



Modello di interoperabilità per le Piattaforme di approvvigionamento digitale

*Allegato 1 al documento “Schema Operativo a supporto
della Certificazione delle Piattaforme di
approvvigionamento digitale”*

0	Servizio Procurement innovativo	/
Rev.	Elaborato	Approvato

REGISTRO DELLE MODIFICHE

Revisione	Data	Descrizione	Paragrafi modificati
0	11/09/2023	Bozza pubblicata per consultazione degli stakeholder	



Sommario

Introduzione	4
1. Riferimenti e sigle	6
1.1 Riferimenti Normativi.....	6
1.2 Linee guida, regole tecniche e documenti di riferimento.....	6
1.3 Termini e definizioni.....	7
2. Registro delle Piattaforme certificate	9
3. Il modello di interoperabilità	10
3.1 Principi generali.....	10
3.2 Fase 0: Adesione a PDND per la fruizione di e-service.....	10
3.3 Fase 1: Certificazione dei componenti di Piattaforma.....	11
3.4 Fase 2: Dichiarazione di Conformità.....	14
4. Attuazione del modello di interoperabilità	18
4.1 Architettura di alto livello.....	18
4.2 Contenuto del token addizionale.....	18
4.3 Piattaforme certificate.....	21
4.3.1 Composizione jws.....	21
4.3.2 Invocazione e-service della Piattaforma ANAC.....	21
4.3.3 Ricezione token PDND da parte di ANAC.....	21

Questo allegato è parte integrante al testo dello Schema Operativo a supporto della Certificazione delle Piattaforme di approvvigionamento digitale e viene aggiornato secondo quanto disposto al capitolo 6 dello stesso.

Draft

Introduzione

Come indicato nel nuovo Codice degli appalti, d.lgs. n.36 del 31 marzo 2023 (Codice), le Piattaforme di approvvigionamento digitale (Piattaforme) sono costituite dall'insieme dei servizi e dei sistemi informatici, interconnessi e interoperanti, utilizzati dalle stazioni appaltanti e dagli enti concedenti per svolgere una o più attività del ciclo di vita dei contratti pubblici ed assicurarne la piena digitalizzazione; a tal fine, interagiscono con i servizi della Banca dati nazionale dei contratti pubblici (BDNCP) nonché con i servizi della Piattaforma digitale nazionale dei dati (PDND).

Come previsto dal Codice l'AGID ha adottato con proprio provvedimento le Regole tecniche per tali Piattaforme che prevede i seguenti ruoli:

- il Titolare di Piattaforma, un soggetto giuridico, pubblico o privato, proprietario dei diritti, anche non esclusivi, di almeno un componente essenziale della Piattaforma, che mette a disposizione, anche mediante contratti, convenzioni/accordi, sviluppa e mantiene il software (direttamente o attraverso terzi dallo stesso incaricati) della Piattaforma, in modo conforme ai requisiti del Codice e delle Regole tecniche e lo sottopone a certificazione AGID ai sensi dell'art. 26, c. 2 del Codice;
- il Gestore di Piattaforma, un soggetto che gestisce per sé (se coincidente con una SA) o per conto terzi una o più Piattaforme. Più precisamente il Gestore è un soggetto giuridico, pubblico o privato, responsabile dell'esercizio di un'istanza di Piattaforma in conformità alle Regole tecniche, coincidente con una SA o dalla stessa incaricato, che ne garantisce il funzionamento, la sicurezza e la protezione dei dati personali. Il Gestore aderisce alla PDND per poter accedere agli e-service esposti da ANAC (v. paragrafo 3.2).

Come previsto dal Codice agli Artt. 21, 22, 23 e 24, la BDNCP rende disponibili mediante interoperabilità i servizi e le informazioni necessarie allo svolgimento delle fasi dell'intero ciclo di vita dei contratti pubblici; l'interoperabilità tra le banche dati e i servizi coinvolti è assicurata attraverso la PDND.

Le Piattaforme, che possono essere costituite da uno o più componenti software, permettono l'accesso agli e-service ANAC esposti in interoperabilità tramite la PDND e inviano dati e documenti relativi alla singola gara/appalto all'infrastruttura abilitante il ciclo di vita dei contratti pubblici ossia la BDNCP gestita da ANAC, costituita dalla Piattaforma Contratti Pubblici - PCP, dal Fascicolo Virtuale dell'Operatore Economico - FVOE, dal Casellario informatico dei Contratti Pubblici, dall'Anagrafe degli Operatori Economici e dall'Anagrafe Unica delle Stazioni Appaltanti - AUSA.

I Componenti delle Piattaforme interagiscono con gli e-service di ANAC tramite la PDND ma, per poter operare in questo ecosistema, devono essere sottoposti a cura del Titolare a certificazione AGID, secondo quanto stabilito nelle Regole tecniche. Ottenuto il certificato, sono censiti nella sezione dei Prodotti certificati del Registro delle piattaforme certificate, descritto nel cap. 2. Tale Registro è curato e gestito da ANAC, in conformità con quanto previsto dall'art. 26 comma 3 del Codice.

