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 D. Lgs. 7 marzo 2005, n. 82

ALLEGATO 4:

Processo di distribuzione dei segnali di variazione

Versione 1.0 del XX.XX.XXXX

Versione	Data	Tipologia modifica
1.0	XX.XX.XXXX	Prima emissione.

Indice

1. Introduzione

La **PDND Interoperabilità** consente agli **Erogatori** di **e-service** di inviare i **Segnali di Variazione** ai **Fruitori** per notificare variazioni apportate al dominio di informazioni di cui sono titolari.

I **Fruitori** interessati hanno così la possibilità di reagire a queste variazioni attivando i propri processi amministrativi all'interno dei loro domini di competenza.

La **PDND Interoperabilità** consente ai **Fruitori** di recuperare i **Segnali di Variazione** relativi ai fatti o stati di loro interesse coerentemente alle richieste di fruizione e analisi del rischio sulla protezione dei dati personali già registrate sulla **PDND Interoperabilità**.

2. Definizioni

Per la descrizione dei termini utilizzati nel seguito di questo documento, si rimanda al capitolo dedicato e contenuto nelle *"Linee Guida sull'infrastruttura tecnologica della Piattaforma Digitale Nazionale Dati per l'interoperabilità dei sistemi informativi e delle basi di dati"* di cui il presente documento è Allegato.

2.1. Segnale di Variazione

Evento tramite il quale un **Aderente** comunica alla **Piattaforma interoperabilità PDND** l'avvenuta variazione di stati e/o fatti conosciuti all'interno del dominio di dati/informazioni di cui lo stesso è titolare.

2.2. Produttore

È un **Aderente** che comunica ai **Consumatori**, per il tramite della **Piattaforma interoperabilità PDND**, i **Segnali di Variazione** in modo da rendere note le variazioni degli stati e fatti conosciuti all'interno del dominio di dati/informazioni di cui lo stesso è titolare.

2.3. Consumatore

È un **Aderente** che recupera dalla **Piattaforma interoperabilità PDND** i **Segnali di Variazione** in modo da essere consapevole delle variazioni degli stati e fatti di sua competenza e interesse.

2.4. Funzione di hashing

Una funzione crittografica di hashing (in breve funzione di hashing) è caratterizzata dalle seguenti proprietà:

- deve essere assicurata l'univocità dell'associazione input/output, ovvero è estremamente improbabile che due differenti input, pur essendo simili, abbiano lo stesso valore di hashing;
- deve essere deterministica, cioè lo stesso input si traduce sempre nello stesso hashing;
- deve essere quasi impossibile generare un input dal suo valore hashing se non provando tutti gli input possibili.

2.5. Funzione di hashing con seme

Una funzione di hashing con seme è un tipo di funzione di hashing che richiede in input un valore aggiuntivo chiamato "seme", utilizzato come parametro.

L'aggiunta del seme rende più sicuro il processo di hashing in quanto rende più difficile per un potenziale attaccante prevedere o trovare un pattern nei risultati di hashing, migliorando la resistenza ai tentativi di attacco.

2.6. Identificatore pseudonimizzato

Un identificatore pseudonimizzato è un dato ottenuto attraverso l'applicazione di una funzione di hashing su un identificatore originale, rendendo così difficile l'associazione diretta con la persona fisica corrispondente senza l'uso di informazioni aggiuntive.

3. Riferimenti e sigle

3.1. 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.

3.2. 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]
[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]

3.3. Linee guida di primario riferimento

Di seguito sono elencate le linee guida emesse da **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

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

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

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

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

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

4. Descrizione del processo

L'**Infrastruttura interoperabilità PDND** concretizza la distribuzione dei **Segnali di Variazione** applicando il paradigma **Fruitore - Erogatore** già descritto nelle presenti Linee Guida.

L'utilizzo del servizio di invio dei segnali è riservato agli **Erogatori** titolari di **e-service** con modalità di **erogazione ordinaria** pubblicati sul **Catalogo API** in stato attivo. In questo contesto, un **Erogatore** viene definito **Produttore**.

L'**Infrastruttura interoperabilità PDND** offre un canale in modalità *push*, detto **servizio di deposito dei segnali**, con cui un **Produttore PUÒ** inoltrare dei **Segnali di Variazione** tramite i quali notifica le variazioni nel proprio dominio e che sono legati agli **e-service** già pubblicati sul **Catalogo API**.

L'utilizzo del **servizio di deposito dei segnali** riferiti ad uno specifico **e-service** è riservato ai **Produttori** per i quali:

- il **Produttore** è titolare dell'**e-service** in oggetto;
- l'**e-service** in oggetto è pubblicato sul **Catalogo API** da parte dell'**Erogatore** e la distribuzione dei segnali di variazione è attività dallo stesso **Erogatore**;
- l'**Erogatore** dell'**e-service** in oggetto deve assicurare la possibilità di recuperare la funzione di hashing e/o il seme afferente allo stesso.

