DOCUMENTO TECNICO

Infrastruttura per l’acquisizione dei dati relativi ai servizi erogati dai soggetti vigilati ai sensi dell’art. 14-bis, comma 2, lett. i) del CAD

Versione	Data	Elenco modifiche
1.0	20/01/2022	Prima emissione
1.1	31/05/2022	Aggiornamento paragrafi 3.10.3 e 3.10.4
1.2	07/07/2022	Inserimento riferimenti all'OID 2.5.4.97

Sommario

Capitolo 1

Introduzione

1.1 Scopo

Il presente Documento Tecnico, nel seguito indicato come DT, ha lo scopo di definire i requisiti per la realizzazione dell'infrastruttura dedicata all'acquisizione dei dati relativi ai servizi che i soggetti vigilati da AgID ai sensi dell'art. 14-bis, comma 2, lett. i) del decreto legislativo 7 marzo 2005, n. 82 e s.m.i. sono tenuti a inviare secondo modalità indicate dalla stessa Agenzia, per scopi di vigilanza.

La specifica e il formato dei dati, che includono ad esempio dati strutturati (misure dei livelli di servizio erogati in un periodo di riferimento; volumi gestiti dal soggetto erogatore; riepilogo degli incidenti e dei disservizi; ecc,), documenti, segnalazioni di incidenti o malfunzionamenti secondo quanto previsto dalle norme di riferimento per ciascuna tipologia di servizio e di qualsiasi altra informazione che deve poter essere acquisita tramite la piattaforma in oggetto, sono descritti nei rispettive Linee Guida, se previste ai sensi dell'art. 71 del decreto legislativo 7 marzo 2005, n. 82 e s.m.i., o in analoghi documenti tecnici emessi dall'Agenzia; tali documenti sono da considerarsi complementari al presente ed essenziali alla corretta interpretazione delle specifiche indicate nel presente DT e all'implementazione della piattaforma in oggetto.

1.2 Struttura

Il presente Documento Tecnico, oltre al documento suddetto, è composto dai seguenti **Documenti Operativi:**

a) Allegato_AcquisizioneDati_EndpointTracciati
b) Allegato_AcquisizioneDati_CodiciResponse

Tali Documenti operativi definiscono le specifiche tecniche implementative che possono variare nel tempo ma che non modificano il riferimento e le regole qui definite.

1.3 Gruppo di lavoro

La redazione del presente documento è stata curata dal gruppo di lavoro AgID con la collaborazione dei destinatari del DT.

1.4 Soggetti destinatari

I soggetti destinatari del presente DT sono tutti i soggetti sottoposti alle funzioni di vigilanza ai sensi dell'art. 14-bis, comma 2, lett. i) del decreto legislativo 7 marzo 2005, n. 82 e s.m.i., i quali devono poter inviare le informazioni e i dati in proprio possesso, richiesti da AgID, tramite la piattaforma oggetto del presente DT.

Capitolo 2

Riferimenti e sigle

2.1 Riferimenti Normativi

Sono riportati di seguito gli atti normativi di riferimento del presente documento.

- **[D.Lgs. 82/2005]** Decreto legislativo 7 marzo 2005, n. 82 recante "Codice dell'amministrazione digitale" (di seguito "CAD").

2.2 Standard di riferimento

Sono riportati di seguito gli standard tecnici di riferimento per l'applicazione del presente documento.

- **[OAS v3]** Open API Specification v3
- **[RFC-7515]** JSON Web Signature (JWS)
- **[RFC-3230]** Instance Digests in HTTP

2.3 Linee guida di riferimento

Di seguito sono elencate le Linee Guida e le Regole Tecniche emesse dall'AgID che verranno richiamate nel presente documento:

- Linea di indirizzo sulla interoperabilità tecnica (Determinazione AgID n. 406/2020);
- Linee Guida per la normalizzazione dei dati statistici dei servizi erogati dai Gestori PEC, dai Conservatori e dai Prestatori di servizi fiduciari qualificati (Determinazione AgID n. 259/2021).

