AGID
Agenzia per l'Italia Digitale

Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati

ai sensi dell'articolo 50-ter, comma 2 del CAD

ALLEGATO 3:

Standard e dettagli tecnici utilizzati per la fruizione dei Voucher di autorizzazione

Versione 1.0 del 10.12.2021

1 Introduzione

Il presente allegato individua gli standard e le tecnologie per l'emissione e fruizione dei **Voucher** di autorizzazione per l'utilizzo di un **e-service** e le modalità tecniche attuate dagli **Aderenti** per l'utilizzo degli stessi.

Il **Gestore** definisce la documentazione tecnica per attuare quanto disposto nel presente Allegato, considerando anche le linee guida emanate ai sensi dell'articolo 71 del **CAD** che hanno rilevanza per la realizzazione **Infrastruttura interoperabilità PDND.** La documentazione tecnica definita dal **Gestore** e resa disponibile agli **Aderenti** attraverso la pubblicazione sul portale della **Infrastruttura interoperabilità PDND.**

2 Riferimenti e sigle

2.1 Note di lettura del documento

Conformemente alle norme ISO/IEC Directives, Part 3 per la stesura dei documenti tecnici, le presenti **Linee Guida** utilizzeranno le parole chiave «DEVE», «DEVONO», «NON DEVE», «NON DEVONO», «DOVREBBE», «NON DOVREBBE», «PUÒ», «POSSONO» e «OPZIONALE», la cui interpretazione è descritta di seguito.

- **DEVE** o **DEVONO**, indicano un requisito obbligatorio per rispettare la linea guida;
- **NON DEVE** o **NON DEVONO** o **NON PUÒ** o **NON POSSONO**, indicano un assoluto divieto delle specifiche;
- **DOVREBBE** o **NON DOVREBBE**, indicano che le implicazioni devono essere comprese e attentamente pesate prima di scegliere approcci alternativi;
- **PUÒ** o **POSSONO** o l'aggettivo **OPZIONALE**, indica che il lettore può scegliere di applicare o meno senza alcun tipo di implicazione la specifica.

2.2 Standard di riferimento

Sono riportati di seguito gli standard tecnici indispensabili per l'applicazione delle presenti **Linee Guida**.

[X.509]	Standard per la crittografia asimmetrica definito in RFC5280[1]
[JWT]	JSON Web Token definito in RFC7519[2]

[1] https://tools.ietf.org/html/rfc5280

[2] https://tools.ietf.org/html/rfc7519

[JWT-BCP]	JWT Best Current Practices definito in RFC8725[3]
[JWK]	JSON Web Key (JWK) in RFC7517[4]
[JWT_PK]	JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants RFC7523[5]

2.3 Linee guida di primario riferimento

Di seguito sono elencate le linee guida emesse dall'**AgID** che verranno espressamente richiamate nelle presenti **Linee Guida**.

[LG INTEROPERABILITÀ TECNICA]	Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni
[LG SICUREZZA]	Linee Guida Tecnologie e standard per assicurare la sicurezza dell'interoperabilità tramite API dei sistemi informatici

[3] https://tools.ietf.org/html/rfc8725

[4] https://datatracker.ietf.org/doc/html/rfc7517

[5] https://tools.ietf.org/html/rfc7523

3 Trust degli Aderenti alla PDND

La **Infrastruttura Interoperabilità PDND** DEVE fornire agli **Aderenti** le funzionalità necessarie ad assicurare l'autenticazione e autorizzazione dei **Fruitori** al fine di accedere agli **e-service** messi a disposizione degli **Erogatori**.

L'identificazione degli **Aderenti,** assicurata dal Processo di adesione all'**Infrastruttura interoperabilità PDND,** determina un insieme definito di partecipanti ("sistema chiuso").

Si assume come prerequisito per la comunicazione tra **Erogatori** e **Fruitori** che:

- gli **Erogatori** DEVONO registrare sul **Catalogo API** gli **e-service** che mettono a disposizione dei **Fruitori** e i relativi **Requisiti di fruizione** che questi ultimi devono soddisfare per accedere agli **e-service**;
- il **Fruitore** DEVE chiedere all'**Erogatore** la fruizione di un suo **e-service** e compilare l'Analisi del rischio, ove indicherà le finalità per cui fruirà dell'**e-service.**

In merito alle modalità per assicurare i prerequisiti indicati in precedenza, si rimanda all'Allegato 2 delle **Linee guida**.

