nella *authentication request* stessa.
In caso l'utente non disponga di una identità con un livello di sicurezza adeguato (maggiore o uguale a quello richiesto), il processo di autenticazione non va a buon fine e verrà restituito un messaggio di errore.
Si evidenzia, inoltre, che gli attributi minimi obbligatori (dati dell'utente condivisi) ricevuti dal SP in fase di autenticazione mediante eIDAS, sono quelli rappresentati in Figura 2 (*nome, cognome, data di nascita e identificativo univoco* associato all'identità eIDAS). L'identificativo univoco (costituito da: codice del paese identificatore/codice del paese destinatario della richiesta/combinazione alfa-numerica) permette di individuare il paese che ha rilasciato l'identità.

Mandatory attributes of the eIDAS minimum data set must always be requested and provided during the eIDAS authentication.

Attribute (Friendly) Name	eIDAS MDS Attribute	ISA Core Vocab Equivalent	Notes
FamilyName	Current Family Name	cbc:FamilyName	Encoded as xsd:string
FirstName	Current First Names	cvb:GivenName	Encoded as xsd:string
DateOfBirth	Date of Birth	cvb:BirthDate	Encoded as xsd:date
PersonIdentifier	Unique Identifier	cva:Cvidentifier	Encoded as xsd:string

Figura 2: eIDAS minimun data set

D. **Preview Space** – Componente che consente all'utente di visualizzare in anteprima le prove recuperate per mezzo del sistema OOTS, prima di utilizzarli nel procedimento amministrativo di interesse;

E. **Backbone Servizi SDG** – Insieme di componenti (Common Services) necessari per garantire l'interoperabilità, la ricerca ed il recupero delle prove e dei dati.

1.4 GLOSSARIO DEFINIZIONI ED ACRONIMI

Definizione/Acronimo	Descrizione
AdE	Agenzia delle Entrate
API	Application Programming Interface
eIDAS	electronic IDentification Authentication and Signature
MoDI	Modello Di Interoperabilità delle Pubbliche Amministrazioni
OOTS	Once Only Technical System
PA	Pubblica Amministrazione
PDND	Piattaforma Digitale Nazionale Dati per l'interoperabilità di dati e servizi
SBD	Standard Business Document (come definito dallo standard SBDH di UN/CEFACT)
SDG	Single Digital Gateway
MS	Stato Membro
UE	Unione Europea
PP	Procedure Portal
DS	Data Service
Regolamento eIDAS	Regolamento EU 2014/910
Regolamento SDG	Regolamento EU 2018/1724 del Parlamento Europeo e del Consiglio del 2 ottobre 2018
Regolamento di Esecuzione SDG	Regolamento di Esecuzione (UE) 2022/1463 della Commissione Europea del 5 agosto 2022
Regolamento di Esecuzione eIDAS	Regolamento di Esecuzione (UE) 2015/1501 della Commissione del 8 settembre 2015

1.5 RIFERIMENTI

ID	Titolo	Descrizione
DC_01	Technical Design Document	Specifiche tecniche e operative del Once Only Technical System, stabilite nel regolamento di esecuzione della Commissione ((UE) 2022/1463) che definisce il sistema preparate congiuntamente dalla Commissione e Stati membri. (https://ec.europa.eu/digital-building-blocks/wikis/display/OOTS/Technical+Design+Documents)
DC_02	Linee Guida PDND per interoperabilità	Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati (https://docs.italia.it/AgID/documenti-in-consultazione/lg-pdnd-docs/it/bozza/index.html)
DC_03	Repository GitHub SDG - Componenti Nazionali	Repository ufficiale della documentazione per l'integrazione (https://github.com/AgID/sdg_it_architype/tree/master/SDG%20-%20Componenti%20Nazionali)

2 LA SOLUZIONE ITALIANA

2.1 GLI ATTORI

I principali attori coinvolti nei processi gestiti tramite SDG sono i seguenti:

Soggetto	Ruolo	Sistema
AgID - Agenzia per l'Italia Digitale	Attuatore di SDG Italia	Infrastruttura nazionale SDG (Access Point, Catalogo dei servizi, Evidence Broker, Data Service Directory, Architecture Common Services, Preview Space)
Pubbliche Amministrazioni fruitrici di prove e dati	PA che tramite i portali istituzionali implementano l'erogazione di servizi inclusi nel Progetto SDG	Procedure Portal istituzionale
Pubbliche Amministrazioni erogatrici	Erogatori di servizi tesi al reperimento delle prove (Evidence) necessarie per portare a termine un procedimento amministrativo	Data Service
PagoPA	Responsabile per realizzazione della Piattaforma Digitale Nazionale Dati che abilita l'interoperabilità dei sistemi informativi degli Enti e dei Gestori di Servizi Pubblici.	PDND
Agenzia Delle Entrate	Fornitore del servizio di verifica di corrispondenza del Codice Fiscale dichiarato dall'utente con quello censito dall'Anagrafe Tributaria in corrispondenza di quanto fornito dal nodo eIDAS (nome, cognome, data di nascita del titolare) e quanto dichiarato dall'utente (Codice Fiscale, genere, Stato di nascita).	Servizio di verifica del CF

Tabella 1 - Attori Coinvolti nei processi gestiti da SDG

2.2 L'ARCHITETTURA

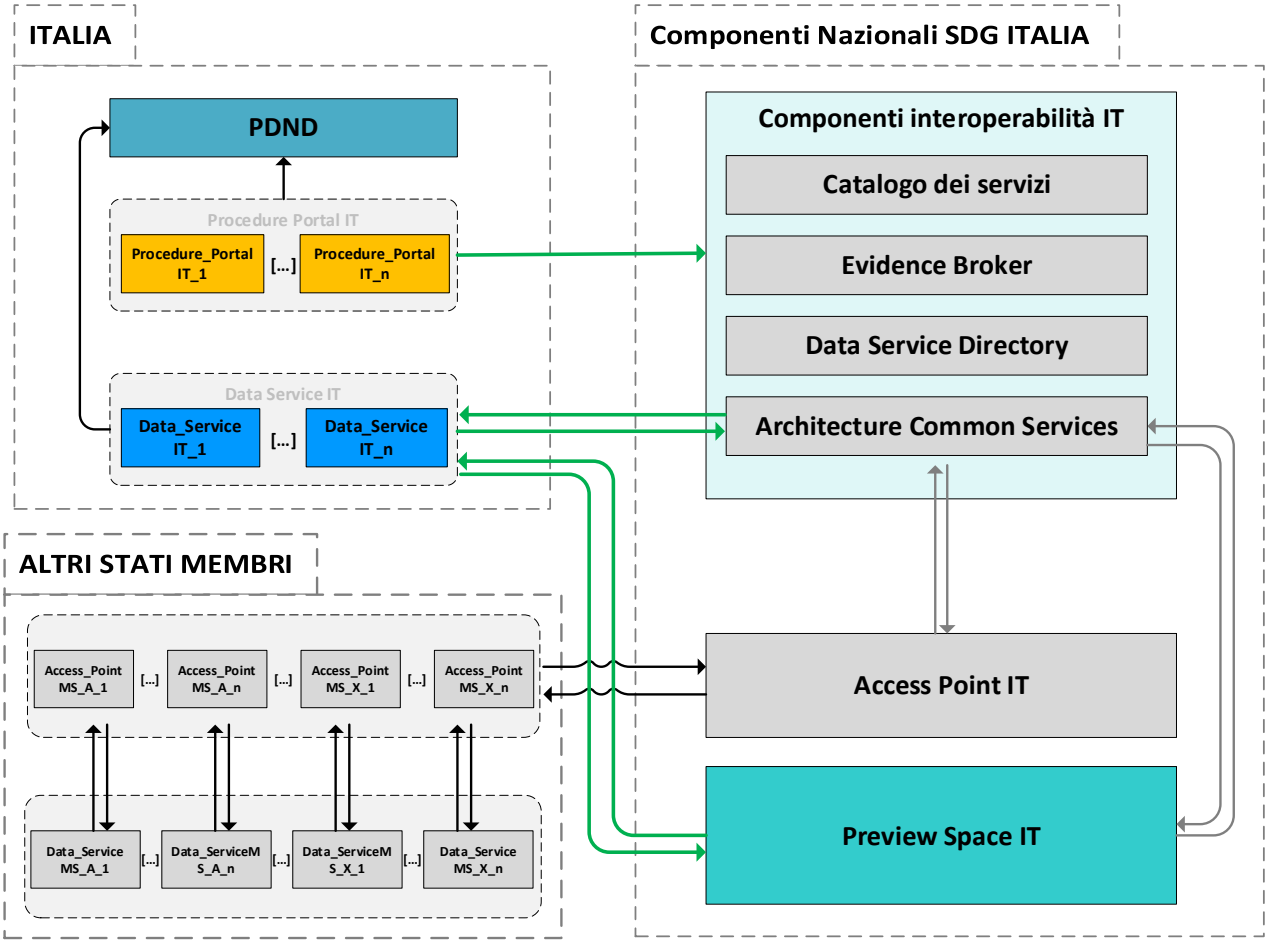

Figura 3 - Diagramma logico di architettura OOTS

Nel confine logico "Componenti Nazionali SDG ITALIA", rappresentato in Figura 3 sono presenti le seguenti componenti applicative:

- Blocco **Componenti Interoperabilità IT** contenente:
    - **Catalogo dei Servizi**
      Componente applicativo dell'infrastruttura SDG IT che consente alle PA italiane di censire i Procedimenti amministrativi di interesse ed associarli ai Requirement definiti a livello europeo.
    - **Evidence Broker**
      Componente applicativo dell'infrastruttura SDG IT che fornisce i dati relativi ai Requirement e alle liste di Evidence Type definite a livello europeo.
    - **Data Service Directory**