2.4 Termini e definizioni

Di seguito si riportano gli ACRONIMI che verranno utilizzati:

- **[AgID]** Agenzia per l'Italia Digitale
- **[PA]** Pubblica Amministrazione
- **[MODELLO INTEROPERABILITÀ]** Linea di indirizzo sulla interoperabilità tecnica, adottata con determinazione AgID n. 406 del 09/09/2020
- **[PIATTAFORMA]** Implementazione dell'infrastruttura oggetto del DT
- **[OAS3]** Open API Specification version 3

Capitolo 3

Requisiti

3.1 Profilo di interoperabilità

Il **MODELLO INTEROPERABILITÀ** rende possibile la collaborazione tra PA e tra queste e soggetti terzi, per mezzo di soluzioni tecnologiche che assicurano l'interazione e lo scambio di informazioni senza vincoli sulle implementazioni, al fine di garantire l'interoperabilità dei sistemi e favorire l'implementazione complessiva del Sistema informativo della PA.

L'infrastruttura per l'acquisizione dati, oggetto del presente DT, di seguito definita **PIATTAFORMA**, si configura nel rispetto del **MODELLO INTEROPERABILITÀ**, attinente al profilo per la non ripudiabilità della trasmissione, con i seguenti pattern:

Pattern di interazione: **CRUD REST**[1]

Pattern di sicurezza: **ID_AUTH_CHANNEL_01, ID_AUTH_REST_02, INTEGRITY_REST_01**[2]

3.2 Interfaccia API RESTful

La **PIATTAFORMA**, è realizzata tramite una interfaccia API RESTful[3] conforme alle specifiche OpenAPI v.3[4] (**OAS3**) ed implementata secondo quanto indicato nel seguito.

[1] **[MODELLO INTEROPERABILITÀ] -** Pattern di interazione 7.1
[2] **[MODELLO INTEROPERABILITÀ]** – Pattern di sicurezza 4.1, 5.4, 6.2
[3] REST (Representational State Transfer). Roy Fielding
[4] Open API Specification v3. [https://swagger.io/specification]

3.3 Documento OpenAPI

L'interfaccia OpenAPI che realizza la **PIATTAFORMA** è completamente descritta da un unico file JSON, definito documento OpenAPI, compatibile con le specifiche **OAS3** e con le specifiche riportate nel seguito.

3.4 Versioning

Al fine di garantire scalabilità ed evitare che successive modifiche alle API abbiano ripercussioni sulle integrazioni esistenti, tutti gli endpoint supportano il versionamento sull'URL. Sarà possibile, quindi, effettuare un'interrogazione verso una specifica versione dell'API indicando l'URL corrispondente, che DEVE essere formata nel seguente modo:

https://**<HOST>/api/v<MAJOR>[.<MINOR>][.<PATCH>]/<operation>**

I numeri MAJOR, MINOR e PATCH sono da intendere secondo l'accezione SemVer[5].

Nota: <HOST> è il dominio dell'AA
<MAJOR> è il numero MAJOR corrispondente alla versione dell'API
<MINOR> è il numero MINOR corrispondente alla versione dell'API
<PATCH> è il numero PATCH corrispondente alla versione dell'API
<operation> è il path della chiamata API

I numeri indicati tra parentesi quadre non sono obbligatori e possono essere omessi. In tal caso verrà indirizzata la versione corrispondente al numero MINOR o PATCH, rispettivamente, più alto disponibile. Sono di seguito riportati alcuni esempi di URL per versioni differenti della stessa chiamata API.

```
https://data.agid.gov.it/api/v1.0.0/identita-digitali
https://data.agid.gov.it/api/v1.1/identita-digitali
```

Il numero di versione, indicato dalla parte v<MAJOR>[.<MINOR>][.<PATH>], identifica la versione globale dell'interfaccia API. Eventuali modifiche, apportate a un singolo endpoint dell'API, comportano il rilascio di una nuova versione API, valida per tutti gli endpoint. Sarà cura di AgID comunicare ai soggetti destinatari del presente DT, nelle modalità che si riterranno opportune, gli aggiornamenti di versione e la versione da utilizzare.

Alla URL dell'host presso il quale sono esposte le varie versioni dell'interfaccia API: **https://<HOST>/api** DOVREBBERO essere elencate le versioni disponibili e, opzionalmente, i changelog di ogni specifica versione.

[5] Semantic Version Specification. (https://semver.org/)

3.5 Documentazione API

Alla URL base dell'API, comprensiva dei riferimenti relativi al versioning, è esposta la documentazione generata automaticamente sulla base del documento **OAS3**. Con riferimento agli esempi riportati nel paragrafo precedente, le rispettive documentazioni saranno esposte alla seguenti URL:

```
https://data.agid.gov.it/api/v.1.0.0
https://data.agid.gov.it/api/v.1.1
```

3.6 Endpoint per tracciati record

L'interfaccia API dovrà implementare un endpoint (path) per ognuno dei **tracciati record** i cui dati devono poter essere acquisiti dalla **PIATTAFORMA**. Tali **tracciati record** sono descritti negli altri documenti operativi emanati da AgID e complementari al presente DT. Le definizioni dei path per ciascuno dei tracciati record previsti, sono riportati nel documento operativo allegato "**Allegato_AcquisizioneDati_EndpointTracciati**".