Ottenuta la certificazione, i Titolari comunicano ad AGID i riferimenti dei Gestori autorizzati ad usare ciascuno dei propri Componenti per consentire il popolamento della sezione dei Gestori autorizzati di tale Registro.

I Gestori predispongono le istanze di Piattaforma integrando uno o più componenti certificati, eseguono i test di integrazione per ciascuna istanza in ambiente di collaudo della PDND e, a seguito dell'esito positivo di tali test, rilasciano la Dichiarazione di conformità per ciascuna istanza di piattaforma e la trasmettono ad AGID. Le Piattaforme per cui sono state rilasciate le Dichiarazioni sono censite nell'apposita sezione del Registro e ne abilitano la messa in esercizio nell'ambiente di produzione della PDND.

AGID comunica ad ANAC le informazioni per il mantenimento del Registro.

I capitoli 3 e 4 del presente documento specificano il modello di interoperabilità e la sua implementazione, a supporto dell'attuazione dello Schema operativo.

1.1 Riferimenti Normativi

Sono riportati di seguito gli atti che compongono il quadro giuridico, di principale riferimento del presente documento.

- [CAD]** Decreto legislativo 7 marzo 2005, n. 82 recante “Codice dell’amministrazione digitale”.
- [Codice]** Decreto legislativo 31 marzo 2023, n. 36 “Codice dei contratti pubblici in attuazione dell’articolo 1 della legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici”.
- [eIDAS]** Regolamento (UE) n° 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
- [GDPR]** REGOLAMENTO (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

1.2 Linee guida, regole tecniche e documenti di riferimento

Di seguito sono elencati i documenti le Linee guida emesse da AGID ai sensi dell’art. 71 del CAD e altra documentazione regolamentare, che sono richiamate, anche indirettamente, nel presente documento. Le Linee guida AGID sono disponibili tramite il sito istituzionale al seguente indirizzo: <https://www.agid.gov.it/it/linee-guida>, dove sono pubblicati anche i relativi aggiornamenti in conseguenza dell’evoluzione tecnologica o della necessità di adeguamento alla normativa di riferimento.

- [Regole tecniche]** il documento “Requisiti tecnici e modalità di certificazione delle Piattaforme di approvvigionamento digitale” adottato dall’AGID ai sensi dell’art. 26 del Codice con Determinazione N. 137/2023 e disponibile all’indirizzo:

https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetti/2315113573700_ODt_approvazione+provvedimento+eprocurement_con_allegato_firmato.pdf).

- [LG_PDND_INTER]** Linee guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi delle basi dati
- [LG_SIC_INTER]** Linee Guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici
- [LG_INTER_TEC]** Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni
- [ModI]** Modello di Interoperabilità, disponibile all'indirizzo: <https://www.agid.gov.it/it/infrastrutture/sistema-pubblico-connettivita/il-nuovo-modello-interoperabilita>
- [MO_PDND]** Manuale Operativo della PDND Interoperabilità, disponibile all'indirizzo: <https://docs.pagopa.it/interoperabilita-1>
- [RT_SPID]** Regolamento recante Regole Tecniche di SPID e documentazione collegata, disponibile all'indirizzo: <https://www.agid.gov.it/it/piattaforme/spid>

1.3 Termini e definizioni

Di seguito si riportano gli ACRONIMI che verranno utilizzati nel presente documento:

- [PA]** Pubblica amministrazione.
- [SA]** Stazione appaltante e, ove applicabile in base al Codice, l'ente concedente.
- [OE]** Operatore economico.
- [BDNCP]** Banca dati nazionale dei contratti pubblici, di cui all'articolo 62-bis del CAD.
- [PDND]** Piattaforma digitale nazionale dei dati, di cui all'articolo 50-ter del CAD.
- [JSON]** JavaScript Object Notation.
- [jwt]** JSON Web Token.
- [jws]** jwt firmato con una Chiave Privata.
- [LoA]** Livello di garanzia (Level of Assurance) come definito dallo standard ISO/IEC 29115.

Nota: i livelli di garanzia dell'ISO/IEC 29115 si rapportano indicativamente a SPID come segue: LoA2 -> SPID-1, LoA3 -> SPID-2 o LoA4 -> SPID-3.

Ai fini del presente documento valgono le definizioni delle Regole tecniche (in particolare le definizioni di: Titolare, Gestore, Componente) e le seguenti:

- [Fruitore]** Aderente alla PDND che richiede l'accesso a un e-service.
- [Chiave pubblica]** In un cifrario a chiave pubblica, la chiave della coppia di chiavi di un'entità che è pubblica.
- [Chiave privata]** In un cifrario a chiave pubblica la chiave della coppia di chiavi di un'entità che è conosciuta solo da quell'entità.

2.