      Componente applicativo dell'infrastruttura SDG IT che fornisce i dati relativi ai Data

Service offerti dagli Evidence Provider e i dati richiesti all'Utente transfrontaliero per il recupero della Evidence.

- **Architecture Common Services SDG IT**
  Componente applicativo dell'infrastruttura SDG IT che espone, ai Procedure Portal italiani e Data Service italiani, le API per generare l'URL che reindirizza l'Utente sul Preview Space SDG IT. Il componente consente inoltre l'interazione con l'Access point SDG IT per scambiare i messaggi SBD necessari ai processi OOTS.

- **Access Point**
  Componente applicativa che rende trasparente agli Enti Fruitori e agli Enti Erogatori, appartenenti a Stati Membri differenti, le scelte implementative, garantendo gli opportuni livelli di sicurezza nello scambio di dati cross-border. In attuazione dell'eDelivery AS4 Profile ([REF12 del TDD]), l'Italia ha adottato l'AP Domibus (Documentazione AP Domibus).

- **Preview Space SDG IT**
  Componente applicativo dell'infrastruttura SDG IT che permette all'Utente transfrontaliero di poter visualizzare l'anteprima della Evidence oggetto del Recupero.

Queste componenti cooperano al fine di esporre servizi da/per i Data Service italiani e i Procedure Portal italiani che offrono servizi *in scope* con i processi OOTS.

Nel confine logico indicato come "ITALIA", vengono rappresentati:

- la **Piattaforma Digitale Nazionale Dati** (PDND), l'infrastruttura nazionale che abilita l'interoperabilità dei sistemi informativi e delle banche dati degli Enti e dei gestori di servizi pubblici italiani;
- Un blocco logico **Procedure Portal IT** contenente, a titolo esemplificativo, i portali istituzionali delle PA attraverso i quali gli utenti portano avanti i procedimenti amministrativi di interesse;
- Un blocco logico **Data Service IT** contenente, a titolo esemplificativo, i data service italiani che forniscono prove ed informazioni necessarie per l'espletamento dei procedimenti amministrativi.