Tutti gli esempi riportati nel presente documento, che fanno riferimento a dati di tracciati record, sono presentati puramente a titolo esemplificativo e, pertanto, non sono da considerarsi normativi.

3.7 Autenticazione

Tutti gli endpoint delle API sono protetti tramite autenticazione. L'unica tipologia di autenticazione consentita è la Bearer Authentication tramite token in formato JWT, costituito dagli elementi descritti di seguito e firmato utilizzando la JWT Compact Serialization.

L'header è costituito dalle seguenti informazioni:

Parametro	Descrizione
typ	valorizzato con la stringa "JWT" ad indicare che il token è un JSON Web Token.
alg	valorizzato con l'identificativo JWA dell'algoritmo crittografico utilizzato.
x5c	valorizzato con il certificato o la catena dei certificati, in formato X.509, corrispondente alla chiave pubblica del certificato di sigillo elettronico utilizzato. Il certificato o la catena dei certificati sono codificati come array JSON di stringhe corrispondenti ai valori dei certificati in formato DER. Ogni stringa nell'array è codificata in Base64. Il certificato contenente la chiave pubblica del sigillo utilizzato per firmare il token deve essere la prima stringa dell'array.

Il payload è costituito dalle seguenti informazioni

Parametro	Descrizione
iss	deve corrispondere al Soggetto mittente, come indicato nel campo "OrganizationIdentifier" (OID 2.5.4.97) del certificato di sigillo elettronico contenuto nel campo x5c dell' header.
jti	identificativo unico del token.
aud	deve contenere il valore "**https://agid.gov.it**".
iat	istante di generazione della richiesta, codificato come NumericDate come indicato in RFC 7519 – JSON Web Token (JWT)[6]

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

exp	istante di scadenza della richiesta, codificato come NumericDate come indicato in RFC 7519 – JSON Web Token (JWT)[6]
signed_headers	array contente gli header HTTP da inserire nel token. Es. [{"digest": "SHA-256=… "}, {"content-type": "application/json"}]

3.8 Tipologie di operazioni

Sugli endpoint definiti per l'acquisizione dei tracciati sono consentite le operazioni per:

- il recupero dei dati relativi a uno o più record;
- l'inserimento di nuovi record;
- l'aggiornamento parziale o completo di record esistenti;
- la cancellazione di record esistenti.

La mappatura delle operazioni sui metodi DEVE seguire l'accezione derivante dal paradigma REST, ed in particolare:

- operazioni sul metodo GET per il recupero di dati relativi ad uno o più record;
- operazioni sul metodo POST per l'inserimento di nuovi record;
- operazioni sul metodo PATCH per l'aggiornamento parziale di specifico record;
- operazioni sul metodo PUT per l'aggiornamento completo di specifico record;
- operazioni sul metodo DELETE per la cancellazione di specifico record.

L'utilizzo di ogni operazione è limitato ai client che ne hanno la specifica autorizzazione secondo quanto indicato nel successivo paragrafo **3.9 Autorizzazioni**. I requisiti per ogni operazione sono definiti nel documento operativo allegato "**Allegato_AcquisizioneDati_EndpointTracciati**".

3.9 Autorizzazioni

I client che possono interrogare i servizi esposti dall'interfaccia API della **PIATTAFORMA**, devono autenticarsi tramite un token JWT firmato mediante un certificato di sigillo elettronico rilasciato dall'Agenzia.

Il certificato di sigillo elettronico identifica il soggetto unitamente alla tipologia di soggetto che effettua l'interrogazione, in coerenza con quanto previsto dall'Agenzia per l'emissione dei certificati di sigillo elettronico.

Nel documento operativo allegato "**Allegato_AcquisizioneDati_EndpointTracciati**", in relazione alla tipologia di soggetto o al soggetto stesso, sono definiti:

- gli endpoint che il soggetto può interrogare
- le operazioni ammesse su ogni endpoint

3.10 Request

In relazione alla tipologia di operazione si distinguono i seguenti tipi di Request:

- request per inserimento di un nuovo record
- request per aggiornamento parziale di un record esistente
- request per aggiornamento completo di un record esistente
- request per il recupero di uno specifico record
- request per il recupero di più record

Nei paragrafi seguenti sono descritte la modalità di invio e di specifica dei parametri e lo schema di response attesa per ogni tipo di request. I parametri utilizzabili sugli endpoint sono corrispondenti ai campi dei relativi tracciati, come definiti negli allegati tecnici.