Un **Aderente** per cui sussistano le condizioni di cui ai precedenti punti **PUÒ** attivare l'utilizzo del **servizio di deposito dei segnali** assumendosi la responsabilità dei dati e informazioni inviate per il tramite quest'ultimo.

Un **Erogatore PUÒ** abilitare la funzionalità di distribuzione dei segnali per i propri **e-service** in **Erogazione Ordinaria** pubblicati sul **Catalogo API**. Nel caso in cui un **Erogatore** abiliti la funzionalità di distribuzione dei segnali per un suo **e-service DEVE** utilizzare il **servizio di deposito dei segnali**, reso disponibile dall'**Infrastruttura interoperabilità PDND**, per inoltrare i **Segnali di Variazione** per ogni modifica di uno o più dei dati che caratterizzano l'**e-service** stesso, indipendentemente dai **Produttori** che utilizzano la funzionalità di distribuzione dei segnali.

Analogamente, l'**Infrastruttura interoperabilità PDND** offre un canale in modalità *pull*, detto **servizio di recupero dei segnali**, attraverso il quale un **Produttore** di un **e-service PUÒ** recuperare i **Segnali di Variazione** legati ai cambiamenti di stati o fatti occorsi all'interno del dominio di conoscenza del **Produttore**.

Il modello prevede che il **Consumatore** dell'**e-service** di **recupero dei segnali DEVE** richiedere periodicamente (*polling*) alla **Infrastruttura interoperabilità PDND** i **Segnali di Variazione** di suo interesse con una frequenza massima definita dal **Gestore**.

L'utilizzo del **servizio di recupero dei segnali** riferito a uno specifico **e-service** è riservato ai **Consumatori** per i quali:

- il **Consumatore** possiede almeno una **Finalità** attiva per l'**e-service** in oggetto;
- l'**e-service** in oggetto è pubblicato sul **Catalogo API** da parte dell'**Erogatore**, e la distribuzione dei segnali di variazione è attività dallo stesso **Erogatore**.

Un **Aderente** per cui sussistano le condizioni di cui ai precedenti punti **PUO'** attivare l'utilizzo del **servizio di recupero dei segnali** assumendosi la responsabilità dei dati e informazioni ricevute tramite quest'ultimo.

Un **Fruitore PUÒ** usufruire della funzionalità di distribuzione dei segnali per gli **e-service** resi disponibili **dagli Erogatori** che hanno reso disponibile la suddetta funzione sul **Catalogo API**. Nel caso in cui un

Fruitore decide di usufruirne **DEVE** utilizzare il **servizio di recupero dei segnali**, reso disponibile dall'**Infrastruttura interoperabilità PDND**, per recuperare i **Segnali di Variazione** relativi all'**e-service** stesso.

La **PDND Interoperabilità** rende disponibili gli **e-service**:

- **servizio di deposito dei segnali**, per permettere ai **Produttori** di inoltrare i **segnali di variazione** relativi ai dati e informazioni relativamente ai propri **e-service** pubblicati sul **Catalogo API**;
- **servizio di recupero dei segnali**, per permettere ai Consumatori di recuperare i **segnali di variazione** relativa ai soggetti per cui hanno in essere uno specifico procedimento.

Nel caso in cui i **Segnali** siano riferiti a dati o fatti relativi a persone fisiche o comunque ad informazioni riservate, la **Infrastruttura interoperabilità PDND DEVE** garantire il rispetto dei principi previsti dalla normativa sulla protezione dei dati personali. Per questo motivo, i **Segnali** di questa fattispecie **DEVONO** contenere identificativi pseudonimizzati con funzioni di hashing con seme. In tale contesto, la **Infrastruttura interoperabilità PDND** agevola e regola le modalità con cui i **Produttori** e i **Consumatori** condividono le misure tecniche di pseudonimizzazione.