Il confine logico indicato come "ALTRI STATI MEMBRI", considerato non di interesse per questo documento in quanto rappresenta le componenti nazionali omologhe degli altri Stati Membri, è riportato sul documento solo per completezza di informazione e miglior riferimento al Technical Design Document (DC_01).

2.3 AUTENTICAZIONE E AUTORIZZAZIONE TRAMITE PDND

L'infrastruttura nazionale SDG ha aderito alla Piattaforma Digitale Nazionale Dati (PDND) e rende disponibili i propri servizi (c.d. "*e-services*") ad altri soggetti aderenti a tale piattaforma per consentire la fruizione di dati o l'integrazione tra i processi (cfr. **Error! Reference source not found.**).

Di fatto, nel contesto PDND, l'infrastruttura Componenti Nazionali SDG IT assume il ruolo di **Erogatore** dei servizi esposti ai Data Service delle PA italiane, i quali, a loro volta assumono il ruolo di **Fruitore**.

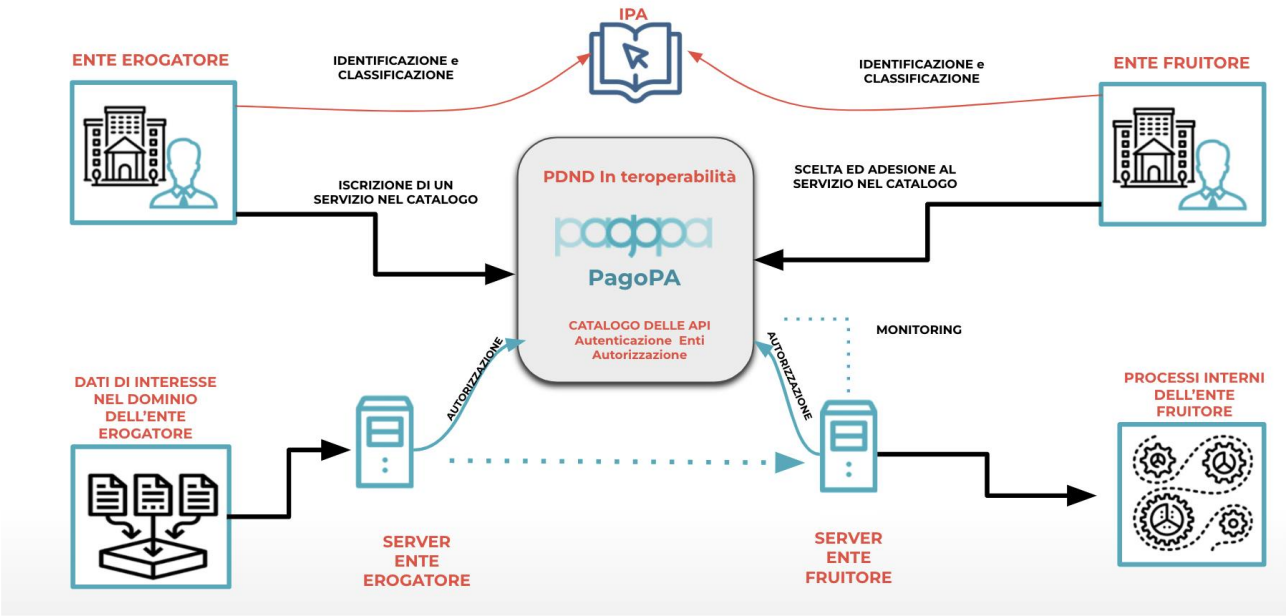

Figura 4 - Rappresentazione dei processi offerti dalla PDND

Come riportato nella Figura 4, la piattaforma PDND non si interpone nelle comunicazioni machine-to-machine tra Fruitore ed Erogatore, ma si occupa di autenticare e autorizzare il Fruitore tramite distribuzione di un *Authorization Token* OAuth 2.0.

La PDND, per ogni *e-service*, eroga al Fruitore il *token* di autorizzazione solo se:

- esiste una richiesta di fruizione del servizio in stato attivo;
- il Fruitore ha dichiarato le finalità di accesso associate alla richiesta di fruizione.