3.10.1 Request Header

Gli Header HTTP delle request devono rispettare quanto previsto nel profilo **INTEGRITY_REST_01**[7] del **MODELLO INTEROPERABILITÀ** al fine di garantire l'integrità del messaggio. In particolare, l'header dovrà contenere il campo **Digest** ed il campo **Agid-JWT-Signature** contenente il token di autorizzazione costruito come indicato in **3.7 Autenticazione**.

La tabella seguente presenta l'insieme minimo dei campi che DEVONO essere sempre presenti nelle Request:

Header	Valore
Accept	**application/json**
Agid-JWT-Signature	token di autenticazione, come indicato in **3.7 Autenticazione**
Digest	calcolato dal body del messaggio secondo **[RFC-3230]**
Content-Type	**application/json**

Viene di seguito riportato un esempio di Header di una Request:

```
POST https://data.agid.gov.it/api/v1.0/identita-digitali

Accept: application/json
Agid-JWT-Signature: eyJhbGciOiJSUzI1NiIsInR5c.vz8...
Digest: SHA-256=cFfTOCesr...
Content-Type: application/json
```

[7] **[MODELLO INTEROPERABILITÀ]** - Pattern sicurezza 6.2

3.10.2 Inserimento di un nuovo record

La chiamata a un endpoint per l'inserimento di un record è formata nel seguente modo:

POST https://<HOST>/api/v<MAJOR>.<MINOR>[.<PATH>]/<operation>

Nel body della request DEVE essere presente un JSON Array contenente i record da inserire. L'array potrà essere costituito anche da un solo elemento. Ogni elemento presente nell'array DEVE essere costituito dagli elementi previsti per l'endpoint in oggetto e descritti nei documenti che definiscono lo specifico tracciato.

Viene di seguito riportato un esempio per l'inserimento di un nuovo record relativo ad "Identità digitali" presso l'endpoint "identita-digitali".

```
POST https://data.agid.gov.it/api/v1.0/identita-digitali
[{
   identityProviderName: "IDP1",
   identityProviderID: https://entityid.idp1
   identityCode: "id_1"
   day: "100"
   year: "2019",
   idStatus: "2",
   recogMethod: "5",
   placeOfBirth: "F205",
   countyOfBirth: "MI",
   yearOfBirth: "1981",
   domicile: "IT-F205",
   gender: "M",
   userType: "1",
   releaseTime: "3"
}]
```

La registrazione del record prevede la registrazione sullo stesso di data e ora in formato UTC dell'istante di acquisizione dei dati.

La registrazione del record implica l'associazione dello stesso al soggetto che ha effettuato l'inserimento, identificato tramite il campo "OrganizationIdentifier " contenuto nel certificato di sigillo elettronico con il quale viene effettuata l'autenticazione presso l'endpoint.

La response sarà formata secondo le specifiche indicate nel paragrafo **3.11 Response**. In caso di esito positivo dell'inserimento essa conterrà, nel campo **result,** un array con i riferimenti

URI ai record appena creati. Viene di seguito riportato un esempio di response relativa all'esempio di request precedente.

```
HTTP 201 CREATED
{
   result: [https://data.agid.gov.it/api/v1.0.0/identita-digitali/10]
}
```

Nel body della request, oltre agli elementi previsti per l'endpoint in oggetto, potrà essere presente anche il parametro **externalRef**. La presenza del parametro externalRef non è obbligatoria ma, se presente, il valore specificato per *externalRef* sullo specifico record DEVE risultare univoco per la risorsa di cui all'endpoint.

Se tra i record inviati all'interno del payload della request, è presente almeno un record il cui valore specificato per *externalRef* è già presente tra i record registrati sulla risorsa o se tra i record inviati all'interno del payload della request, sono presenti più record aventi lo stesso valore specificato per *externalRef*, l'esito della richiesta d'inserimento sarà negativo e verrà restituito uno specifico errore, in accordo con quanto indicato nel documento operativo allegato **"Allegato_AcquisizioneDati_CodiciResponse"**.

Se *externalRef* non è specificato, il salvataggio del record DEVE essere invece consentito.

