

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 4:

Processo di distribuzione dei segnali di variazione



Versione	Data	Tipologia modifica
1.0	30.07.2024	Prima emissione.

In consultazione pubblica



Indice

1. Introduzione	1
2. Definizioni	2
2.1. Segnale di variazione	2
2.2. Produttore di segnali (Produttore)	2
2.3. Consumatore di segnali (Consumatore)	2
2.4. Funzione di hashing	2
2.5. Funzione di hashing con seme	2
2.6. Identificatore pseudonimizzato	2
3. Riferimenti e sigle	3
3.1. Note di lettura del documento	3
3.2. Standard di riferimento	3
3.3. Linee guida di primario riferimento	3
4. Descrizione del processo	4
5. Classi di segnali	8
6. Disponibilità dei segnali	9
7. Riservatezza delle informazioni	10
7.1. Algoritmo di pseudonimizzazione condiviso	10
7.1.1. Algoritmo di pseudonimizzazione	12
7.1.2. Parametri dell'algoritmo di pseudonimizzazione	12
8. Valutazione tecnica per l'utilizzo della distribuzione dei segnali di variazione	14

1. Introduzione

La **PDND Interoperabilità** consente agli erogatori di **e-service** di inviare segnali agli **Aderenti** 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 relativi ai fatti o stati di loro interesse coerentemente agli **Accordi di Adesione** e alle richieste di fruizione già registrate sulla **PDND Interoperabilità**.

In consultazione pubblica

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 di segnali (Produttore)

È un **Aderente** che comunica ai consumatori di segnali, per il tramite della **Piattaforma interoperabilità PDND**, dei 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 di segnali (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 l'individuo 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

La **PDND Interoperabilità** 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** pubblicati sul **Catalogo API** in stato attivo. In questo contesto, un **Erogatore** viene definito **Produttore di segnali** (in breve **Produttore**).

PDND Interoperabilità offre un canale in modalità *push*, detto **servizio di deposito dei segnali**, con cui un **Produttore** può inoltrare dei messaggi tramite i quali notifica le variazioni nel proprio dominio e che sono legati agli **e-service** già pubblicati sul **Catalogo API**: questi messaggi sono denominati **Segnali**.

Analogamente, **PDND Interoperabilità** offre un canale in modalità *pull*, detto **servizio di recupero dei segnali**, attraverso il quale un **Fruitore** di un **e-service**, in questo contesto definito **Consumatore di segnali** (in breve **Consumatore**), può recuperare i **Segnali** legati ai cambiamenti di stati o fatti occorsi all'interno del dominio di conoscenza del **Produttore**.

L'utilizzo del **servizio di recupero dei segnali** riferiti ad 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.

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 **PUO'** attivare l'utilizzo del **servizio di deposito dei segnali** assumendosi la responsabilità dei dati e informazioni inviate per il tramite quest'ultimo.

In questo scenario la **PDND Interoperabilità** assume il ruolo di **Erogatore** di:

- un **e-service** dedicato ai **Produttori**, quale implementazione del **servizio di deposito dei segnali**. Nell'utilizzo di questo **e-service**, i **Produttori** agiranno come **Fruitori** della **PDND Interoperabilità**;
- un **e-service** dedicato ai **Consumatori**, quale implementazione del **servizio di recupero dei segnali**. Nell'utilizzo di questo **e-service**, i **Consumatori** agiranno come **Fruitori** della **PDND Interoperabilità**.

Ne consegue che:

- il **servizio di deposito dei segnali** è pubblicato sul **Catalogo API** come **e-service** erogato da **PDND Interoperabilità**;

- il **servizio di recupero dei segnali** è pubblicato sul **Catalogo API** come **e-service** erogato da **PDND Interoperabilità**;
- l'accesso agli **e-service** di **deposito e recupero dei segnali** è subordinato alla richiesta di fruizione agli **e-service** da parte dell'**Aderente** che intende fruirne come **Produttore** o **Consumatore di Segnali**;
- l'impiego di questi **e-service** è subordinato alla compilazione di un'analisi del rischio.

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

Nel caso in cui i **Segnali** siano riferiti a dati o fatti relativi a persone fisiche o comunque ad informazioni riservate, la **PDND Interoperabilità** **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 **PDND Interoperabilità** agevola e regola le modalità con cui i **Produttori** e i **Consumatori** condividono le misure tecniche di pseudonimizzazione.