Il Fruitore dovrà passare all'Erogatore *l'access token* ricevuto dalla PDND in ogni chiamata effettuata verso l'*e-service* dell'Erogatore e quest'ultimo provvederà alla verifica del *token* tramite chiave pubblica.

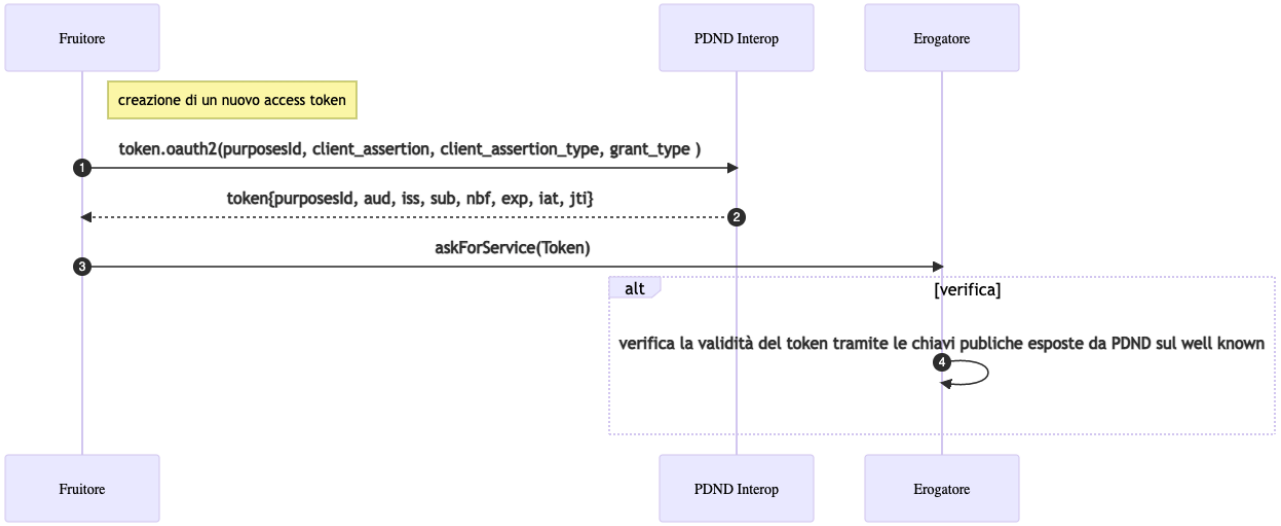

Figura 5 – Richiesta di un *access token* e fruizione del servizio

L'*Access Token* emesso dalla PDND consiste in un JWT conforme all'RFC7515, il suo utilizzo è obbligatorio per tutte le chiamate verso i servizi esposti dai Componenti Nazionali SDG IT.

La Figura 5, estratta dalla documentazione tecnica della PDND, modella il processo di Richiesta di un *access token* e la fruizione di un servizio.

2.4 INTERFACE AGREEMENT

Per consentire ai fruitori e agli erogatori di servizi italiani di interagire con le Componenti nazionali del SDG sono stati redatti e distribuiti a tutti i soggetti coinvolti due documenti contenenti le specifiche tecniche di interfaccia.

I documenti contengono la descrizione della soluzione implementata per l'Italia e le specifiche per l'utilizzo delle API che servono i processi in *scope* rispettivamente per le Pubbliche Amministrazioni:

- titolari dei Procedimenti Amministrativi che implementano i Procedure Portal (riferimento al *documento AGID_SDG_CdC_Specifiche di integrazione Procedure Portal_v.x.x.x*)
- responsabili per l'erogazione di prove che soddisfano i requisiti OOTS e che implementano i Data Services (riferimento al *documento AGID_SDG_CdC_Specifiche di integrazione Data Services_v.x.x.x*)

Per la condivisione in tempo reale della documentazione è stato predisposto un repository pubblico GitHub "*SDG – Componenti Nazionali*" (cfr. DC_03) sul quale saranno sempre disponibili le specifiche di interfaccia aggiornate.