L'operazione di inserimento di nuovi record DEVE intendersi sempre in transazione, pertanto non dovrà essere possibile, per qualsivoglia ragione, che alcuni record dell'array inviato nel payload della request vengano salvati e altri no.

3.10.3 Aggiornamento parziale di un record esistente

La chiamata ad un endpoint per l'aggiornamento limitato ad alcuni campi di un record esistente è formata nel seguente modo:

PATCH

https://<HOST>/api/v<MAJOR>.<MINOR>[.<PATH>]/<operation>/<id>

dove **<id>** è l'identificativo unico del record.

Nel body della request DEVE essere presente un oggetto JSON contenente i campi da aggiornare, in coerenza con quanto previsto per l'endpoint in oggetto e descritto nel documento relativo allo specifico tracciato. Viene di seguito riportato un esempio per l'aggiornamento dell'anno di nascita dell'identità digitale inserita sull' id 10 presso l'endpoint "identita-digitali".

```
PUT  https://data.agid.gov.it/api/v1.0/identita-digitali/10
{
   yearOfBirth: "1980"
}
```

L'id viene creato al momento dell'inserimento del record ed è associato al soggetto che lo ha inserito, identificato tramite il campo OrganizationIdentifier contenuto nel certificato di sigillo elettronico con il quale viene effettuata l'autenticazione presso l'endpoint.

Nel body della request, oltre agli elementi previsti per l'endpoint in oggetto, potrà essere presente anche il parametro **externalIdType**. La presenza del parametro externalIdType non è obbligatoria ma, se il parametro è presente ed è valorizzato con la stringa *externalRef*, il valore del parametro <id> deve intendersi come valore del parametro externalRef indicato all'atto della creazione del record, invece che come valore dell'indentificativo interno del record, e l' operazione di aggiornamento deve insistere sul record identificato dal corrispondente campo externalRef.

Nel caso in cui non dovesse esistere alcun record identificato dal campo indicato tramite il parametro externalIdType, oppure nel caso in cui dovessero corrispondere più record associati al valore del campo indicato tramite il parametro externalIdType, l'esito della richiesta di aggiornamento sarà negativo e verrà restituito uno specifico errore, in accordo con quanto indicato nel documento operativo allegato **"Allegato_AcquisizioneDati_CodiciResponse"**.

Ulteriori valori di tipo per il parametro externalIdType potranno essere specificati in apposito documento allegato.

L'aggiornamento del record prevede la registrazione sullo stesso di data e ora in formato UTC dell'istante di acquisizione dei dati, come data di ultima modifica. Il sistema DEVE, in ogni caso, permettere di risalire sempre anche alla data di inserimento del record.

Nel caso di aggiornamento di un record effettuato da un soggetto diverso dal soggetto che ha inserito inizialmente il record, verrà restituito uno specifico errore, in accordo con quanto indicato nel documento operativo allegato **"Allegato_AcquisizioneDati_CodiciResponse"**.

La response sarà formata secondo le specifiche indicate nel paragrafo **3.11 Response**. In caso di esito positivo dell'aggiornamento essa conterrà, nel campo **result**, il riferimento URI al record aggiornato. Viene di seguito riportato un esempio di response.

```
HTTP 200 OK

{
   result: "https://data.agid.gov.it/api/v1.0.0/identita-digitali/10"
}
```

3.10.4 Aggiornamento completo di un record esistente

La chiamata ad un endpoint per l'aggiornamento di tutti i campi di un record esistente è formata nel seguente modo:

PUT

https://<HOST>/api/v<MAJOR>.<MINOR>[.<PATH>]/<operation>/<id>

dove **<id>** è l'identificativo unico del record.

Nel body della request DEVE essere presente un oggetto JSON contenente TUTTI i campi della risorsa con il nuovo valore da aggiornare, in coerenza con quanto previsto per l'endpoint in oggetto e descritto nel documento relativo allo specifico tracciato. Viene di seguito riportato un esempio per l'aggiornamento dell'anno di nascita dell'identità digitale inserita sull' id 10 presso l'endpoint "identita-digitali".

```
PUT  https://data.agid.gov.it/api/v1.0/identita-digitali/10
{
   identityProviderName: "IDP1",
   identityProviderID: https://entityid.idp1
   identityCode: "id_1"
   day: "101"
   year: "2019",
   idStatus: "2",
   recogMethod: "5",
   placeOfBirth: "F205",
   countyOfBirth: "MI",
   yearOfBirth: "1980",
   domicile: "IT-F205",
   gender: "M",
   userType: "1",
   releaseTime: "3"
}
```

L'id viene creato al momento dell'inserimento del record ed è associato al soggetto che lo ha inserito, identificato tramite il campo OrganizationIdentifier contenuto nel certificato di sigillo elettronico con il quale viene effettuata l'autenticazione presso l'endpoint.

