AGID | Agenzia per l'Italia Digitale

Modello di interoperabilità per le Piattaforme di approvvigionamento digitale

Allegato 1 al documento "Regole tecniche"

AGID | via Liszt, 21 – 00144 Roma | protocollo@pec.agid.gov.it | www.agid.gov.it | tel. 06 85264.1

Sommario

Questo allegato al documento "Regole tecniche" viene aggiornato direttamente dall'AGID, secondo quanto disposto al capitolo 8 delle suddette Regole tecniche.

.

Introduzione

Le Piattaforme di Approvvigionamento Digitale (PAD) 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 agli Artt. 21, 22, 23 e 24, la BDNCP rende disponibili mediante interoperabilità i servizi e le informazioni necessari 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. Per questo motivo ogni Gestore PAD deve aderire alla PDND.

Le PAD 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.

Il processo per ottenere la certificazione della PAD è a **carico del Gestore PAD** che, **preliminarmente** all'invio ad AGID della richiesta di certificazione deve avere svolto tutti i test e recuperato tutti i titoli previsti nelle Regole tecniche.

Il Registro della Piattaforma Certificate (RPC) è strettamente coinvolto nell'assegnazione degli attributi certificati nell'ambito della PDND quale fonte "autorizzativa" per ottenere l'accesso agli e-service di ANAC, sia in ambiente di collaudo che di esercizio.

In particolare il modello di interoperabilità prevede, tramite RPC, l'adesione alla PDND per lo svolgimento dei test in ambiente di collaudo PDND necessari all'ottenimento dei titoli di Classe 3[1] rilasciato da ANAC.

RPC consente inoltre il passaggio finale della PAD in ambiente di produzione PDND a seguito dell'ottenimento della certificazione.

In generale un Gestore può utilizzare anche Componenti PAD sviluppati da terzi e in tal caso deve verificare se tali Componenti PAD abbiano i titoli e i requisiti richiesti dalle Regole tecniche; in caso contrario debbono provvedere direttamente ad ottenerli prima di effettuare l'istanza di certificazione.

L'attestazione di ANAC circa il corretto svolgimento dei requisiti di Classe 3 è uno dei titoli richiesti dalle Regole tecniche. Pertanto i Componenti PAD che svolgono le funzioni di Classe 3, siano essi sviluppati da terzi o direttamente dai Gestori delle PAD, devono ottenere l'attestazione di ANAC per essere utilizzati dalle PAD.

I capitoli 3 e 4 del presente documento specificano il modello di interoperabilità e la sua implementazione affinché i Componenti PAD ottengano l'attestazione ANAC per i requisiti di Classe 3 e le PAD che hanno ottenuto la certificazione passino in ambiente di produzione.

Per le definizioni si fa riferimento alle Regole tecniche.

1 I titoli di Classe 3 riguardano infatti gli aspetti di interoperabilità della PAD e prevedono l'interazione con la BDNCP tramite la PDND

1. Riferimenti e sigle

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

Nell'Allegato 3 alle Regole tecniche sono elencati i documenti normativi, le Linee guida emesse da AGID e gli standard, che sono richiamati, anche indirettamente, nel presente allegato.

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 4 sezioni:

- Gestori PAD
- PAD certificate
- Soggetti interessati ad ottenere l'attestazione ANAC
- Componenti PAD che svolgono le funzioni dei requisiti di Classe3

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

Le informazioni pubblicamente accessibili tramite il RPC sono esclusivamente le PAD certificate e i relativi Gestori. Esse consentono a Stazioni Appaltanti ed Enti Concedenti di verificare lo stato di certificazione delle PAD.

Le altre informazioni sono funzionali all'implementazione del modello d'interoperabilità e consentono una continuità con l'attuale operatività.

3. Il modello di interoperabilità

3.1 Principi generali

Quanto di seguito riportato, individua la soluzione tecnica per:

- Lo svolgimento dei test per i requisiti di Classe 3 in ambiente di collaudo PDND;
- La messa in produzione delle PAD certificate in ambiente di esercizio PDND.