L'interfaccia degli **e-service** di **deposito e recupero** dei **Segnali di Variazione** viene definita dal **Gestore** all'interno della documentazione tecnica della **Infrastruttura interoperabilità PDND** e **DEVE**:

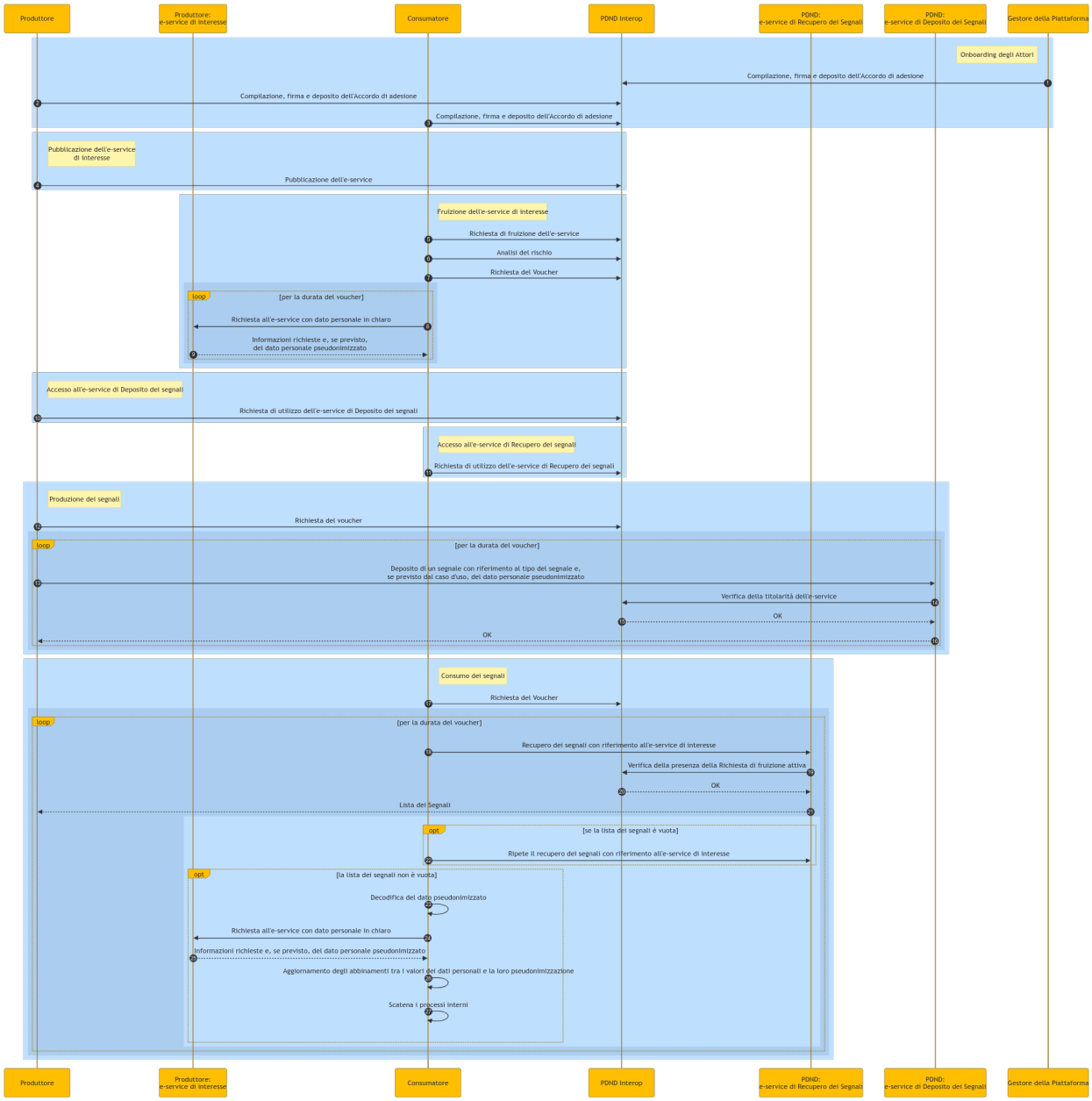
- consentire l'applicazione di quanto indicato all' ALLEGATO 3: STANDARD E DETTAGLI TECNICI UTILIZZATI PER LA FRUIZIONE DEI VOUCHER DI AUTORIZZAZIONE delle presenti **Linee Guida** in relazione all'utilizzo del **Voucher** rilasciato dalla **Infrastruttura interoperabilità PDND**;
- permettere l'identificazione dell'**e-service** a cui il singolo **Segnale di Variazione** è riferito;
- contenere, se previsto dal caso d'uso, il dato pseudonimizzato a cui il **Segnale di Variazione** è riferito ad una o più persona fisica o comunque contiene informazioni riservate;
- permettere l'identificazione della **Classe dei Segnali** di appartenenza dell'evento legato al segnale.