Nel body della request, oltre agli elementi previsti per l'endpoint in oggetto, potrà essere presente anche il parametro **externalIdType**. La presenza del parametro externalIdType non è obbligatoria ma, se il parametro è presente ed è valorizzato con la stringa *externalRef*, il valore del

parametro <id> deve intendersi come valore del parametro externalRef indicato all'atto della creazione del record, invece che come valore dell'indentificativo interno del record, e l' operazione di aggiornamento deve insistere sul record identificato dal corrispondente campo externalRef.

Nel caso in cui non dovesse esistere alcun record identificato dal campo indicato tramite il parametro externalIdType, oppure nel caso in cui dovessero corrispondere più record associati al valore del campo indicato tramite il parametro externalIdType, l'esito della richiesta di aggiornamento sarà negativo e verrà restituito uno specifico errore, in accordo con quanto indicato nel documento operativo allegato **"Allegato_AcquisizioneDati_CodiciResponse"**.

Ulteriori valori di tipo per il parametro externalIdType potranno essere specificati in apposito documento allegato.

L'aggiornamento del record prevede la registrazione sullo stesso di data e ora in formato UTC dell'istante di acquisizione dei dati, come data di ultima modifica. Il sistema DEVE, in ogni caso, permettere di risalire sempre anche alla data di inserimento del record.

Nel caso di aggiornamento di un record effettuato da un soggetto diverso dal soggetto che ha inserito inizialmente il record, verrà restituito uno specifico errore, in accordo con quanto indicato nel documento operativo allegato **"Allegato_AcquisizioneDati_CodiciResponse"**.

La response sarà formata secondo le specifiche indicate nel paragrafo **3.11 Response**. In caso di esito positivo dell'aggiornamento essa conterrà, nel campo **result**, il riferimento URI al record aggiornato. Viene di seguito riportato un esempio di response.

```
HTTP 200 OK

{
   result: "https://data.agid.gov.it/api/v1.0.0/identita-digitali/10"
}
```

3.10.5 Recupero di uno specifico record

La chiamata ad un endpoint per il recupero di uno specifico record è formata nel seguente modo:

GET https://<HOST>/api/v<MAJOR>.<MINOR>[.<PATH>]/<operation>/<id>

dove **<id>** è l'identificativo unico del record.

Viene di seguito riportato un esempio per il recupero del record num. 10 relativo al tracciato "Identità digitali", presso l'endpoint "indentita-digitali":

```
GET  https://data.agid.gov.it/api/v1.0/identita-digitali/10
```

L'id viene creato al momento dell'inserimento del record ed è associato al soggetto che lo ha inserito, identificato tramite il campo OrganizationIdentifier contenuto nel certificato di sigillo elettronico con il quale viene effettuata l'autenticazione presso l'endpoint.

Nel caso in cui venga richiesto un record da un soggetto diverso dal soggetto che ha inserito inizialmente il record, tale record potrà essere restituito solo se il soggetto richiedente è abilitato a poter effettuare interrogazioni sul metodo GET sull'endpoint in oggetto. In caso contrario, verrà restituito uno specifico errore, in accordo con quanto indicato nel documento operativo allegato **"Allegato_AcquisizioneDati_CodiciResponse"**.

La response sarà formata secondo le specifiche indicate nel paragrafo **3.11 Response**. In caso di record recuperato con successo essa conterrà, nel campo **result**, un oggetto JSON rappresentativo del record richiesto. Viene di seguito riportato un esempio di response relativa all'esempio di request precedente.

```
HTTP 200 OK
{
   result: {
      identityProviderName: "IDP1",
      identityProviderID: https://entityid.idp1
      identityCode: "id_1"
      day: "100"
      year: "2019",
      idStatus: "2",
      recogMethod: "5",
      placeOfBirth: "F205",
      countyOfBirth: "MI",
      ...
   }
}
```

3.10.6 Recupero di uno specifico record tramite *ExternalRef*

Se con l'inserimento di un record è stato specificato un valore per il parametro *externalRef*, sarà possibile recuperare il record indirizzandolo per tramite di tale valore.