Registro delle Piattaforme certificate

Il Registro delle piattaforme certificate, gestito da ANAC, è composto da 3 sezioni:

- Componenti delle Piattaforme, certificati da AGID. Contiene almeno un identificativo del componente e la sua versione.
- I Gestori autorizzati: ogni Titolare di uno o più componenti di Piattaforma deve dichiarare ad AGID, per ogni componente, la versione e i riferimenti dei Gestori cui è stato fornito.
- Le Istanze di Piattaforma per cui il relativo Gestore ha rilasciato la dichiarazione di conformità, che contiene almeno un identificativo della piattaforma e la sua versione.

Le informazioni necessarie per popolare il Registro delle piattaforme sono comunicate da AGID ad ANAC.

Tale Registro è strettamente coinvolto nell'assegnazione degli attributi certificati nell'ambito della PDND come indicato nelle sezioni successive.

Le informazioni sui componenti certificati e le piattaforme che hanno ottenuto la certificazione sono pubblicamente accessibili.

Il modello di interoperabilità

3.1 Principi generali

Quanto di seguito riportato, individua la soluzione tecnica per il soddisfacimento da parte delle Piattaforme dei “Requisiti di interoperabilità (Classe 3)” di cui al paragrafo 3.4 delle Regole tecniche di cui all’articolo 26, comma 1 del decreto legislativo 31 marzo 2023, n. 36 (in breve Regole tecniche).

Nello specifico, la soluzione tecnica individuata soddisfa i seguenti requisiti:

- certificazione funzionale dei componenti delle Piattaforme attraverso il “processo di certificazione” definito al capitolo 4 delle Regole tecniche a carico dei Titolari degli stessi;
- dichiarazione di conformità delle Piattaforme utilizzate dalle Stazione Appaltanti così come disciplinato al capitolo 5 delle Regole tecniche.

Il modello di interoperabilità tramite PDND per l’e-procurement è stato disegnato distinguendo le seguenti fasi elencate di seguito.

3.2 Fase 0: Adesione a PDND per la fruizione di e-service

L’adesione a PDND è un atto formale che un Gestore autorizzato deve sottoscrivere con PagoPA come indicato in MO_PDND. Di seguito sono elencati i principali passi per poter fruire di un e-service su PDND da parte di un fruitore:

- 1) Il Gestore autorizzato effettua l’Adesione su PDND:
 - a) Scelta del registro di riferimento:
 - i) il Gestore pubblico può scegliere se fare l’adesione su PDND in riferimento all’Indice PA (e quindi avere anche la possibilità di accedere ad e-service diversi da quelli per l’e-procurement) o perché presente nel Registro delle Piattaforme Certificate nella sezione Gestori autorizzati;

- ii) il Gestore privato, invece, potrà effettuare adesione se e solo se è presente nel Registro delle Piattaforme Certificate nella sezione Gestori autorizzati e potrà dunque accedere solo agli e-service di e-procurement.

Nota: la procedura di adesione per l'accesso agli e-service di e-procurement è attualmente in sviluppo.

- b) Designazione Rappresentanti Amministrativi.
c) Firma Accordo di Adesione da parte del Rappresentante Legale.
d) Upload Accordo Adesione firmato.
e) Designazione Operatori Tecnici e di Sicurezza.
- 2) Il Gestore, in qualità di Fruitore, configura il Client per l'interoperabilità:
- a) Creazione Client.
b) Upload di una chiave pubblica associata al client (la chiave privata deve essere mantenuta riservata e custodita in luogo sicuro dal Fruitore).
- 3) Richiesta di accesso e indicazione Finalità:
- a) Il Gestore, se presente nella sezione Gestori autorizzati del Registro delle piattaforme certificate, in qualità di Fruitore effettua richiesta di fruizione all'e-service esposto da ANAC.
b) Configurazione di una finalità per la fruizione.

3.3 Fase 1: Certificazione dei componenti di Piattaforma

In questa fase il Titolare di un componente di piattaforma, in occasione della prima certificazione o al rilascio una nuova versione software e, che risulta conforme ai requisiti di certificazione di Classe 2, deve completare la fase di certificazione superando i test relativi ai requisiti di interoperabilità (Classe 3).

Per questa attività il Titolare della piattaforma deve incaricare un Gestore (Gestore incaricato) che si farà carico di effettuare i test per i requisiti di classe 3 interagendo con gli e-service esposti da ANAC in ambiente di collaudo della PDND.

Mediante l'invio dell'istanza di certificazione il Titolare comunica ad AGID:

- Identificativo del componente da sottoporre a certificazione e relativa versione.
- La relativa checklist da cui risulta la conformità ai requisiti di Classe 2 e l'indicazione dei test individuati per dimostrare il soddisfacimento dei requisiti di Classe 3.
- I riferimenti del Gestore incaricato per l'esecuzione dei test di Classe 3.