Il modello di interoperabilità tramite PDND per l'e-procurement è stato disegnato distinguendo le fasi descritte nei successivi paragrafi.

3.2 Fase 0 (ove necessario): Adesione a PDND per la fruizione di e-service

L'adesione a PDND è un atto formale compiuto da un soggetto interessato mediante sottoscrizione con PagoPA di un accordo, come indicato in MO_PDND.

Il Gestore PAD o il soggetto che deve ottenere l'attestazione ANAC di un Componente PAD agisce nel ruolo di Fruitore dell'e-service ANAC e, se non ha già aderito a PDND, deve procedere secondo i seguenti passi:

a) Scelta del registro di riferimento:
   i) Nel caso di soggetto pubblico può fare l'adesione su PDND in riferimento all'Indice PA.
   ii) nel caso di soggetto privato può fare l'adesione su PDND in riferimento al Registro Imprese.
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.

3.3 Fase 1: Ambiente di collaudo PDND

Questa fase consiste nell'abilitazione all'ambiente di collaudo PDND del Fruitore per ottenere l'attestazione ANAC per i test di Classe 3 di una PAD o di un Componente PAD. Ciò consiste nella possibilità per il Fruitore di eseguire i test di Classe 3 in ambiente di collaudo PDND.

Il Fruitore predispone ed invia ad AGID la richiesta per effettuare i test previsti per i requisiti di Classe 3 della PAD o del Componente PAD.

AGID trasmette ad ANAC le informazioni necessarie per l'inserimento del Fruitore nel Registro delle piattaforme certificate.

PDND associa al Fruitore un attributo certificato (a titolo di esempio `e-proc_test_classe 3`) in modo da autorizzarlo ad usare gli e-service esposti da ANAC in ambiente di collaudo.

3.3.1 Attività del Fruitore per il collaudo della PAD

La presente sezione descrive le fasi iniziali del processo di certificazione della PAD che prevedono la configurazione della PAD nel ruolo di "Client Fruitore PDND" degli e-service ANAC in ambiente di **collaudo PDND.**

- [3.3.1-1] Il Fruitore **deve:**
    - [3.3.1-1.1] effettuare la registrazione del "Client Fruitore PDND" in ambiente di **collaudo** PDND.
    - [3.3.1-1.2] compilare la finalità di accesso provvedendo all' "analisi del rischio sulla protezione dei dati personali" in ambiente di **collaudo** PDND (come definito al capitolo 6 delle [LG_PDND_ITER]) relativamente alla finalità di cui al comma 3 dell'articolo 23 del Codice;
    - [3.3.1-1.3] effettuare la richiesta di fruizione degli e-service ANAC in ambiente di **esercizio** PDND, nel ruolo di Fruitore (come definito ai paragrafi 4.5 e 7 [LG_PDND_ITER]) a tutti gli e-service ANAC;

A seguito dell'esecuzione positiva dei test, ANAC rilascia l'attestato di superamento dei test ed aggiorna in RPC lo stato della PAD o del Componente PAD in "Attestato ANAC OK".

3.4 Fase 2: Ambiente di esercizio PDND

Questa fase è riservata ai Gestori PAD che avviano formalmente il processo di certificazione, che consente il passaggio in produzione in ambiente di esercizio PDND.

Per l'ottenimento della certificazione della PAD i Gestori devono inviare ad AGID tutti i titoli necessari (compresa l'attestazione ANAC per i requisiti di Classe 3 ottenuta al superamento della Fase 1) secondo le indicazioni delle Regole tecniche.

Effettuate le necessarie verifiche AGID comunica ad ANAC le informazioni sul Gestore e sulla relativa PAD. ANAC procede ad inserire nelle rispettive sezioni del Registro delle piattaforme certificate il Gestore e la relativa PAD che sono così abilitati all'ambiente di produzione PDND.