Il trust realizzato tra l'**Infrastruttura interoperabilità PDND** e gli **Aderenti** è fondato sul:

- materiale crittografico pubblico registrato sull'**Infrastruttura interoperabilità PDND** dai **Fruitori**;
- la certezza della fonte per la verifica del materiale crittografico realizzata dall'**Infrastruttura interoperabilità PDND**.

I **Fruitori** DEVONO registrare sulla **Infrastruttura interoperabilità PDND** i propri sistemi informatici (di seguito **Client Fruitore**) che fruiranno degli **e-service** pubblicati sul **Catalogo API** dagli **Erogatori**.

Fatta salva la necessità di registrare almeno un **Client Fruitore** per potere fruire degli **e-service** pubblicati sul **Catalogo API** dagli **Erogatori**, i **Fruitori** POSSONO registrare più **Client Fruitore** sull'**Infrastruttura interoperabilità PDND.**
Per ogni **Client Fruitore** DEVE essere associato il materiale crittografico generato dal **Fruitore** stesso.

Per garantire la continuità della fruizione in caso di aggiornamento degli algoritmi (si veda RFC7696 Algorithm Agility sezione 2.3) l'**Infrastruttura interoperabilità PDND** DEVE permettere di associare più istanze di materiale crittografico ai **Client Fruitore**.

I **Fruitori** relativamente al materiale crittografico associato ai **Client Fruitore** registrati sulla **Infrastruttura interoperabilità PDND** DEVONO assicurare i necessari aggiornamenti in caso di compromissione del materiale crittografico.

L'**Infrastruttura interoperabilità PDND** DEVE assicurare l'integrità e l'immodificabilità del materiale crittografico associato ai **Client Fruitore**.

Per ogni fruizione di un **e-service** basata su una determinata finalità individuata nell'Analisi del rischio, i **Fruitori** DEVONO associare i **Client Fruitore** che accederanno agli **e-service** per dare seguito alla specifica finalità. Un **Fruitore** PUÒ associare uno stesso **Client Fruitore** a più **e-service** e così anche per le relative finalità di fruizione.

L'**Infrastruttura interoperabilità PDND** DEVE realizzare la funzione di *Registry* per il materiale crittografico registrato dagli **Aderenti**.

La **Infrastruttura interoperabilità PDND** DEVE rendere disponibili agli **Utenti degli aderenti** le funzionalità per permettere agli:

- **Operatori Amministrativi** di registrare un **Client Fruitore** e associarlo ad un **Operatore Sicurezza**;
- **Operatori di Sicurezza** di registrare il materiale crittografico pubblico dei **Client Fruitore** a cui è associato.

L'**Infrastruttura interoperabilità PDND** DEVE tracciare le operazioni realizzate dagli **Utenti degli Aderenti** relative alla:

- registrazione dei **Client Fruitore**;
- associazione del materiale crittografico ai **Client Fruitore**;
- registrazione dei **Client Fruitore** che accedono agli **e-service**.

L'**Infrastruttura interoperabilità PDND** DEVE rendere accessibile il materiale crittografico pubblico registrato dagli **Aderenti.** L'accesso DEVE essere garantito tramite API REST conformi alle [LG

INTEROPERABILITÀ TECNICA] applicando il pattern sicurezza [ID_AUTH_CHANNEL_01] con l'utilizzo di certificati qualificati ai sensi del [eIDAS] e delle [LG SICUREZZA].

Gli **Erogatori** DEVONO utilizzare sui propri sistemi informatici che implementano gli **e-service** registrati sul **Catalogo API** certificati X.509, nel rispetto delle [LG SICUREZZA], per assicurare almeno l'applicazione del pattern di sicurezza [ID_AUTH_CHANNEL_01] individuato nelle [LG INTEROPERABILITÀ TECNICA]. Gli **Erogatori** si dotano dei suddetti certificati X.509 al di fuori della **Infrastruttura interoperabilità PDND.**

Sulla base della tipologia dei dati oggetto delle comunicazioni realizzate per il tramite degli **e-service** messi a disposizione dei **Fruitori,** gli Erogatori DEVONO individuare gli opportuni pattern e profili previsti nelle [LG INTEROPERABILITÀ TECNICA].