Nel diagramma di sequenza riportato di seguito si illustra il flusso operativo di scambio dei segnali tramite l'**Infrastruttura interoperabilità PDND** per cui si identificano le principali attività:

- *onboarding degli attori coinvolti*: il **Produttore** e il **Consumatore** devono aderire alla **Infrastruttura interoperabilità PDND**, così da poter effettuare le attività di pubblicazione degli **e-service** sul **Catalogo API**, richiedere la fruizione degli **e-service**, ottenere i **Voucher**;
- *pubblicazione dell'e-service di interesse*: il **Produttore**, nel ruolo di **Erogatore**, pubblica sul **Catalogo API** l'**e-service** dedicato alla distribuzione della conoscenza dei fatti di cui è titolare, specificando l'abilitazione della distribuzione dei segnali di variazione degli stessi fatti;
- *fruizione dell'e-service di interesse*: il **Consumatore**, nel ruolo di **Fruitore**, individua come di suo interesse l'**e-service** pubblicato sul **Catalogo API** al punto precedente e procede sulla **Infrastruttura interoperabilità PDND** alla richiesta di fruizione e quindi all'analisi del rischio. Il **Consumatore** da ora può interrogare l'**e-service**;
- *iscrizione all'e-service di distribuzione dei segnali*: il **Produttore** procede sulla **Infrastruttura interoperabilità PDND** alla richiesta di utilizzare l'**e-service** reso disponibile dalla stessa dedicato al **deposito dei segnali**;
- *iscrizione all'e-service di recupero dei segnali*: il **Consumatore** procede sulla **Infrastruttura interoperabilità PDND** alla richiesta utilizzare l'**e-service** reso disponibile dalla stessa dedicato al **recupero dei segnali**;
- *produzione segnali*: il **Produttore** richiede alla **Infrastruttura interoperabilità PDND** un **Voucher** di accesso all'**e-service** di **deposito dei segnali**. Il **Produttore** invoca l'**e-service** utilizzando il

Voucher e riportando i riferimenti dell'evento di variazione nel **Segnale** e l'**e-service** di interesse a cui lo stesso afferisce. Il **Gestore** deve verificare l'autenticità del **Voucher**, la legittimità dell'accesso all'**e-service** di deposito e confermare la titolarità del **Produttore** al **e-service** di interesse. Solo dopo queste verifiche il **Gestore DEVE** accettare la richiesta del **Produttore** e procedere con la distribuzione del segnale. Il **Segnale** depositato, nel caso sia legato a persone fisiche, non deve riportare in chiaro le informazioni sulle persone fisiche coinvolte, bensì deve trasferire identità pseudonimizzate tramite gli algoritmi condivisi dal **Produttore** con il **Consumatore** dei **Segnali**;

- *consumo dei segnali*: il **Consumatore** richiede periodicamente alla **Infrastruttura interoperabilità PDND** un **Voucher** di accesso all'**e-service** di **recupero dei segnali**. Il **Consumatore** invoca l'e-service utilizzando il **Voucher** e dichiarando l'**e-service** d'interesse per il quale vuole raccogliere i **Segnali**. Il **Gestore DEVE** verificare l'autenticità del **Voucher**, la legittimità dell'accesso al servizio di recupero e confermare la legittimità dell'accesso del **Consumatore** all'**e-service** di interesse. Solo dopo queste verifiche il **Gestore DEVE** accettare la richiesta del **Consumatore** e dare seguito al recupero dei segnali relativi all'**e-service** di interesse. I segnali recuperati, nel caso siano legati a persone fisiche, non riportano in chiaro le persone fisiche coinvolte, ma il **Consumatore** può determinarle tramite gli algoritmi di pseudonimizzazione condivisi con il **Produttore**. Il **Consumatore**, determinata l'identità delle persone fisiche, stabilisce se invocare l'e-service di interesse per recuperati gli stati o fatti che riguardano le persone fisiche per cui sono stati generati tali **Segnali**.


Produttore
Produttore: e-service di interesse
Consumatore
PDND Interop
PDND: e-service di Recupero dei Segnali
PDND: e-service di Deposito dei Segnali
Gestore della Piattaforma
Onboarding degli Attori
1 Compilazione, firma e deposito dell'Accordo di adesione
2 Compilazione, firma e deposito dell'Accordo di adesione
3 Compilazione, firma e deposito dell'Accordo di adesione
Pubblicazione dell'e-service di interesse
4 Pubblicazione dell'e-service
Fruizione dell'e-service di interesse
5 Richiesta di fruizione dell'e-service
6 Analisi del rischio
7 Richiesta del Voucher
loop [per la durata del voucher]
8 Richiesta all'e-service con dato personale in chiaro
9 Informazioni richieste e, se previsto, del dato personale pseudonimizzato
Accesso all'e-service di Deposito dei segnali
10 Richiesta di utilizzo dell'e-service di Deposito dei segnali
Accesso all'e-service di Recupero dei segnali
11 Richiesta di utilizzo dell'e-service di Recupero dei segnali
Produzione dei segnali
12 Richiesta del voucher
loop [per la durata del voucher]
13 Deposito di un segnale con riferimento al tipo del segnale e, se previsto dal caso d'uso, del dato personale pseudonimizzato
14 Verifica della titolarità dell'e-service
15 OK
16 OK
Consumo dei segnali
17 Richiesta del Voucher
loop [per la durata del voucher]
18 Recupero dei segnali con riferimento all'e-service di interesse
19 Verifica della presenza della Richiesta di fruizione attiva
20 OK
21 Lista dei Segnali
opt [se la lista dei segnali è vuota]
22 Ripete il recupero dei segnali con riferimento all'e-service di interesse
opt [la lista dei segnali non è vuota]
23 Decodifica del dato pseudonimizzato
24 Richiesta all'e-service con dato personale in chiaro
25 Informazioni richieste e, se previsto, del dato personale pseudonimizzato
26 Aggiornamento degli abbinamenti tra i valori dei dati personali e la loro pseudonimizzazione
27 Scatena i processi interni