Il Gestore riceve da PDND un nuovo attributo certificato (a titolo di esempio `e-proc`) che autorizza la PAD a fruire dei relativi e-service ANAC sulla PDND di esercizio.

3.4.1 Attività dei Gestori per l'esercizio della PAD

La presente sezione descrive le fasi conclusive del processo di certificazione della PAD che prevedono la configurazione della PAD nel ruolo di "Client Fruitore PDND" dei relativi e-service ANAC in ambiente di **esercizio PDND.**

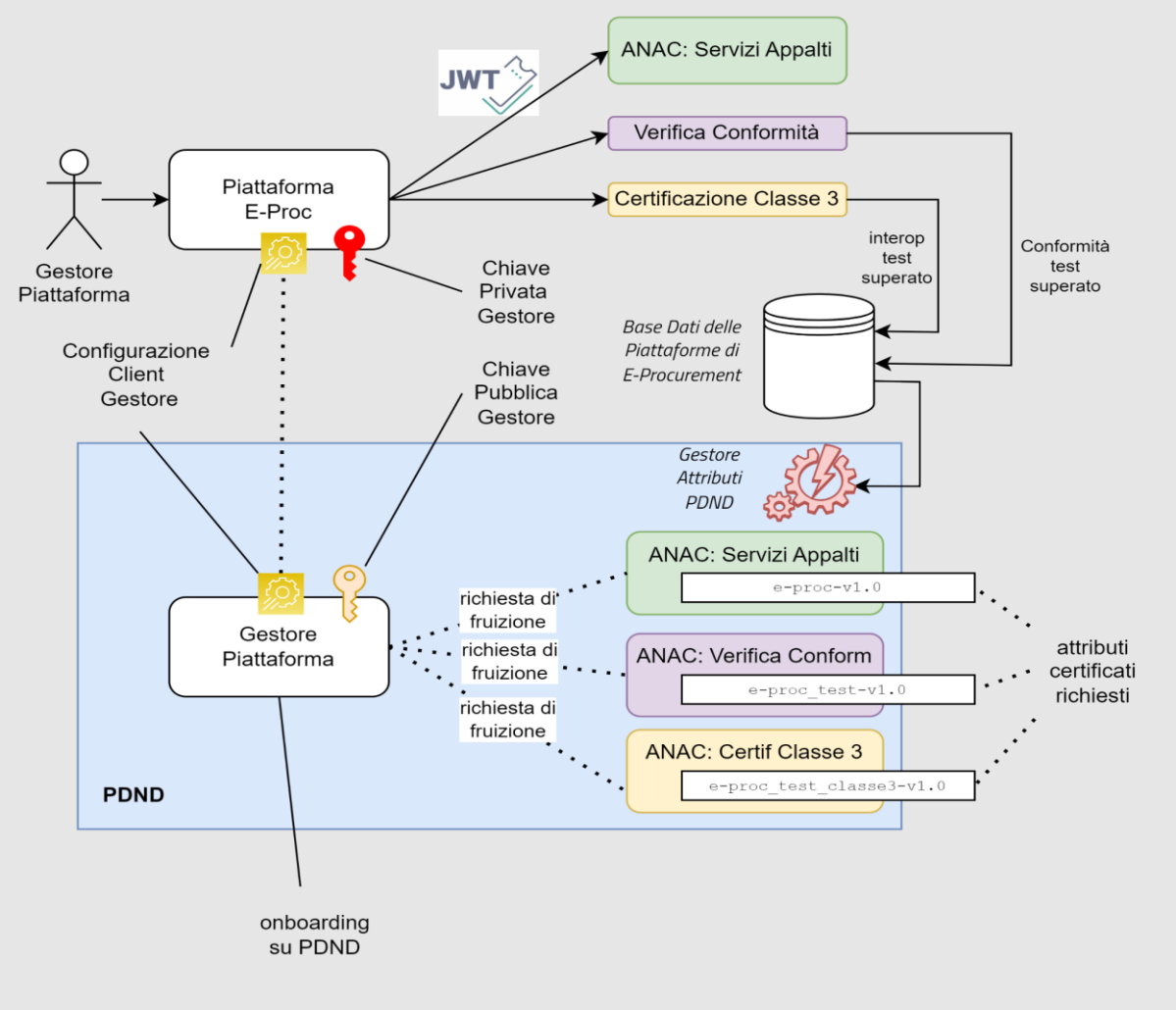
- [3.4.1-1] Il Gestore PAD **deve:**
    - [3.4.1-1.1] effettuare la registrazione della PAD come "Client Fruitore PDND" in ambiente di **esercizio** PDND.
    - [3.4.1-1.2] compilare la finalità di accesso provvedendo all' "analisi del rischio sulla protezione dei dati personali" in ambiente di **esercizio** PDND (come definito al capitolo 6 delle [LG_PDND_ITER]) relativamente alla finalità di cui al comma 3 dell'articolo 23 del Codice;
    - [3.4.1-1.3] effettuare la richiesta di fruizione degli e-service ANAC in ambiente di **esercizio** PDND, nel ruolo di Fruitore (come definito dalle [LG_PDND_ITER]) a tutti gli e-service che ANAC ha predisposto per le PAD;