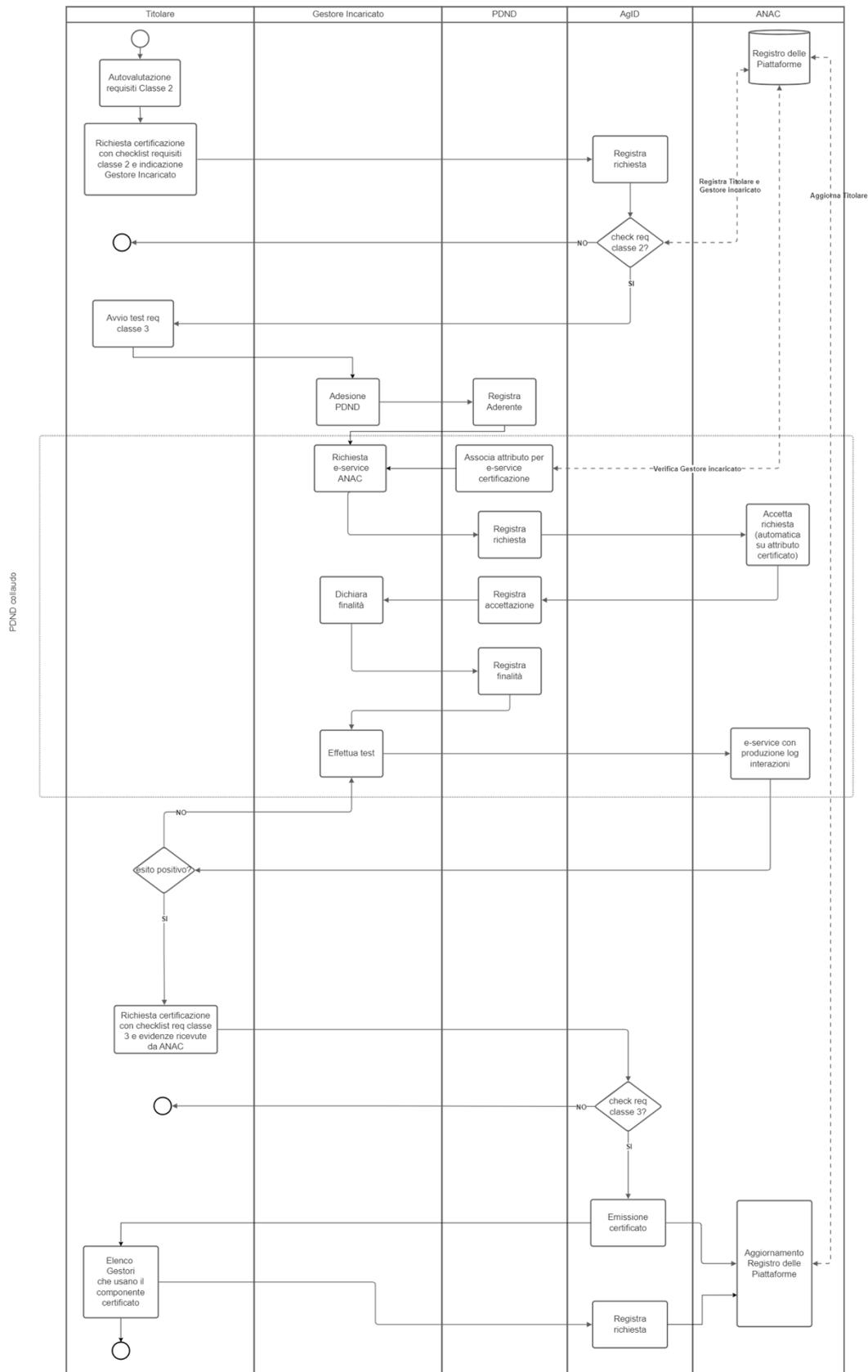
AGID trasmette ad ANAC le informazioni necessarie per l'aggiornamento delle sezioni Gestori autorizzati e Componenti delle Piattaforme del Registro delle piattaforme certificate indicando i riferimenti del Gestore incaricato e del componente, che risulterà nello stato “da certificare” quindi utilizzabile esclusivamente dal Gestore incaricato ai fini dell'esecuzione dei test di Classe 3. Se il Gestore incaricato non ha ancora aderito a PDND deve eseguire i passi indicati al paragrafo precedente (ed evidenziati anche nel diagramma che segue). Non appena il Gestore incaricato risulta inserito nella sezione Gestori autorizzati del Registro delle piattaforme certificate, PDND associa ad esso un attributo certificato (a titolo di esempio e-`proc_test_classe3`) tramite il quale il Gestore incaricato può chiamare gli e-services esposti da ANAC per completare il processo di certificazione relativamente ai requisiti di classe 3 delle Regole tecniche.

Ad esito positivo dei test, tramite gli e-service esposti da ANAC su PDND il Gestore incaricato deve ottenere il log delle interazioni. ANAC garantisce l'autenticità di tale log.