5. Classi di segnali

I segnali sono comunicazioni tra **Produttore** e **Consumatore** e **DEVONO** appartenere a categorie definite nella documentazione tecnica dal **Gestore**.

Si identificano da subito, oltre ai **Segnali di Variazione**, le seguenti categorie:

- **segnali legati al ciclo di vita di una entità**: fanno parte di questa categoria la creazione, la variazione o il raggiungimento di uno stato finale di una entità;
- **segnali di agevolazione delle comunicazioni tra Produttore e Consumatore**: fanno parte di questa categoria le comunicazioni che permettono al **Produttore** di allineare il **Consumatore** sulle modalità di pseudonimizzazione (funzione di hashing, seme, ...).

6. Disponibilità dei segnali

I **Segnali** sono disponibili al recupero entro un numero di ore dichiarato dal **Gestore** nella documentazione tecnica della stessa.

Il **Gestore PUÒ** rimuovere i **Segnali** che superano il periodo di cui al precedente capoverso: gli stessi **Segnali** non saranno più recuperabili tramite l'**e-service** che implementa il **servizio di recupero dei segnali**.

7. Riservatezza delle informazioni

Con le modalità esposte di seguito l'**Erogatore** soddisfa l'esigenza di non far mai conoscere le informazioni relative a persone fisiche alla **Infrastruttura interoperabilità PDND**.

I **Segnali** indicheranno tramite informazioni pseudonimizzate le persone fisiche cui si rivolgono. Solo il **Produttore** e i **Consumatori** che avranno la conoscenza necessaria potranno risalire all'identità delle persone fisiche afferenti alle informazioni pseudonimizzate. Tale conoscenza verrà indicata nella modalità di pseudonimizzazione definita e condivisa tra **Produttore** e i **Consumatori**.

Di seguito è esposta la modalità per dare seguito alla pseudonimizzazione.

Il **Produttore** nella definizione della modalità di pseudonimizzazione applicata **DEVE** considerare le indicazioni in materia di protezione dei dati personali consultabili sul sito web del Garante per la protezione dei dati personali[6] e quelle rese dall'Agenzia per la Cybersicurezza Nazionale[7].

7.1. Algoritmo di pseudonimizzazione condiviso

Il **Produttore DEVE** individuare sotto la propria responsabilità l'algoritmo di pseudonimizzazione con seme – tra quelli dichiarati all'interno della cornice di sicurezza definita dal **MoDI** – e dei parametri per la sua esecuzione (es. il **seme**). Nella selezione dell'algoritmo di pseudonimizzazione il **Produttore DEVE** assicurare la non invertibilità dello stesso. Il **Produttore** comunica al **Consumatore** la scelta dell'algoritmo di pseudonimizzazione e dei parametri per la sua esecuzione.