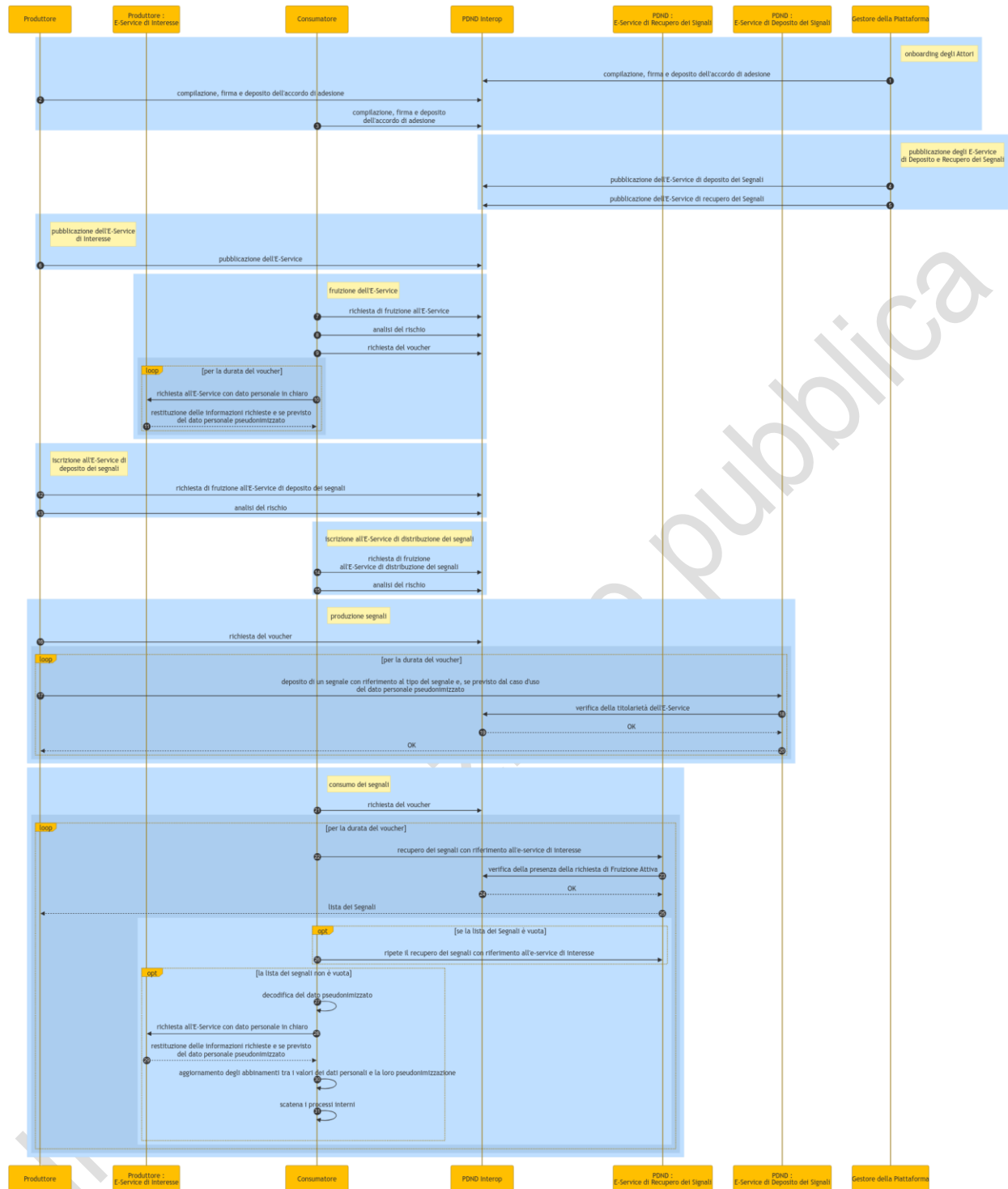
L'interfaccia degli **e-service** di **deposito e recupero dei Segnali** viene definita dal **Gestore** all'interno della documentazione tecnica della **PDND Interoperabilità** e **DEVE**:

- 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 da **PDND Interoperabilità**;
- permettere l'identificazione dell'**e-service** a cui il singolo **Segnale** è riferito;
- contenere, se previsto dal caso d'uso, il dato pseudonimizzato a cui il **Segnale** 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 **PDND Interoperabilità** per cui si identificano le principali attività:

- *onboarding degli attori coinvolti*: il **Produttore**, il **Consumatore** e il **Gestore** della **PDND Interoperabilità** devono aderire alla **PDND Interoperabilità**, così da poter effettuare le attività di pubblicazione degli **e-service** sul **Catalogo API**, richiedere la fruizione degli **e-service**, ottenere i **Voucher**;
- *pubblicazione degli e-service di deposito e recupero dei Segnali*: il **Gestore** pubblica sul **Catalogo API** gli **e-service** dedicati al **servizio di deposito dei segnali** e al **servizio di recupero dei segnali**;
- *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 **PDND Interoperabilità** 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**, nel ruolo di **Fruitore**, procede sulla **PDND Interoperabilità** alla richiesta di fruizione e alla selezione dell'analisi del rischio per l'**e-service** pubblicato sul **Catalogo API** dal **Gestore** dedicato al **deposito dei segnali**;

- *iscrizione all'e-service di distribuzione dei segnali*: il **Consumatore**, nel ruolo di **Fruitore**, procede sulla **PDND Interoperabilità** alla richiesta di fruizione e poi all'analisi del rischio dell'**e-service** pubblicato sul **Catalogo API** dal **Gestore della Piattaforma** e dedicato al **recupero dei segnali**;
- *produzione segnali*: il **Produttore** richiede alla **PDND Interoperabilità** 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 **PDND Interoperabilità** 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 recuperare gli stati o fatti che riguardano le persone fisiche per cui sono stati generati tali **Segnali**.