La chiamata ad un endpoint per il recupero di uno specifico record tramite il parametro *externalRef* è formata nel seguente modo:

GET https://<HOST>/api/v<MAJOR>.<MINOR>[.<PATH>]/<operation>?externalRef=<external_ref>

dove **<external_ref>** è il valore specificato per *externalRef* in fase di creazione del record. Viene di seguito riportato un esempio per il recupero tramite *externalRef*, presso l'endpoint "indentita-digitali", dell'identità digitale registrata con externalRef=X

```
GET  https://.../identita-digitali?externalRef=X
```

Sarà restituito il record risultante dalla ricerca e appartenente al soggetto identificato tramite il campo "OrganizationIdentifier " contenuto nel certificato di sigillo elettronico con il quale viene effettuata l'autenticazione presso l'endpoint.

Nel caso in cui la richiesta venga effettuata da un soggetto diverso dal soggetto che ha inserito inizialmente il record, tale record potrà essere restituito solo se il soggetto richiedente è abilitato a poter effettuare interrogazioni sul metodo GET sull'endpoint in oggetto. In caso contrario, verrà restituito uno specifico errore, in accordo con quanto indicato nel documento operativo allegato **"Allegato_AcquisizioneDati_CodiciResponse"**.

La response sarà formata secondo le specifiche indicate nel paragrafo **3.11 Response**. In caso di record recuperato con successo essa conterrà, nel campo **result**, un oggetto JSON rappresentativo del record richiesto. Viene di seguito riportato un esempio di response relativa all'esempio di request precedente.

```
HTTP 200 OK
{
   result: {
      externalRef: "X",
      identityProviderName: "IDP1",
      ...
   }
}
```

3.10.7 Recupero di più record

La chiamata ad un endpoint per il recupero di più record è formata nel seguente modo:

GET https://<HOST>/api/v<MAJOR>.<MINOR>[.<PATH>]/<operation>?query

dove **<query>** è la querystring costituita dall'elenco dei parametri per i quali effettuare la ricerca.

Viene di seguito riportato un esempio per il recupero, presso l'endpoint "indentita-digitali", delle identità digitali di tipo "persona fisica" rilasciate nell'anno "2019"

```
GET  https://.../identita-digitali?userType=1&idStatus=2&year=2019
```

Saranno restituiti i record risultanti dalla ricerca e appartenenti al soggetto identificato tramite il campo "OrganizationIdentifier " contenuto nel certificato di sigillo elettronico con il quale viene effettuata l'autenticazione presso l'endpoint.

Nel caso in cui la richiesta venga effettuata da un soggetto diverso dal soggetto che ha inserito inizialmente il record, tale record potrà essere restituito solo se il soggetto richiedente è abilitato a poter effettuare interrogazioni sul metodo GET sull'endpoint in oggetto. In caso contrario, verrà restituito uno specifico errore, in accordo con quanto indicato nel documento operativo allegato **"Allegato_AcquisizioneDati_CodiciResponse"**.

La response sarà formata secondo le specifiche indicate nel paragrafo **3.11 Response**. Nel caso di esito positivo essa conterrà, nel campo **result**, un array JSON rappresentativo dell'insieme dei record risultanti dalla ricerca, come nel seguente esempio.

```
{
   result: [
      {
         identityProviderName: "IDP1",
         identityProviderID: https://entityid.idp1
         identityCode: "id_1"
         day: "100"
         year: "2019",
         idStatus: "2",
         recogMethod: "5",
         placeOfBirth: "F205",
         countyOfBirth: "MI",
         yearOfBirth: "1981",
         ...
      },
      ...
   ]
}
```

3.10.8 Parametri di ricerca

Sulla querystring di un'operazione di recupero è possibile specificare i parametri per i quali effettuare la ricerca. I parametri che è possibile utilizzare per la ricerca e il relativo formato sono descritti nei documenti del relativo tracciato.