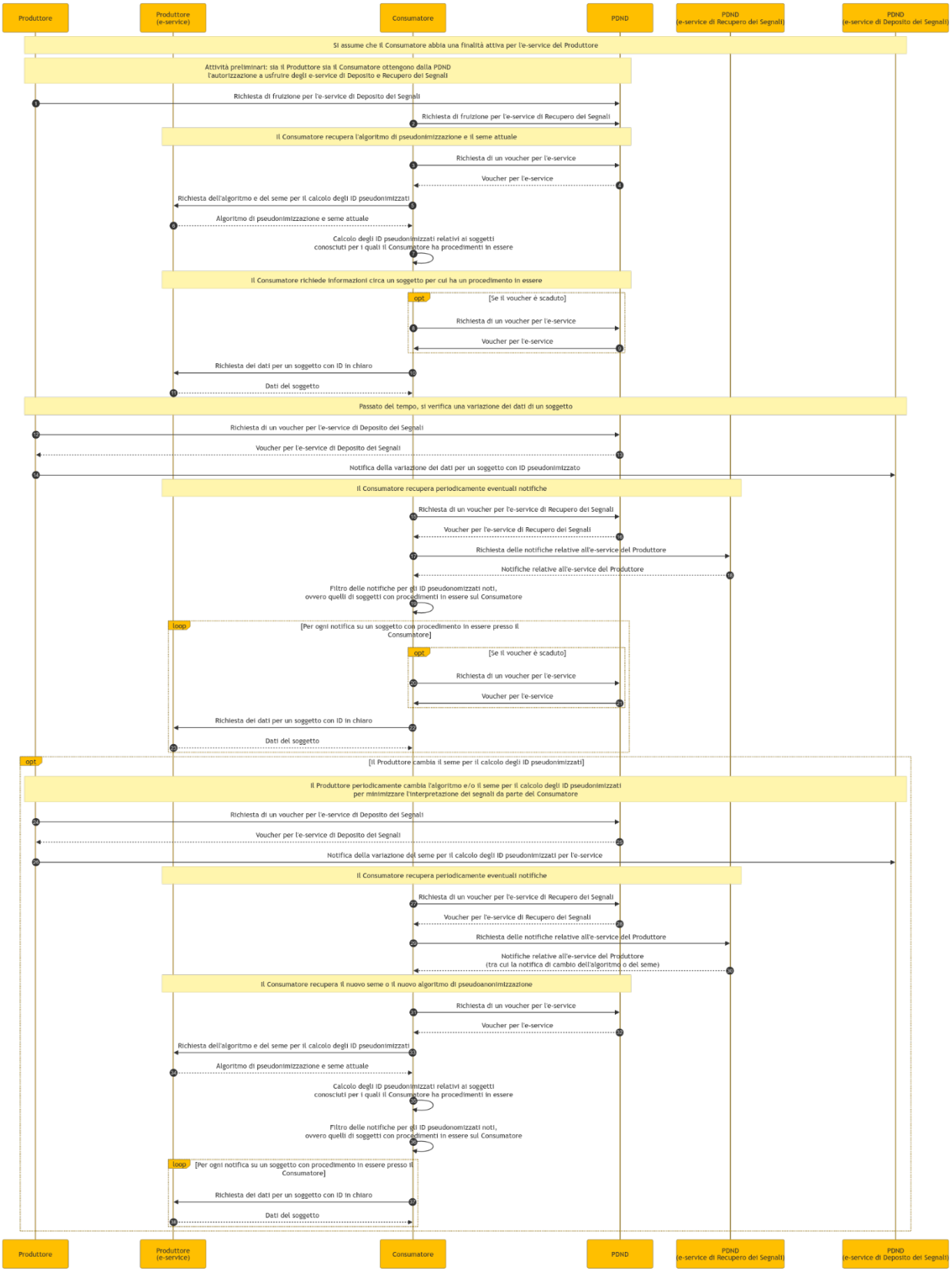
Il **Consumatore** deve mantenere riservate le informazioni ricevute dal **Produttore** e calcolare gli pseudonimi per i soli soggetti per cui esiste un procedimento amministrativo attivo che richiede il costante aggiornamento degli stati e dei fatti, al fine di interpretare le informazioni pseudonimizzate dei **Segnali** recuperati dalla **Piattaforma Interoperabilità PDND**.

Il **Produttore DEVE** assicurare la rotazione periodica dei parametri dell'algoritmo di pseudonimizzazione. La periodicità della modifica dei parametri è definita dal **Produttore** e **DEVE** essere proporzionale alla tipologia di dati personali o della riservatezza delle informazioni oggetto degli stati e dei fatti cui le variazioni possono riferirsi.

Il **Produttore** DEVE assicurare l'univocità del seme per l'applicazione dell'algoritmo di pseudonimizzazione relativamente ai singoli **e-service** pubblicati sul **Catalogo API** per cui è attivato la distribuzione dei segnali di variazione.

In quanto segue sono riportate alcune considerazioni che il **Produttore DOVREBBE** valutare nell'individuazione dell'algoritmo di pseudonimizzazione e nella gestione dei parametri dello stesso.