Il Gestore incaricato fornisce al Titolare tutte le informazioni per completare la checklist relativa ai requisiti di classe 3, incluso il log di cui al capoverso precedente, da inviare ad AGID per completare l'iter di certificazione, secondo quanto indicato al paragrafo 3.2 dello Schema operativo. Ad esito positivo, AGID trasmette ad ANAC le informazioni necessarie per l'aggiornamento dello stato del componente nella sezione Componenti di Piattaforma del Registro delle Piattaforme certificate.

Per poter attivare il processo di fase 2, ogni Titolare è tenuto ad effettuare una o più comunicazioni ad AGID con i riferimenti di tutti i Gestori che hanno in uso un proprio componente di piattaforma certificato e la relativa versione. AGID comunica anche queste informazioni, utilizzando gli appositi servizi di ANAC, per l'aggiornamento della sezione Gestori autorizzati del Registro delle piattaforme certificate.

Allegato 1 - Modello di interoperabilità per le Piattaforme di approvvigionamento digitale



3.4 Fase 2: Dichiarazione di Conformità

In questa fase un Gestore che ha creato un'istanza di Piattaforma, integrando uno o più componenti, ciascuno con una versione che è stata certificata, deve eseguire i test di integrazione, ed ottenere da ANAC il log relativo alla sessione test da allegare alla dichiarazione di conformità, che il Gestore rilascia a conferma dell'esecuzione dei test e per accedere agli e-service ANAC in ambiente di produzione.

Come conseguenza vengono effettuate le seguenti azioni:

- Viene aggiunta, in corrispondenza di ogni Gestore indicato dai Titolari, l'informazione relativa a quali componenti certificati utilizza. Il Registro annota per ogni istanza di piattaforma di ogni Gestore tutti i componenti certificati di cui è composta e la relativa versione;
- notifica a PDND che i componenti dell'istanza della piattaforma del Gestore sono certificati.
- PDND associa a quel Gestore un attributo certificato (a titolo di esempio `e-proc_test`) in modo da autorizzarlo ad usare gli e-service esposti da ANAC in ambiente di collaudo per il completamento della conformità dell'istanza di piattaforma.

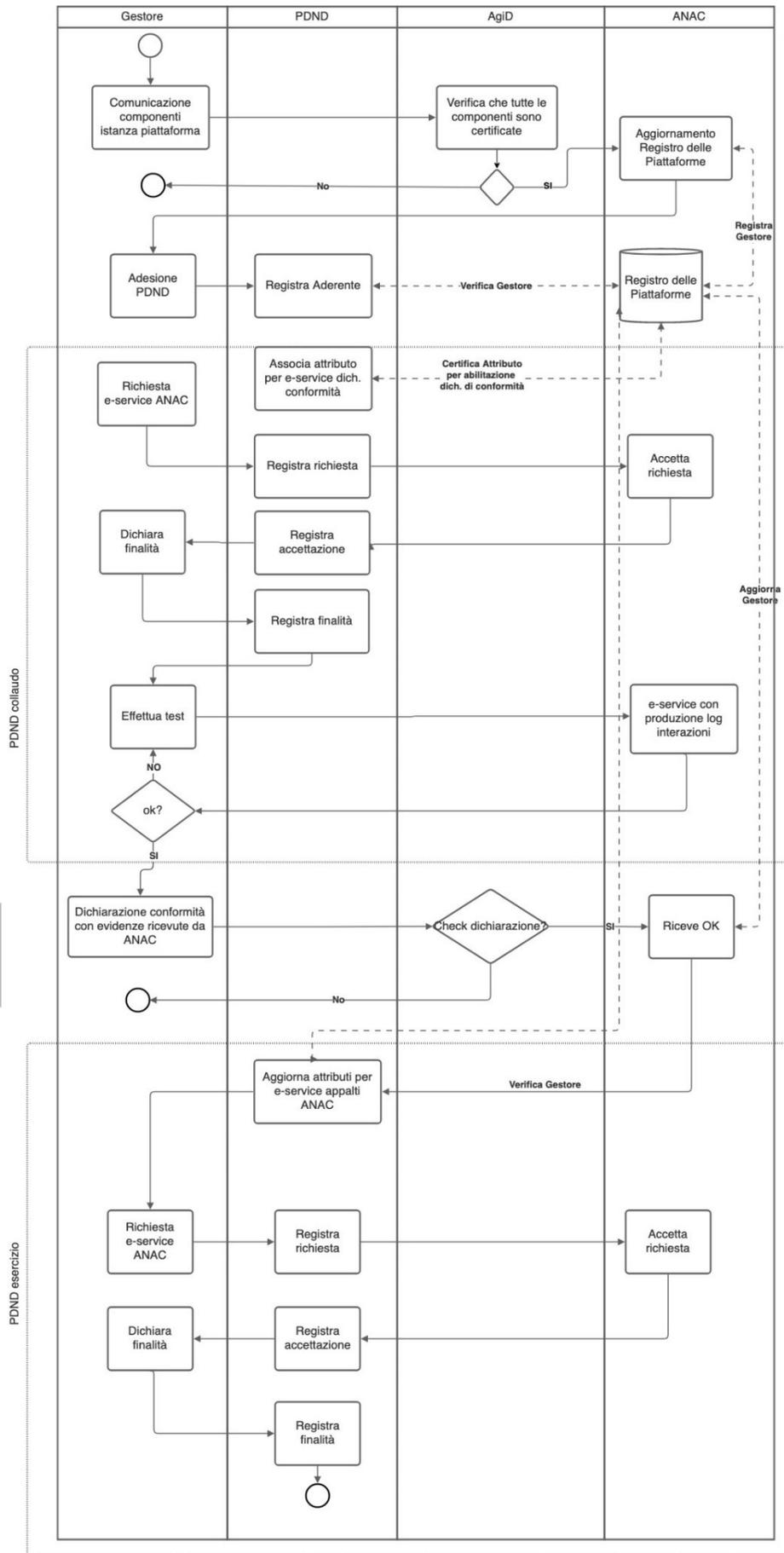
Il Gestore verifica che ogni componente, nella specifica versione utilizzata nella propria istanza di piattaforma e che interagisce con la PDND e gli e-service ANAC, risulta in possesso del certificato (tramite la procedura di fase 1).