2.5 IDENTIFICAZIONE E AUTENTICAZIONE EIDAS

Il Regolamento di Esecuzione SDG, che definisce le specifiche tecniche e operative del sistema tecnico per lo scambio transfrontaliero automatizzato di prove e l'applicazione del principio «*once only*» a norma del Regolamento SDG del Parlamento europeo e del Consiglio, considera il sistema di autenticazione dei nodi eIDAS, previsto dal Regolamento di Esecuzione eIDAS[1], una valida soluzione tra quelle riutilizzabili sviluppate a livello di Unione.

In particolare, la Commissione ritiene che l'autenticazione basata su nodi eIDAS consenta di elaborare la richiesta e la fornitura di un'autenticazione transfrontaliera di un utente. I nodi eIDAS dovrebbero consentire l'autenticazione degli utenti che accedono a servizi digitali previsti dal progetto SDG, erogati da pubbliche amministrazioni, secondo il principio *once only*.

Il Regolamento eIDAS sull'identità digitale, infatti, ha fornito una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri nonché una base normativa comune per interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni.

Considerando che le Pubbliche Amministrazioni italiane nella quasi totalità dei casi utilizzano come chiave primaria di accesso ai propri servizi il Codice Fiscale dell'utente, si è ritenuto di utilizzare tale codice quale dato aggiuntivo rispetto a quelli acquisiti con l'autenticazione eIDAS, ove ritenuto necessario dalla PA competente di un determinato procedimento amministrativo. Tale previsione è opzionale per la PA che eroga il procedimento amministrativo ed è consentita dall'articolo 16 del Regolamento di Esecuzione, che prevede l'acquisizione di dati ulteriori al fine di facilitare, ove necessario, il processo di identificazione dell'utente.
A tale scopo, è stato predisposto un servizio denominato "*verifica CF"* messo a disposizione dall'Agenzia delle Entrate ed esposto tramite API sulla Piattaforma Digitale Nazionale Dati (PDND), in coerenza con la strategia nazionale di interoperabilità. Nel fornire tale servizio, AdE si limita a verificare la sola corrispondenza dei dati dell'utente (in parte acquisiti dal nodo eIDAS, in parte dichiarati dall'utente stesso) con quelli censiti da AdE stessa sull'Anagrafe Tributaria al momento dell'interrogazione, come di seguito specificato.
L'identificazione degli utenti rimane a carico degli Identity Provider del Paese d'origine che colloquiano con il nodo eIDAS per consentire l'autenticazione degli utenti secondo il livello di garanzia dei mezzi di identificazione elettronica previsto dall'Erogatore della singola procedura richiesta.

La PA richiedente invoca il servizio di *verifica CF tramite la PDND.* Il servizio è disponibile in modalità "base" e in modalità "avanzata".

Il "servizio base" di *verifica CF* prevede la raccolta dei dati che seguono:

1. Nome

[1] *Regolamento di esecuzione (UE) 2015/1501 della Commissione, dell'8 settembre 2015, relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (GU L 235 del 9.9.2015, pag. 1)*

2. Cognome
3. Data di nascita
4. Codice Fiscale
5. Genere
6. Nazione di nascita

I primi tre rappresentano gli attributi afferenti al dataset minimo di eIDAS e vengono acquisiti automaticamente al momento dell'autenticazione tramite eIDAS; i restanti tre sono necessari per verificare la corrispondenza univoca tra il codice fiscale dichiarato dall'utente e quello eventualmente presente in Anagrafe Tributaria dell'AdE al momento dell'interrogazione e sono inseriti dall'utente in una interfaccia predisposta dalla PA che deve erogare la procedura.

Il servizio di *verifica CF* di AdE restituirà un OK in caso di corrispondenza dei 6 dati sopra definiti con quelli in possesso dell'Anagrafe Tributaria di AdE, oppure un KO in caso di: mancanza di corrispondenza; inesistenza del CF dichiarato dall'utente; omocodia.

L'Amministrazione che ha proceduto all'invocazione del servizio di *verifica CF*, che riceva un OK da parte di AdE, relativamente alla verifica del CF, può decidere di consentire all'utente di proseguire con l'erogazione del servizio prescelto.