[6] https://www.garanteprivacy.it/temi/pseudonimizzazione
[7] https://www.acn.gov.it/portale/documents/20119/85999/ACN_LineeGuida_Hash.pdf/e1d36f5c-c75e-06b7-9c5f-aa535ed39b33?version=1.0&t=1704377457344&download=true


Produttore
Produttore (e-service)
Consumatore
PDND
PDND (e-service di Recupero dei Segnali)
PDND (e-service di Deposito dei Segnali)
Si assume che il Consumatore abbia una finalità attiva per l'e-service del Produttore
Attività preliminari: sia il Produttore sia il Consumatore ottengono dalla PDND l'autorizzazione a usfruire degli e-service di Deposito e Recupero dei Segnali
Richiesta di fruizione per l'e-service di Deposito dei Segnali
Richiesta di fruizione per l'e-service di Recupero dei Segnali
Il Consumatore recupera l'algoritmo di pseudonimizzazione e il seme attuale
Richiesta di un voucher per l'e-service
Voucher per l'e-service
Richiesta dell'algoritmo e del seme per il calcolo degli ID pseudonimizzati
Algoritmo di pseudonimizzazione e seme attuale
Calcolo degli ID pseudonimizzati relativi ai soggetti conosciuti per i quali il Consumatore ha procedimenti in essere
Il Consumatore richiede informazioni circa un soggetto per cui ha un procedimento in essere
opt
[Se il voucher è scaduto]
Richiesta di un voucher per l'e-service
Voucher per l'e-service
Richiesta dei dati per un soggetto con ID in chiaro
Dati del soggetto
Passato del tempo, si verifica una variazione dei dati di un soggetto
Richiesta di un voucher per l'e-service di Deposito dei Segnali
Voucher per l'e-service di Deposito dei Segnali
Notifica della variazione dei dati per un soggetto con ID pseudonimizzato
Il Consumatore recupera periodicamente eventuali notifiche
Richiesta di un voucher per l'e-service di Recupero dei Segnali
Voucher per l'e-service di Recupero dei Segnali
Richiesta delle notifiche relative all'e-service del Produttore
Notifiche relative all'e-service del Produttore
Filtro delle notifiche per gli ID pseudonimizzati noti, ovvero quelli di soggetti con procedimenti in essere sul Consumatore
loop
[Per ogni notifica su un soggetto con procedimento in essere presso il Consumatore]
opt
[Se il voucher è scaduto]
Richiesta di un voucher per l'e-service
Voucher per l'e-service
Richiesta dei dati per un soggetto con ID in chiaro
Dati del soggetto
opt
[Il Produttore cambia il seme per il calcolo degli ID pseudonimizzati]
Il Produttore periodicamente cambia l'algoritmo e/o il seme per il calcolo degli ID pseudonimizzati per minimizzare l'interpretazione dei segnali da parte del Consumatore
Richiesta di un voucher per l'e-service di Deposito dei Segnali
Voucher per l'e-service di Deposito dei Segnali
Notifica della variazione del seme per il calcolo degli ID pseudonimizzati per l'e-service
Il Consumatore recupera periodicamente eventuali notifiche
Richiesta di un voucher per l'e-service di Recupero dei Segnali
Voucher per l'e-service di Recupero dei Segnali
Richiesta delle notifiche relative all'e-service del Produttore
Notifiche relative all'e-service del Produttore (tra cui la notifica di cambio dell'algoritmo o del seme)
Il Consumatore recupera il nuovo seme o il nuovo algoritmo di pseudoanonimizzazione
Richiesta di un voucher per l'e-service
Voucher per l'e-service
Richiesta dell'algoritmo e del seme per il calcolo degli ID pseudonimizzati
Algoritmo di pseudonimizzazione e seme attuale
Calcolo degli ID pseudonimizzati relativi ai soggetti conosciuti per i quali il Consumatore ha procedimenti in essere
Filtro delle notifiche per gli ID pseudonimizzati noti, ovvero quelli di soggetti con procedimenti in essere sul Consumatore
loop
[Per ogni notifica su un soggetto con procedimento in essere presso il Consumatore]
Richiesta dei dati per un soggetto con ID in chiaro
Dati del soggetto
Produttore
Produttore (e-service)
Consumatore
PDND
PDND (e-service di Recupero dei Segnali)
PDND (e-service di Deposito dei Segnali)

7.1.1. Algoritmo di pseudonimizzazione

Gli algoritmi di pseudonimizzazione raccomandati, o funzioni crittografiche di hashing, sono:

- SHA-2: insieme di funzioni crittografiche di hashing progettato dalla NSA (National Security Agency) per migliorare le proprietà di sicurezza del predecessore SHA-1
  - SHA-256
  - SHA-512/256
  - SHA-384
  - SHA-512
- SHA-3: insieme di funzioni crittografiche di hashing progettato dal NIST (National Institute of Standards and Technology) per migliorare le proprietà di sicurezza del predecessore SHA-2:
  - SHA3-256
  - SHA3-384
  - SHA3-512
  - SHAKE128
  - SHAKE256

Per completezza, in tabella sono riassunte le specifiche delle funzioni crittografiche di hash raccomandate allo stato[8].