4 Materiale crittografico

I **Fruitori** tramite le funzionalità della **Infrastruttura interoperabilità PDND** associano ad ognuno dei propri **Client Fruitore** il materiale crittografico.

Il materiale crittografico generato nel dominio dei **Fruitori** DEVE rispettare quanto indicato dal **Gestore** nella documentazione tecnica predisposta dallo stesso per attuare quanto disposto nel presente Allegato, posto che:

- il materiale crittografico deve rispettare le "Raccomandazioni in merito agli algoritmi per XML Canonicalization, Digest and signature public key SOAP e Digest and signature public key REST" previste dalle [LG SICUREZZA];
- il materiale crittografico NON DEVE essere utilizzato con algoritmi di Message Authentication Code (MAC);
- il materiale crittografico associato ai **Client Fruitore** NON DEVE mai contenere chiavi private;
- la **Infrastruttura interoperabilità PDND** pubblica il materiale crittografico in formato [JWK] RFC7517 Sezione 5 tramite API REST conformi alle [LG INTEROPERABILITÀ TECNICA];
- la **Infrastruttura interoperabilità PDND** genera ed associa un identificativo univoco al materiale crittografico registrato dai **Fruitori**;
- i **Fruitori** NON POSSONO modificare l'identificativo univoco generato dalla **Infrastruttura interoperabilità PDND**.

La **Infrastruttura interoperabilità PDND** NON DEVE permettere di associare uno specifico materiale crittografico a più **Client Fruitore**.

La **Infrastruttura interoperabilità PDND** in caso di variazione del materiale crittografico di un **Client Fruitore** DEVE notificare la circostanza agli **Erogatori** degli **e-service** fruiti dallo stesso **Client Fruitore** e per cui è abilitata l'opzione "Voucher PoP".

5 Protocollo di emissione dei Voucher con API REST

L'**Infrastruttura interoperabilità PDND** DEVE assicurare l'emissione dei **Voucher** utilizzati dai **Fruitori** per accedere agli e-service degli **Erogatori** rendendo disponibile agli stessi delle API REST conformi alle [LG INTEROPERABILITÀ TECNICA].

I profili di emissione dei **Voucher** sono definiti come applicazione del RFC6749, assumendo che i **Voucher** sono gli **Access Token** indicati nell'RFC, prevedendo la seguente mappatura dei ruoli:

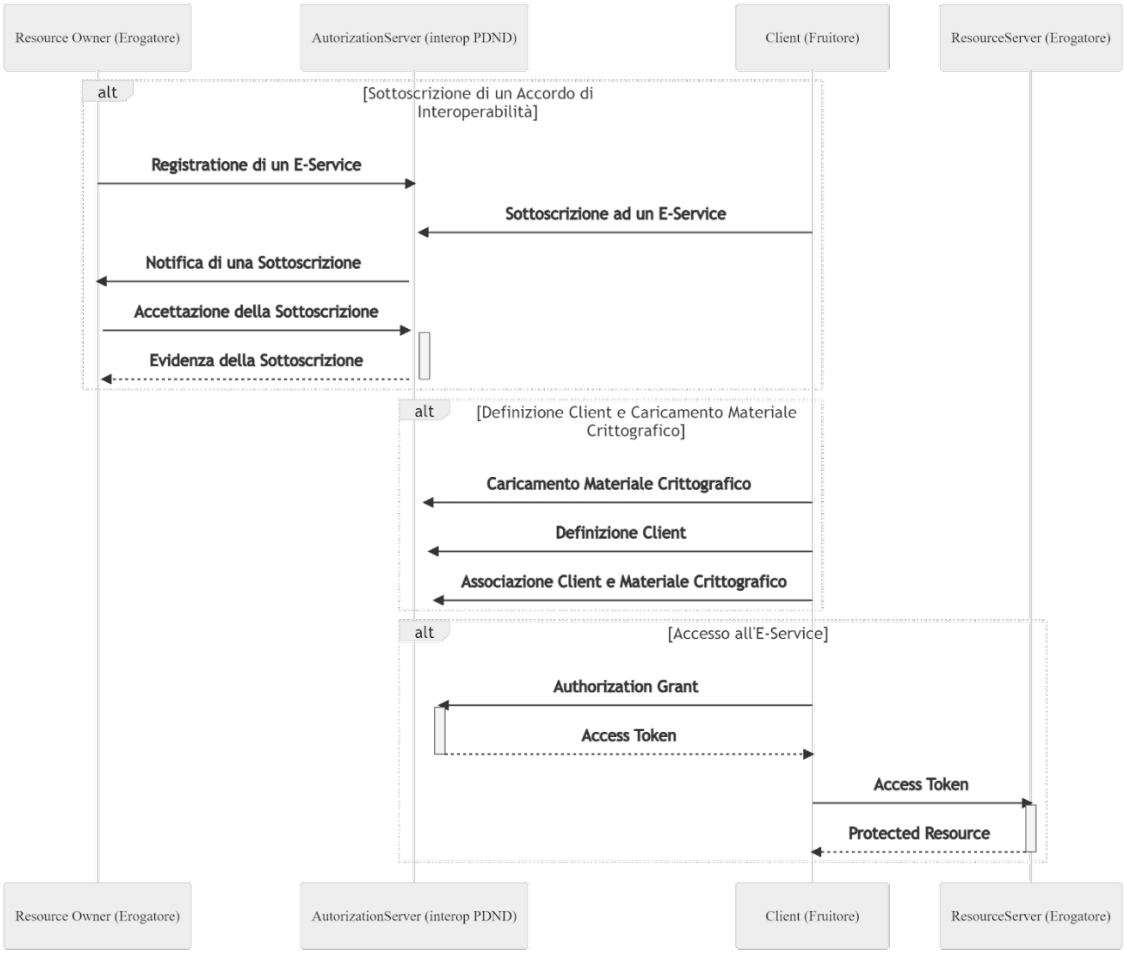
- *Resource Owner*: corrisponde all'**Erogatore** che, tramite le funzionalità della **Infrastruttura interoperabilità PDND** per la definizione dei **Requisiti di fruizione** degli **e-service**, individua le policy di accesso ai propri e-service;
- *Resource Server*: è il sistema informatico dell'**Erogatore** che rende disponibile l'**e-service**;
- *Client*: corrisponde al sistema informatico (di seguito **Client Fruitore**) del **Fruitore** che, a valle della richiesta di fruizione dell'**e-service**, dell'indicazione delle finalità espresse con l'Analisi del rischio e dell'autorizzazione alla fruizione dell'**e-service da parte dell'Erogatore,** accede all'**e-service** erogato dal *Resource Server*;
- *Authorization Server*: corrisponde alla componente dell'**Infrastruttura interoperabilità PDND** che emette gli **Access Token** per autorizzare l'accesso agli **e-service** degli **Erogatori**.

I passi previsti nel flusso base indicato in RFC6749 trovano la corrispondenza indicata di seguito.

- L'Authorization request e il rilascio dell'Authorization Grant è assicurato tramite la richiesta di fruizione dell'**e-service** da parte del **Fruitore** e alla successiva conferma di accettazione da parte dell'**Erogatore.** Il processo è realizzato per il tramite dell'**Infrastruttura interoperabilità PDND**. Tali passi non sono oggetto dei profili indicati di seguito ma sono garantiti dalle funzionalità per la richiesta di accesso e l'indicazione della finalità per la fruizione dell'**e-service**, assicurate dalla **Infrastruttura interoperabilità PDND**.
- La **Infrastruttura interoperabilità PDND** DEVE erogare le funzionalità di *Authorization Server* implementando il *Token Endpoint* per permettere al **Fruitore** di dare seguito all'*Access Token Request*. L'**Infrastruttura interoperabilità PDND** ricevuta l'*Access Token Request* di un **Client Fruitore** autentica lo stesso e constata l'avvenuta registrazione da

parte del **Fruitore** della finalità entro cui intende operare, in caso di esito positivo, rilascia l'**Access Token**;

- Il **Fruitore** utilizza l'*Access Token* ricevuto dalla **Infrastruttura interoperabilità PDND** per accedere all'**e-service**.



5.1 [REST_JWS_2021_Bearer] Profilo di emissione dei Voucher JWS Bearer

Il presente profilo è definito assumendo che:

- l'*Access Token Request* del **Client Fruitore** all'**Infrastruttura interoperabilità PDND** è basata su JSON Web Token (JWT) Profile for OAuth 2.0 (RFC7523);

- l'autenticazione del **Client Fruitore** da parte dell'**Infrastruttura interoperabilità PDND** è realizzata utilizzando il materiale crittografico registrato sulla stessa infrastruttura;
- l'**Infrastruttura interoperabilità PDND** emette un Bearer Access Token OAuth2 conforme all'RFC6750 veicolato tramite l'HTTP Header Authorization definito in RFC7235;
- l'Access Token emesso dall'**Infrastruttura interoperabilità PDND** consiste in un JWS conforme all'RFC7515 firmato dall'**Infrastruttura interoperabilità PDND**.