Nel caso in cui per un parametro sia possibile indicare più valori, questi DEVONO essere separati dal carattere separatore "virgola". Viene di seguito riportato un esempio per il recupero, presso l'endpoint "indentita-digitali", delle identità digitali di tipo "persona fisica" rilasciate negli anni "2017", "2018", "2019"

```
GET  https://.../identita-digitali?userType=1&idStatus=3&year=2017,2018,2019
```

3.10.9 Ricerca per soggetto

Sulla querystring di un'operazione di recupero è possibile specificare il parametro *subject* valorizzato con il soggetto che ha inizialmente creato il record, ovvero con il valore dell'attributo O (Organization) dell'elemento Subject del certificato di sigillo elettronico con il quale è stata eseguita l'autenticazione durante l'operazione di creazione del record.

```
GET  https://.../identita-digitali?subject=Organization
```

Nel caso in cui sia specificato un valore per il parametro *subject* corrispondente ad un soggetto diverso dal soggetto che sta eseguendo l'interrogazione, il risultato dell'interrogazione potrà essere restituito solo se il soggetto richiedente è abilitato a poter effettuare interrogazioni per soggetti diversi dal soggetto che ha inizialmente creato il record. In caso contrario, verrà restituito uno specifico errore, in accordo con quanto indicato nel documento operativo allegato **"Allegato_AcquisizioneDati_CodiciResponse"**.

3.10.10 Paginazione di più record

Nel caso in cui la ricerca produca un numero rilevante di record, per ottimizzare la chiamata, è possibile utilizzare la paginazione dei risultati. In particolare è possibile specificare sulla querystring i seguenti parametri aggiuntivi

Parametro	Descrizione	Valore di default
page	Numero di pagina da restituire, a partire dal valore 1	0
numRows	Numero di record per ogni pagina	50

Se il parametro page manca, oppure è valorizzato con il numero "0", oppure è valorizzato con la stringa "false", la paginazione si intende disattivata. Se, invece, viene specificato per il parametro page un numero intero maggiore di 0, la paginazione è attivata e sarà restituito un numero di record pari al valore indicato nel parametro numRows o al suo valore di default se questo non viene specificato.

La response sarà formata secondo le specifiche indicate nel paragrafo **3.11 Response**. Nel caso di esito positivo essa conterrà, inoltre, i seguenti elementi

Elemento	Descrizione
totRows	Numero totale di record risultante dalla ricerca
totPages	Numero totale di pagine risultanti dalla ricerca
currentPage	Numero di pagina corrente
result	Array JSON con l'insieme dei record della pagina corrente

Viene di seguito mostrato un esempio di request per ottenere la terza pagina, costituita da 25 record, di tutte le identità digitali rilasciate e la relativa response.

```
GET  https://.../identita-digitali?idStatus=2&page=3&numRows=25
```

```
{
   totRows: 50000,
   totPages: 2000,
   currentPage: 3,
   result: [
      ...
   ]
}
```

3.11 Response

Le Response sono restituite come Media-Type *application/json*. Il body della Response contiene un oggetto JSON avente almeno i seguenti elementi:

Elemento	Descrizione
status	HTTP status code, come nell' Header
title	Descrizione standard del codice di ritorno
result	Dati response

Oltre agli elementi sopra indicati potranno essere presenti ulteriori elementi, come ad esempio nel caso di paginazione (vedi paragrafo **3.10.10 Paginazione di più record**).

Le tipologie di response possibili, comprensive dei valori previsti per status e title, sono elencate nel documento operativo allegato "**AcquisizioneDati_CodiciResponse**"

3.12 Errori

In caso di errore, verrà resitutita una Response come Media-Type application/json avente codice di stato HTTP relativo all'errore e, nel body, un oggetto JSON avente i seguenti elementi, in accordo con le indicazioni contenute nella norma RFC7807[8]:

Elemento	Descrizione
status	HTTP status code, come nell' Header
code	Codice specifico dell'errore

[8] RFC7807 - Problem Details for HTTP APIs (https://tools.ietf.org/rfc/rfc7807.txt)

title	Descrizione standard dell'errore
detail	Messaggio specifico dell'errore

Le tipologie di errore possibili, comprensive dei valori previsti per status, code e title, sono elencate nel documento operativo allegato "**Allegato_acquisizioneDati_CodiciResponse**"

3.13 Gestione dei Log

La **PIATTAFORMA** conserverà traccia di:

- ogni request ricevuta, comprensiva di data e ora di ricezione e delle informazioni relative all'eventuale certificato con il quale è stata effettuata l'autenticazione presso l'endpoint.
- ogni response inviata, comprensiva di data e ora di invio, e del riferimento alla relativa request.

I log sono conservati per 24 mesi.

3.14 Sistema di Notifiche

La **PIATTAFORMA** consentirà di configurare uno o più indirizzi e-mail ai quali inviare le stesse informazioni previste per i log. Le notifiche e-mail saranno inviate a tutti gli indirizzi e-mail configurati nel momento dell'invio della response.