Ne consegue che:

- il Registro delle piattaforme certificate, mantenuto da ANAC, è la fonte autoritativa per la PDND in relazione a:
    - i Gestori PAD;
    - le PAD certificate con relativa versione.

- le PAD, al momento dell'accesso agli e-service di ANAC, dichiarano la versione della stessa, 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 di sicurezza" delle "Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni".

Di seguito una schematizzazione del modello di interoperabilità:



4. 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 addizionale. Tale token sarà firmato dalla PAD utilizzando una chiave privata relativa al client registrato su PDND dal Gestore. In questo modo PDND può certificare che queste informazioni siano state effettivamente inviate dal fruitore all'erogatore.

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

4.2 Contenuto del token addizionale

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

- **[4.2-1] Informazioni sull'utente della SA** che sta inviando la richiesta, tra queste ci dovranno essere come minimo:
  - [4.2-1.1] Codice Fiscale dell'utente che effettua l'accesso;
  - [4.2-1.2] Modalità di autenticazione (SPID, CIE, eIDAS o Custom);
  - [4.2-1.3] Livello di garanzia (LoA 3 o LoA 4).
- [4.2-2] Il Livello di garanzia, che deve essere determinato come segue:
  - [4.2-2.1] Se la Modalità di autenticazione è SPID il Livello di garanzia trasmesso è LoA 3 per SPID di livello 2 oppure LoA 4 per SPID di livello 3.
  - [4.2-2.2] Se la Modalità di autenticazione è CIE il Livello di garanzia trasmesso è LoA 3 per CIE di livello 2 oppure LoA 4 per CIE di livello 3.
  - [4.2-2.3] Se la Modalità di autenticazione è conforme ad uno dei meccanismi previsti dal Regolamento eIDAS il Livello di garanzia

trasmesso è LoA 3 per credenziali con livello di garanzia "significativo" oppure LoA 4 per credenziali con livello di garanzia "elevato", compreso l'utilizzo di un Portafoglio europeo di identità digitale fornito da uno Stato membro UE secondo quanto previsto all'articolo 5-bis, paragrafo 1, del Regolamento eIDAS.

- [4.2-2.4] Se la modalità di autenticazione è Custom ed è stato classificato dal Gestore come LoA 3 (si veda il requisito [3.3.1.1-3] delle Regole tecniche) e l'utente si è identificato alla Piattaforma almeno una volta precedentemente alla sessione corrente con una qualsiasi delle modalità di cui ai punti [4.2-2.1], [4.2-2.2] o [4.2-2.3] il Livello di garanzia trasmesso è LoA 3.
- [4.2-2.5] Se la modalità di autenticazione è Custom ed è stato classificato dal Gestore come LoA 4 (si veda il requisito [3.3.1.1-3] delle Regole tecniche) e l'utente si è identificato alla Piattaforma almeno una volta precedentemente alla sessione corrente con una qualsiasi delle modalità di cui ai punti [4.2-2.1], [4.2-2.2] o [4.2-2.3] il Livello di garanzia trasmesso è lo stesso che è stato trasmesso durante tale precedente identificazione.