La validità temporale dell'*Access Token* emesso dall'**Infrastruttura interoperabilità PDND** PUÒ essere basata su un time-to-live eventualmente definito dall'**Erogatore** ed entro cui lo stesso può essere utilizzato dal **Client Fruitore** per accedere all'**e-service**.

5.1.1 Access Token Request del Client Fruitore

Le informazioni contenute nell'*Access Token Request* del **Client Fruitore** DEVONO permettere alla **Infrastruttura interoperabilità PDND** di individuare le seguenti informazioni:

- l'indicazione del **Client Fruitore** per cui si richiede l'emissione dell'*Access Token*.
- l'indicazione dell'autorizzazione in conseguenza dalla richiesta di fruizione che abilitano il **Client Fruitore** all'accesso all'**e-service** dell'**Erogatore**;
- l'indicazione della finalità indicata dal **Fruitore** entro cui il **Client Fruitore** si impegna ad utilizzare la risposta dell'**e-service** dell'**Erogatore.**

5.1.2 Access Token

Le informazioni contenute nell'Access Token emesso dall'**Infrastruttura interoperabilità PDND** DEVONO permettere all'**Erogatore** di individuare almeno le seguenti informazioni:

- l'indicazione del **Client Fruitore** per cui è stato emesso l'*Access Token*.
- l'indicazione dell'autorizzazione dell'**Erogatore** che abilita il **Client Fruitore** all'accesso all'**e-service**;
- l'indicazione della finalità indicata dal **Fruitore** entro cui il **Client Fruitore** si impegna a utilizzare la risposta dell'**e-service** dell'**Erogatore**.

5.1.3 Inoltro dell'Access Token all'Erogatore

Il **Client Fruitore** implementa la request all'**e-service** del **Erogatore** nel rispetto di quanto registrato da quest'ultimo sul **Catalogo API** e DEVE inserire nella richiesta l'*Access Token* emesso dall'**Infrastruttura interoperabilità PDND** nell'HTTP header Authorization come indicato in RFC6750.

Il **Fruitore** assicura il tracciamento delle richieste effettuate con l'*Access Token* emesso dall'**Infrastruttura interoperabilità PDND.**

5.1.4 Verifica del Voucher da parte dell'Erogatore

L'**Erogatore**, ricevuta la richiesta del **Client Fruitore**, DEVE almeno verificare:

- la validità della firma dell'*Access Token* apposta dall'**Infrastruttura interoperabilità PDND** mediante il materiale crittografico generato dalla stessa infrastruttura a tal fine e le informazioni contenute nel JWT;
- la scadenza dell'*Access Token* ed il time-to-live, ove presente, nel rispetto di quanto indicato dall'**Erogatore** nel descrittore dell'**e-service**.

In caso di esito positivo delle verifiche, l'**Erogatore** DEVE consentire al **Client Fruitore** l'accesso all'**e-service**.

Nel caso di esito negativo delle verifiche, l'**Erogatore** NON DEVE consentire al **Client Fruitore** l'accesso all'**e-service**.

L'**Erogatore** assicura il tracciamento delle richieste ricevute dai **Client Fruitore** con gli *Access Token* emessi dall'**Infrastruttura interoperabilità PDND.**

Le specifiche tecniche delle API REST rese disponibili dall'**Infrastruttura interoperabilità PDND** per permettere ai **Client Fruitori** di dare seguito all'*Access Token Request* e il dettaglio del contenuto dell'*Access Token* emesso dalla stessa infrastruttura sono oggetto della documentazione tecnica predisposta dal **Gestore**.

5.2 [REST_JWS_2021_POP] Profilo di emissione dei Voucher JWS POP

Il presente profilo è motivato dalla possibile esigenza che in alcuni scenari sia richiesto un grado di protezione aggiuntivo nel dominio di sicurezza del **Fruitore**, in base al quale un **Client Fruitore**, necessita di una **proof-of-possession** del materiale crittografico utilizzato per l'*Access Token Request*, al fine di assicurare che il suddetto **Client Fruitore** sia l'unico a potere utilizzare l'*Access Token* emesso dall'**Infrastruttura interoperabilità PDND** per l'accesso ad un determinato **e-service**.