Algoritmo	Versione	Digest (bit)	Stato (bit)	Blocchi (bit)	Round	Sicurezza (bit)	Prestazioni (cpb)
SHA-2	SHA-256	256	256	512	64	128	96.00
	SHA-512/256	256	512	1024	80		141.00
	SHA-384	384				192	135.00
	SHA-512	512				256	141.00
SHA-3	SHA3-256	256	1600	1088	24	128	158.75
	SHA3-384	384		832		192	163.88
	SHA3-512	512		576		256	163.75
	SHAKE128	n		1344		d/2	166.12
	SHAKE256	n		1088		d/2	148.50

7.1.2. Parametri dell'algoritmo di pseudonimizzazione

Gli algoritmi di pseudonimizzazione raccomandati al precedente paragrafo **DEVONO** essere rinforzati con l'utilizzo di un secret.

In merito al secret di raccomanda di:

- effettuare una rotazione dello stesso ad intervalli di tempo regolari, di seguito indichiamo con `rs` il numero di giorni della rotazione del secreto;
- assicurare un livello di entropia dello stesso consono, di seguito indichiamo con `be` il numero di caratteri del secret (assunto come set di caratteri `[A-Za-z0-9]`).

[8] Il **Gestore**, informata AgID, **DEVE** variare l'elenco delle funzioni crittografiche di hash all'interno della documentazione tecnica in ragione dei rilievi di merito sollevati dall'Agenzia per la Cybersicurezza Nazionale. I **Produttori** e i **Consumatori DEVONO** assicurare, sotto la propria responsabilità, l'immediato aggiornamento delle funzioni crittografiche di hash riportate nella documentazione tecnica predisposta dal **Gestore**.

In quanto segue si riportano della raccomandazione per **Produttore** in considerazione alla tipologia dei dati oggetto degli e-service.

Tipologia dei dati	Versione algoritmo	rs	be
Dati che permettono l'identificazione indiretta della persona fisica	Nessuna raccomandazione specifica		
Dati che permettono l'identificazione diretta della persona fisica	Nessuna raccomandazione specifica	<= 120 gg	>= 16 caratteri
Dati sensibili della persona fisica (origine razziale o etnica, convinzioni religiose, filosofiche, opinioni politiche, appartenenza sindacale, relativi alla salute o alla vita sessuale)	• SHA-384 • SHA-512 • SHA3-384 • SHA3-512 • SHAKE128 • SHAKE256	<= 80 gg	>= 32 caratteri
Dati giudiziari della persona fisica (esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale)	• SHA-512 • SHA3-512 • SHAKE128 • SHAKE256	<= 60 gg	>= 64 caratteri
Altri dati della persona fisica (relativi alle comunicazioni elettroniche e che consentono la geolocalizzazione)	Nessuna raccomandazione specifica	<= 120 gg	>= 16 caratteri

8. Valutazione tecnica per l'utilizzo della distribuzione dei segnali di variazione

I **Produttori** e **Consumatori** del servizio di distribuzione dei segnali di variazione reso disponibile dalla **Infrastruttura interoperabilità PDND DEVONO** effettuare una valutazione tecnica in merito all'opportunità di utilizzare lo stesso.

I **Produttori**, relativamente all'abilitazione del **servizio di deposito dei segnali** per un suo specifico **e-service** pubblicato sul **Catalogo API DEVONO**:

- determinare l'algoritmo di pseudonimizzazione da utilizzare in considerazione della specificità dei dati veicolati dall'**e-service**;
- valutare gli oneri derivanti dall'applicazione dell'algoritmo di pseudonimizzazione individuato e, nondimeno, dalla gestione della comunicazione ai **Consumatori** per permettere a questi ultimi di interpretare i dati pseudonimizzazione veicolati nei segnali.

I **Consumatori**, relativamente all'abilitazione del **servizio di recupero dei segnali** per un **e-service** pubblicato da un **Produttore** con abilitazione della distribuzione dei segnali di variazione **DEVONO**:

- considerare i costi derivanti dall'interpretazione dei dati pseudonimizzati in relazione algoritmo di pseudonimizzazione individuato dal **Produttore**;
- valutare l'opportunità di usufruire della distribuzione dei segnali di variazione in relazione a:
    - numero medio di cittadini gestiti per la tipologia di procedimento amministrativi avviati;
    - durata media dei procedimenti amministrativi avviati;
    - indice di variabilità dei dati dei soggetti ottenuti tramite l'**e-service** del **Produttore**;
    - numero medio di utilizzi dei dati ottenuti tramite l'**e-service** del **Produttore**.