Ad esito positivo dei test di integrazione dell'istanza di piattaforma ed effettuata la verifica di cui al capoverso precedente, il Gestore rilascia la Dichiarazione di conformità dell'istanza ai sensi del capitolo 5 delle Regole tecniche e la invia ad AGID allegando il log delle interazioni ottenuto da ANAC tramite e-service su PDND nel corso dell'esecuzione dei test di integrazione. ANAC garantisce l'autenticità di tale log.

AGID aggiorna la sezione delle istanze di piattaforma che hanno ottenuto la dichiarazione di conformità del Registro delle piattaforme certificate.

Per passare in produzione il Gestore riceve da PDND un nuovo attributo certificato (a titolo di esempio `e-proc`) che autorizza l'istanza di piattaforma ad usare la PDND di esercizio e utilizzare gli e-service di ANAC relativi agli appalti pubblici.

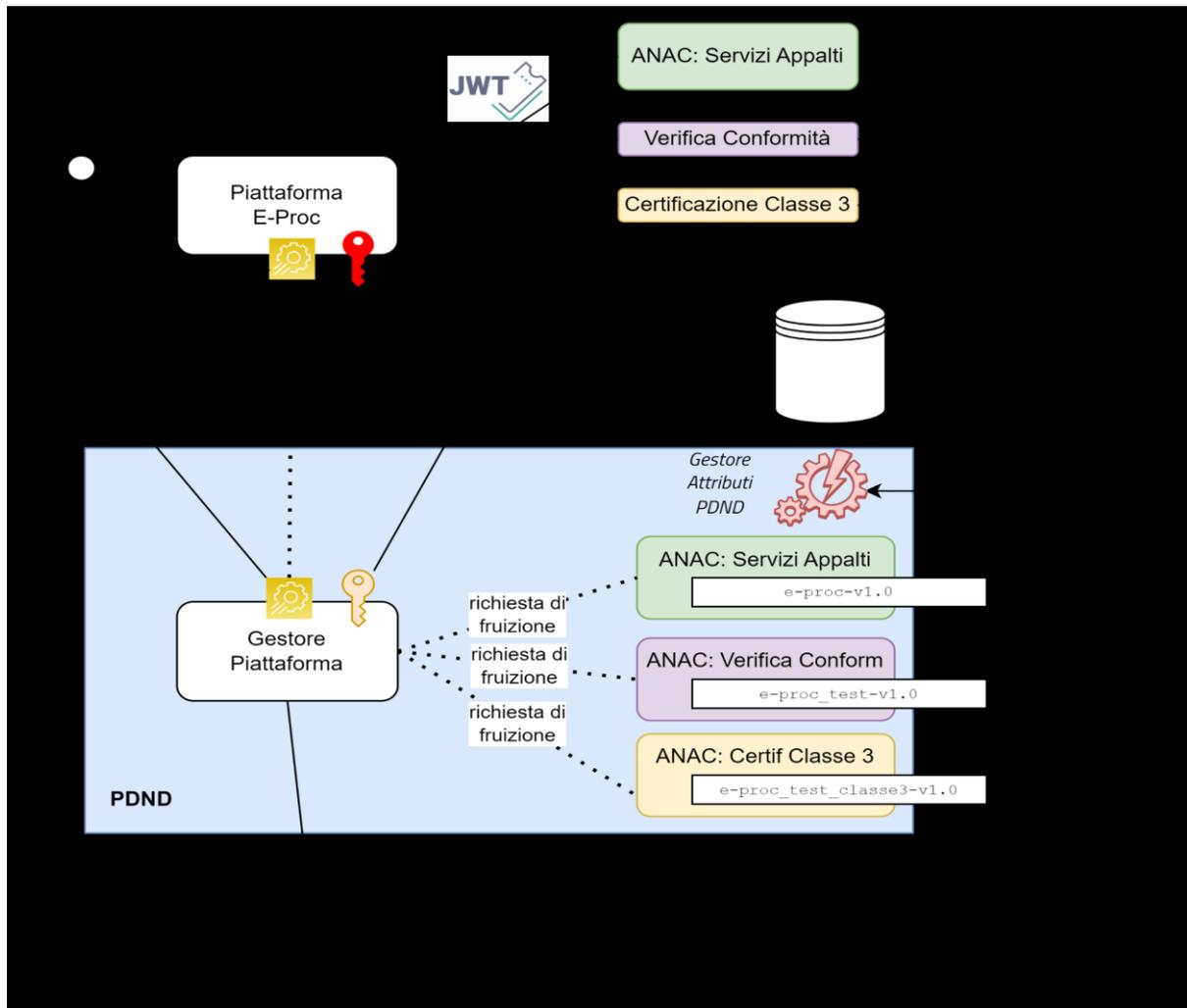
Allegato 1 - Modello di interoperabilità per le Piattaforme di approvvigionamento digitale