Sarà inoltre disponibile un "servizio avanzato di verifica CF" che, oltre ai dati sopra citati, chiede all'utente di inserire informazioni rilasciate al possessore della Tessera Codice Fiscale:

7. il numero identificativo del Tesserino CF oppure
8. il numero identificativo del certificato di attribuzione del CF, acquisito nel processo di rilascio del certificato presso un qualunque Consolato, come mostrato in Figura 6 .

Figura 1 – Tessera del codice fiscale

Figura 2 – Certificato dell'Agenzia delle Entrate

Figura 6 – Esempio di Tesserino CF e di Certificato di Attribuzione CF

Anche in questo caso, il servizio di *verifica CF avanzato* di AdE restituirà un OK in caso di corrispondenza univoca dei dati con quelli eventualmente in possesso dell'Anagrafe Tributaria di AdE unitamente a quelli eventualmente presenti nella banca dati ove AdE censisce il Numero-

Identificativo-Tessera-CF o Numero-identificativo-certificato-CF, oppure un KO qualora non sia possibile verificare univocamente la corrispondenza tra tutti i dati oppure la verifica abbia avuto esito negativo.

Tale soluzione tecnica tiene conto di quanto segue:

1. il Regolamento SDG e gli atti di esecuzioni da esso derivati, tra cui il Regolamento di Esecuzione SDG, sono diventati vincolanti automaticamente in tutta l'UE alla data della loro entrata in vigore;

2. il Regolamento eIDAS e, in particolare, il principio di riconoscimento reciproco di cui all'articolo 6 del Regolamento, vincola le Pubbliche Amministrazioni a identificare i cittadini degli Stati Membri mediante gli strumenti di autenticazione transfrontaliera per l'accesso ai servizi online. Il livello di sicurezza richiesto dalla PA che implementa l'autenticazione eIDAS è indicato dalla stessa nell'invocazione del servizio "*authentication request*". Qualora il livello minimo richiesto dalla PA non possa essere garantito, l'utente transfrontaliero non è autorizzato a proseguire con l'espletamento del servizio richiesto (*cfr. per dettagli pag. 6 sub C e sez. 2.2. "L'Architettura"*).

3. a norma dell'articolo 42, paragrafo 1, del Regolamento SDG, la Commissione ha ricevuto il parere positivo del Garante europeo della protezione dei dati, che ha formulato le proprie osservazioni sul Regolamento di Esecuzione il 6 maggio 2021.

In ogni caso le Pubbliche Amministrazioni, ove lo ritengano necessario, sono libere di adottare ulteriori misure tecniche per la mitigazione del rischio di omonimia e/o omocodia nella fase di autenticazione dell'utente. L'EU, nella definizione Regolamento di esecuzione OOTS, identifica (art.2 comma e) i nodi eIDAS quali strumenti per l'autenticazione degli utenti e determinazione della corrispondenza dell'identità. Le PA che ritengano di elevare il livello di sicurezza assicurato dall'autenticazione eIDAS possono, liberamente, implementare ulteriori misure di sicurezza.

3 LE INDICAZIONI PER LE PA

Si riportano di seguito una serie di indicazioni rivolte alle Pubbliche Amministrazioni che gestiscono i portali ed i data service.

3.1 ENTI FRUITORI – GESTORI DEI PORTALI

I gestori dei portali istituzionali dovranno provvedere ad assicurare:

- **Registrazione dei Portali**: censimento dei metadati relativi ai casi d'uso e dei portali resi disponibili agli utenti finali, per il popolamento della base di conoscenza del *Catalogo dei Servizi IT;*

- **Definizione Tipologie di Prova (Evidence Type)**: Le Amministrazioni cui competono i portali e le amministrazioni che forniscono le prove partecipano alla definizione delle tipologie di prova richieste dalle procedure italiane e dei criteri di equivalenza con le tipologie rese disponibili in altri stati membri;