Con riferimento ai punti [4.2-2.4] e [4.2-2.5], la PAD deve mantenere nel profilo di ogni utente il livello di garanzia più elevato con il quale tale utente si è identificato con una delle modalità di cui ai punti [4.2-2.1], [4.2-2.2] o [4.2-2.3] negli ultimi 3 mesi, passati i quali la PAD deve richiedere nuovamente una identificazione secondo una di tali modalità.

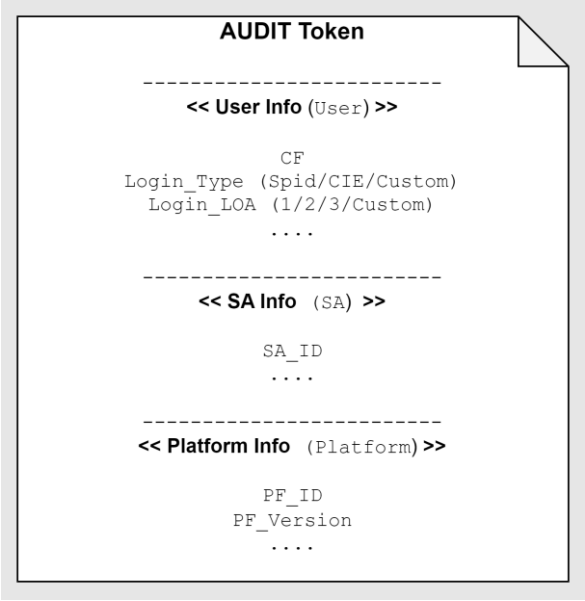
Esempi:

1. l'utente si è identificato alla PAD non oltre tre mesi dalla sessione corrente con SPID o CIE 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 oppure LoA 4, il LoA trasmesso è comunque LoA 3.
2. L'utente si è identificato alla piattaforma almeno una volta precedentemente alla sessione corrente con SPID o CIE di livello 3 o altra credenziale eIDAS di livello "elevato" da non oltre 3 mesi:

- la piattaforma associa al profilo di quell'utente il Livello di garanzia LoA 4;
- il LoA trasmesso nella sessione corrente è LoA 3 o LoA 4 a seconda di come è stata classificata dal Gestore la credenziale custom utilizzata dall'utente.

3. l'utente non si è mai identificato alla Piattaforma con SPID o con CIE o con altra credenziale eIDAS di livello almeno "significativo" o portafoglio di identificazione: non è possibile generare il token addizionale.

- **[4.2-3] 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.
- **[4.2-4] Informazioni sulla PAD** tramite la quale la SA sta inviando la richiesta, tra queste ci dovranno essere come minimo:
  - identificativo univoco della PAD;
  - la sua versione, così come indicato nel Registro delle Piattaforme certificate



4.3 Piattaforme certificate

4.3.1 Composizione jws

Una volta recuperate le informazioni e una volta creato l'Audit token, la PAD 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 PAD è pronta per invocare gli e-service esposti da ANAC perché avrà ricevuto un attributo certificato che la autorizza, come descritto nei paragrafi precedenti.

La PAD 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 PAD per validare l'Audit token.

Come verifica ulteriore la piattaforma ANAC deve controllare che la versione della PAD che ha chiamato l'e-service è tra quelle presenti nel Registro delle piattaforme certificate, in quanto un Gestore può rilasciare una o più versioni che mantengono la compatibilità con la stessa versione degli e-service di ANAC.

Ogni versione della PAD deve effettuare i test in ambiente di collaudo PDND per i requisiti di Classe 3 come 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 della PAD 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.