La definizione della soluzione tecnica riportata di seguito assume che:

- il Registro delle piattaforme certificate, mantenuto da ANAC, certifichi alla PDND:
 - i Titolari di componente certificato;
 - i Gestori autorizzati delle Piattaforme;
 - componenti di piattaforma che hanno superato i test relativi ai requisiti di Classe 3 (Fase 1);
 - istanza di piattaforma - composta da più componenti certificati - che ha superato il test d'integrazione e ottenuto la Dichiarazione di conformità;
- le Piattaforme, al momento dell'accesso agli e-service di ANAC, dichiarino la versione della stessa Piattaforma, la Stazione Appaltante operante, l'utente della stazione appaltante e il LoA utilizzato per l'autenticazione dello stesso applicando i pattern "Inoltro dati tracciati nel dominio del Fruitore" inclusi nel "Documento Operativo - Pattern sicurezza" delle "Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni";
- Tramite interrogazione del Registro i Gestori possono monitorare lo stato delle loro dichiarazioni di conformità, l'elenco dei componenti che costituiscono ogni istanza e il possesso di certificato.

Di seguito una schematizzazione del modello di interoperabilità:



Attuazione del modello di interoperabilità

4.1 Architettura di alto livello

L'architettura è basata sul pattern di interoperabilità [AUDIT REST 01](#) presente nelle Linee Guida di Interoperabilità ModI nella variante "TRUST GESTITO DA PDND".

Questo pattern prevede la possibilità di inserire delle informazioni aggiuntive in modo completamente trasparente alla PDND, tramite un token jws aggiuntivo. Tale token sarà firmato dalla Piattaforma utilizzando una chiave privata relativa al client registrato su PDND dal Gestore utilizzato dall'istanza della stessa. In questo modo PDND può certificare che queste informazioni siano state effettivamente inviate all'erogatore dal fruitore.

Ulteriori dettagli su questo pattern di sicurezza si possono trovare nell'allegato "Pattern di sicurezza" delle Linee Guida ModI.

4.2 Contenuto del token aggiuntivo

Il token aggiuntivo deve contenere almeno i seguenti gruppi di informazioni:

- Informazioni sull'utente della SA che sta inviando la richiesta, tra queste ci dovranno essere come minimo:
 - Codice Fiscale dell'utente che effettua l'accesso;
 - Modalità di autenticazione (SPID, CIE, eIDAS o Custom);
 - Livello di garanzia (LoA 3 o 4).

Se la Modalità di autenticazione è SPID o CIE il Livello di garanzia trasmesso è LoA 3 per SPID o CIE di livello 2, LoA 4 per SPID o CIE di livello 3.

Se la Modalità di autenticazione è eIDAS il Livello di garanzia trasmesso è LoA 3 per credenziali con livello di garanzia "significativo", LoA 4 per credenziali con livello di garanzia "elevato", con riferimento al regolamento eIDAS.

Se la Modalità di autenticazione è Custom il Livello di garanzia del meccanismo di identificazione utilizzato al momento dell'accesso nella sessione di lavoro corrente è definito dal Titolare (ed oggetto di certificazione AGID, si veda il

requisito [3.3.1.1-3] delle Regole tecniche); per poter procedere con la generazione del token addizionale, il meccanismo di identificazione deve avere un Livello di garanzia pari a LoA 3 o 4. Inoltre, deve essere verificata almeno una delle seguenti condizioni:

- a) l'utente si è identificato alla Piattaforma almeno una volta precedentemente alla sessione corrente con SPID di livello 2 o altro mezzo di identificazione elettronica eIDAS di livello "significativo", oppure
- b) l'utente si è identificato alla Piattaforma almeno una volta precedentemente alla sessione corrente con CIE o SPID di livello 3 o altro mezzo di identificazione elettronica eIDAS di livello "elevato".