Il presente profilo estende il profilo REST_JWS_2021_Bearer sopra definito affinché l'*Access Token* emesso dall'**Infrastruttura interoperabilità PDND** per l'accesso ad un determinato **e-service** non costituisca un token di accesso al portatore, e quindi utilizzabile da qualunque parte ne entri in possesso, ma sia resa possibile la verifica da parte dell'**Erogatore** del **Client Fruitore** che ha richiesto l'emissione dell'*Access Token* e per il quale lo stesso è stato emesso.

5.2.1 Access Token Request del Client Fruitore

Le informazioni contenute nell'*Access Token Request* del **Client Fruitore** DEVONO permettere alla **Infrastruttura interoperabilità PDND** di individuare le seguenti informazioni:

- l'indicazione del **Client Fruitore** per cui si richiede l'emissione dell'*Access Token*.
- l'indicazione dell'autorizzazione in conseguenza dalla richiesta di fruizione che abilitano il **Client Fruitore** all'accesso all'**e-service** dell'**Erogatore**;
- l'indicazione della finalità indicata dal **Fruitore** entro cui il **Client Fruitore** si impegna ad utilizzare la risposta dell'**e-service** dell'**Erogatore.**
- Un **proof-of-possession** del materiale crittografico privato corrispondente al materiale crittografico pubblico a cui l''*Access Token* richiesto deve essere collegato.

5.2.2 Access Token

Le informazioni contenute nell'Access Token emesso dall'**Infrastruttura interoperabilità PDND** DEVONO permettere all'**Erogatore** di individuare almeno le seguenti informazioni:

- l'indicazione del **Client Fruitore** per cui è stato emesso l'*Access Token*.

- l'indicazione dell'autorizzazione dell'**Erogatore** che abilita il **Client Fruitore** all'accesso all'**e-service**;
- l'indicazione della finalità indicata dal **Fruitore** entro cui il **Client Fruitore** si impegna a utilizzare la risposta dell'**e-service** dell'**Erogatore**;
- l'indicazione della **proof-of-possession** ricevuta nell''*Access Token Request* per cui il token è emesso.

5.2.3 Inoltro dell'Access Token all'Erogatore

Il **Client Fruitore** implementa la request all'**e-service** del **Erogatore** nel rispetto di quanto registrato da quest'ultimo sul **Catalogo API** e DEVE inserire nella richiesta l'*Access Token* emesso dall'**Infrastruttura interoperabilità PDND** nell'HTTP header Authorization come indicato in RFC6750 e la relativa **proof-of-possession** del materiale crittografico in suo possesso.

Il **Fruitore** assicura il tracciamento delle richieste effettuate con l'*Access Token* emesso dall'**Infrastruttura interoperabilità PDND.**

5.2.4 Verifica del Voucher da parte dell'Erogatore

L'**Erogatore**, ricevuta la richiesta del **Client Fruitore**, DEVE almeno verificare:

- la validità della firma dell'*Access Token* apposta dall'**Infrastruttura interoperabilità PDND** mediante il materiale crittografico generato dalla stessa infrastruttura a tal fine e le informazioni contenute nel JWT;
- la scadenza dell'*Access Token* ed il time-to-live, ove presente, nel rispetto di quanto stipulato nell'**Accordo di interoperabilità** con il **Fruitore**.
- la validità della **proof-of-possession** collegata all'*Access Token*.

In caso di esito positivo delle verifiche, l'**Erogatore** DEVE consentire al **Client Fruitore** l'accesso all'**e-service**.

Nel caso di fallimento delle verifiche, l'**Erogatore** NON DEVE consentire al **Client Fruitore** l'accesso all'**e-service**.

L'**Erogatore** assicura il tracciamento delle richieste ricevute dai **Client Fruitore** con gli *Access Token* emessi dall'**Infrastruttura interoperabilità PDND.**

Le specifiche tecniche delle API REST rese disponibili dall'**Infrastruttura interoperabilità PDND** per permettere ai **Client Fruitori** di dare seguito all'*Access Token Request* e il dettaglio del contenuto dell'*Access Token* emesso dalla stessa infrastruttura sono oggetto della documentazione tecnica predisposta dal **Gestore**.