- **Adesione a PDND**: le Amministrazioni competenti le procedure indicate nell'allegato 2 della SDGR ed il gestore dell'Access Point aderiscono alla PDND secondo le linee guida emanate da AgID per garantire l'interoperabilità tra i loro sistemi;

- **Autenticazione e verifica CF**: i portali delle PA competenti assicurano l'autenticazione degli utenti dotati di eID rilasciate da uno stato membro conforme al Regolamento *eIDAS* e utilizzano il servizio di *verifica CF* se necessario;

- **Integrazione con i servizi OOTS**: integrazione dell'OnLine Procedure Portal con i servizi tecnologici di interoperabilità centralizzati ITA (Evidence Broker, Data Service Directory, Architectural Common Services) per il recupero dei riferimenti del data service, la richiesta ed il recupero delle prove;

- **Integrazione con i Preview Space**: integrazione dell'OnLine Procedure Portal con i servizi di Evidence Preview messi a disposizione dai diversi strati membri, sui singoli provider e centralizzati;

- **Caricamento autocertificazione**: Nel caso in cui l'utente scelga di non usare l'OOTS, il portale dovrà consentire il caricamento di un'autocertificazione;

- **Notifica elettronica**: Dopo la fase istruttoria, l'utente sarà informato sull'esito della procedura tramite una notifica elettronica.

3.2 ENTI EROGATORI – GESTORI DEI DATA SERVICE

I gestori dei Data Services dovranno provvedere ad assicurare:

- **Criteri di equivalenza tra tipologie - Catalogo dei Servizi IT**: le Amministrazioni che gestiscono i *data service* che erogano le prove definiscono i criteri di equivalenza tra tipologie di prove italiane e degli altri stati Membri;

- **Requisiti per Tipologie di Prova fornite**: le Amministrazioni competenti prendono in carico l'erogazione di un *Evidence Type* e individuano il livello di autenticazione previsto chiedendo eventuali informazioni aggiuntive, necessarie per il reperimento della prova stessa. Come sopra già espresso, il Regolamento di Esecuzione SDG consente all'art.16 di acquisire ulteriori dati, successivamente all'autenticazione eIDAS, al fine di facilitare l'identificazione dell'utente, ove necessario.

- **Adesione a PDND**: Il gestore dell'Access Point e gli Enti Erogatori italiani aderiscono alla PDND secondo le linee guida emanate da AgID per garantire l'interoperabilità tra i loro sistemi;

- **Evidence Query Service**: le Amministrazioni che forniscono le prove implementano un *Evidence Query Service* come indicato nelle specifiche di SDG ed in conformità al MoDI per esporre le tipologie di prova di propria competenza e registrano le stesse API sul Catalogo API della piattaforma PDND;

- **Metadati/Schemi dati**: le Amministrazioni che forniscono le prove provvedono alla registrazione sul Catalogo Nazionale Dati/SDG Semantic Repository IT dei metadati e degli schemi dati delle prove di propria competenza;

- **Multilingual Standard Form**: Regolamento applicato ad alcuni documenti pubblici rilasciati dalle Amministrazioni degli Stati Membri. Introduce un form standard multilingue: ausilio alla traduzione dei documenti in lingua non accettata da uno Stato Membro.

3.3 DESIGNAZIONE DEL RESPONSABILE AL TRATTAMENTO DEI DATI

Le Pubbliche Amministrazioni aderenti al Single Digital Gateway in qualità di titolari di procedimenti amministrativi e/o responsabili dell'erogazione di prove, dovranno redigere un atto di nomina che designa AgID quale responsabile al trattamento dei dati utilizzando l'apposito template, fornito dalla Commissione Europea, disponibile sul repository pubblico che accoglie la documentazione di progetto (DC_03 nella cartella *Trattamento Dati*).
Il template opportunamente compilato e firmato dalla PA dovrà essere inviato ad AgID che firmerà per accettazione.

4 STORICO DELLE MODIFICHE AL DOCUMENTO (CHANGELOG)

Vers.	Data	Paragrafi modificati	Tipo modifica	Descrizione modifica
1.0.0	28/09/2023	Tutti	Creazione	Creazione del documento