Con riferimento ai due punti precedenti, la piattaforma deve mantenere nel profilo di ogni utente l'associazione col livello di garanzia più elevato con il quale tale utente si è identificato, ovvero se si è verificata la condizione a) ma non si è mai verificata la condizione b) il livello di garanzia associato al profilo dell'utente è pari a LoA 3 mentre se si è verificata almeno una volta la condizione b) tale livello è pari a LoA 4. Il Livello di garanzia trasmesso dalla Piattaforma e inserito nel token è il Livello di garanzia più basso tra quello associato all'utente e quello del meccanismo di autenticazione utilizzato al momento dell'accesso nella sessione di lavoro corrente. Ad esempio:

1. l'utente si è identificato alla Piattaforma almeno una volta precedentemente alla sessione corrente con SPID di livello 2 o altra credenziale eIDAS di livello "significativo" ma non si è mai identificato con un livello più elevato:
 - la piattaforma associa al profilo di quell'utente il Livello di garanzia LoA 3;
 - se la credenziale custom della piattaforma utilizzata dall'utente per identificarsi nella sessione di lavoro corrente è LoA 3, il LoA trasmesso è identico;
 - se la credenziale della piattaforma utilizzata dall'utente nella sessione corrente è LoA 4 il LoA trasmesso è LoA 3 non essendo stato mai stato identificato dalla piattaforma con LoA 4;

-
2. l'utente si è identificato alla Piattaforma almeno una volta precedentemente alla sessione corrente con SPID di livello 3 o CIE o altra credenziale eIDAS di livello "elevato":
 - la piattaforma associa al profilo di quell'utente che è stato identificato con "robustezza" avente LoA 4;
 - il LoA trasmesso nella sessione corrente è lo stesso della credenziale custom della piattaforma utilizzata dall'utente;
 3. l'utente non si è mai identificato alla Piattaforma con SPID di livello almeno 2 o con CIE o con altra credenziale eIDAS di livello almeno "significativo" oppure la credenziale utilizzata per identificarsi alla sessione di lavoro corrente è inferiore a LoA 3: non è possibile generare il token addizionale.
- Informazioni sulla SA per cui l'utente sta inviando la richiesta, tra queste ci dovranno essere come minimo:
 - Identificativo univoco della SA, corrispondente all'ID presente nella banca dati AUSA
 - Informazioni sulla Piattaforma tramite la quale la SA sta inviando la richiesta, tra queste ci dovranno essere come minimo:
 - identificativo univoco della Piattaforma di e-procurement;
 - la sua versione, così come indicato nel Registro delle Piattaforme certificate

```
AUDIT Token
-----
<< User Info (User) >>
      CF
Login_Type (Spid/CIE/Custom)
Login_LOA (1/2/3/Custom)
      ....
-----
<< SA Info (SA) >>
      SA_ID
      ....
-----
<< Platform Info (Platform) >>
      PF_ID
PF_Version
      ....
```

4.3 Piattaforme certificate

4.3.1 Composizione jws

Una volta recuperate le informazioni e una volta creato l'Audit token la piattaforma deve firmarlo per ottenere il jws relativo come indicato nel pattern AUDIT_REST_01 descritto nell'allegato "Pattern di sicurezza" delle Linee Guida ModI.

4.3.2 Invocazione e-service della Piattaforma ANAC

Una volta ottenuto il token jwt da PDND, la Piattaforma è pronta per invocare gli e-service esposti dalla Piattaforma di ANAC perché avrà ricevuto un attributo certificato che la autorizza, come descritto nei paragrafi precedenti.

La Piattaforma allega alla richiesta sia il token jws che quello jwt come descritto in ModI.

4.3.3 Ricezione token PDND da parte di ANAC

Alla chiamata di un e-service, la piattaforma ANAC deve richiedere a PDND la chiave pubblica della Piattaforma per validare l'Audit token.

Come verifica ulteriore la piattaforma ANAC deve controllare che la versione dell'istanza di Piattaforma che ha chiamato l'e-service è tra quelle per cui è stata rilasciata la Dichiarazione di conformità, in quanto un Gestore può rilasciare una o più versioni che mantengono la compatibilità con la stessa versione di e-service di ANAC. In questo caso l'istanza di piattaforma deve ripetere tutto il ciclo dei test indicato nei paragrafi precedenti ad ogni rilascio di nuova versione degli e-service ANAC, ma a livello di PDND mantiene gli stessi gli attributi certificati associati e quindi è in grado di procedere con l'utilizzo della nuova versione degli e-service ANAC se l'esecuzione dei test è andata a buon fine.

ANAC effettua un controllo sulla versione dell'istanza di Piattaforma sull'API Gateway punto di ingresso dei propri servizi e verifica che la versione dell'istanza della Piattaforma è effettivamente presente nel Registro delle Piattaforme Certificate.

Per ridurre il sovraccarico sull'API Gateway sono in fase di valutazione tecniche di ottimizzazione come, ad esempio, l'utilizzo di blacklist che rifiutano direttamente il jws, se già scartato in precedenza.