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:

- **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**.

In consultazione pubblica

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 **Piattaforma 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 sintetizzata nella modalità di pseudonimizzazione e condivisa tra **Produttore** e i **Consumatori**.

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

Il **Produttore** nella selezione della modalità di pseudonimizzazione applicata DEVE considerare le indicazioni in materia date dal Garante per la Protezione dei dati Personali⁶ e dall'Agenzia per la Cybersicurezza Nazionale⁷.

7.1. Algoritmo di pseudonimizzazione condiviso

Il **Produttore individua** 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**.

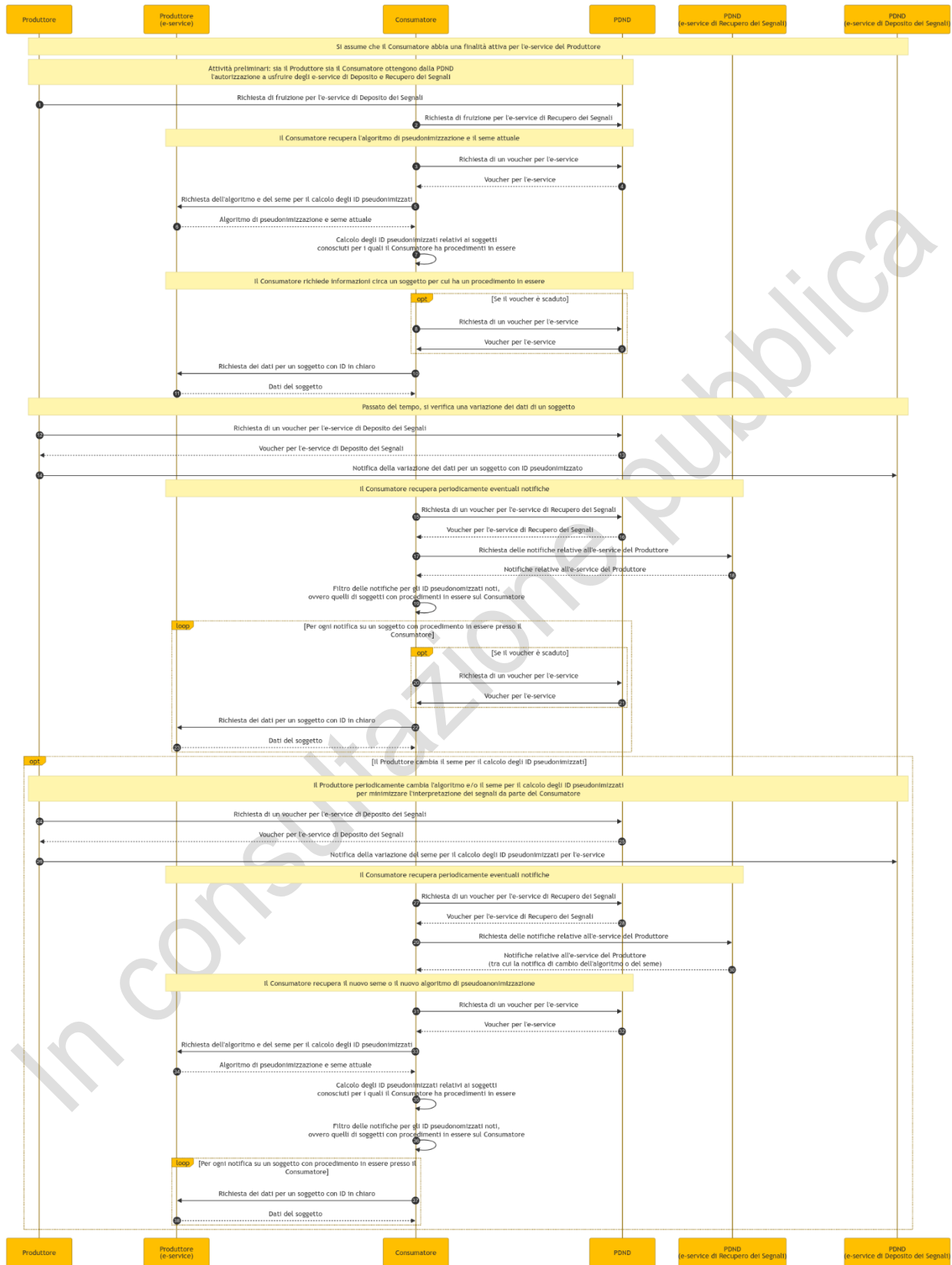
Il **Produttore DEVE** assicurare la rotazione periodica dei parametri dell'algoritmo di pseudonimizzazione. La periodicità della modifica dei parametri è definita dal **Produttore** e **DEVE** essere proporzionale alla tipologia di dati personali o della riservatezza delle informazioni oggetto degli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



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 stato⁸.

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 si raccomanda di:

- effettuare una rotazione dello stesso ad intervalli di tempo regolari, di seguito indichiamo con r_s il numero di giorni della rotazione del secreto;
- assicurare un livello di entropia dello stesso consono, di seguito indichiamo con b_e 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 **Piattaforma 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 pseudonimizzazione 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**.