

**ALLEGATO 4.3 AL CAPITOLATO TECNICO**

**SPECIFICHE TECNICHE PER IL MODELLO D'INTEROPERABILITÀ CON IL POSTALIZZATORE**

## Indice

<b>1. Introduzione .....</b>	<b>3</b>
<b>2. Definizione dell'esigenza .....</b>	<b>4</b>
<b>3. Flussi e funzionalità .....</b>	<b>5</b>
<b>4. Sistema informatico del fornitore .....</b>	<b>7</b>
<b>5. Strutture dati .....</b>	<b>8</b>
<b>6. Sicurezza e modalità di connessione .....</b>	<b>11</b>

## 1. Introduzione

Il presente documento riporta:

1. il dettaglio dei flussi già identificati nell'ambito dello schema di interoperabilità applicativa, con evidenza della responsabilità (Ministero o Fornitore), delle modalità tecniche e dei requisiti che dovrà supportare il sistema Fornitore (vedi paragrafo 3 Flussi e Funzionalità);
2. le informazioni (strutture dati) oggetto dei flussi di scambio, tra il sistema del Fornitore ed i sistemi di registro del Ministero (vedi paragrafo 5 Strutture Dati);
3. i requisiti di sicurezza richiesti al Fornitore (vedi paragrafo 5 Sicurezza e modalità di connessione).

## 2. Definizione dell'esigenza

L'esigenza dell'Amministrazione si focalizza sulla realizzazione un flusso informativo tra UNEP, il Fornitore e Uffici Giudiziari attraverso l'uso di dati strutturati secondo opportuni formati e modelli di interoperabilità applicativa A2A (*application to application*).

Di seguito uno schema dei flussi applicativi che saranno dettagliati nel prossimo capitolo. Si precisa che i flussi "richiestaNotifica" e "relataNotifica" sono a carico dell'Amministrazione e, pertanto, sono esclusi dal perimetro della fornitura descritta nel presente documento.

L'interazione tra il sistema applicativo del Fornitore e i sistemi del dominio Giustizia è prevista tramite l'utilizzo di API (Application Programming Interface). Lo stile architetturale di sviluppo delle API potrà seguire il paradigma REST o SOAP mentre il pattern di sicurezza deve essere in linea con gli standard di sicurezza definiti dall'Amministrazione (Rif § 6 del presente documento).

I dati relativi alle richieste di notificazione (riepilogati nelle c.d. distinte) saranno inviati dal GSU (associati ai cronologici dei vari registri) al sistema informatico del Fornitore ai fini della preparazione delle buste e delle cartoline di esito. Al termine dell'attività di lavorazione della distinta (attribuzione dei numeri di raccomandata, calcolo spese postali, ...), il Fornitore provvederà ad arricchire i dati ricevuti dal GSU con i numeri di raccomandata ed inviare dette informazioni al GSU stesso.

Gli esiti dell'attività di notificazione completata dal Fornitore dovranno essere organizzati in informazioni strutturate restituite ai sistemi civili e penali di gestione dei registri degli Uffici Giudiziari. I dati associati agli esiti della notificazione devono permettere di individuare in maniera univoca il fascicolo di pertinenza e devono contenere tutti i dettagli informativi relativi all'attività svolta dal Fornitore.

Per quanto riguarda le cartoline attestanti l'esito della notificazione, il Fornitore dovrà organizzare un sistema di conservazione e consultazione delle copie per immagine dei supporti cartacei. Le copie per immagine dovranno rispettare quanto disposto dalle "Linee Guida per la formazione, gestione e conservazione del documento informatico" (AgID) ed essere consultabili e ricercabili dal personale degli uffici giudiziari tramite numero di raccomandata o numero procedimento (Ufficio, Registro, numero RG, anno RG).

Al soggetto Fornitore viene richiesto anche di mettere a disposizione dell'Amministrazione un sistema informatico per la consultazione delle informazioni e dei dati utili per l'esecuzione delle attività giudiziarie, nonché il tracciamento dei vari passaggi delle raccomandate, che soddisfi i requisiti (funzionali e non) riportati nel seguito del presente documento. Tutti i dati gestiti dal sistema in parola saranno di proprietà dell'Amministrazione. I costi dell'infrastruttura e della sua gestione sono interamente a carico del fornitore.

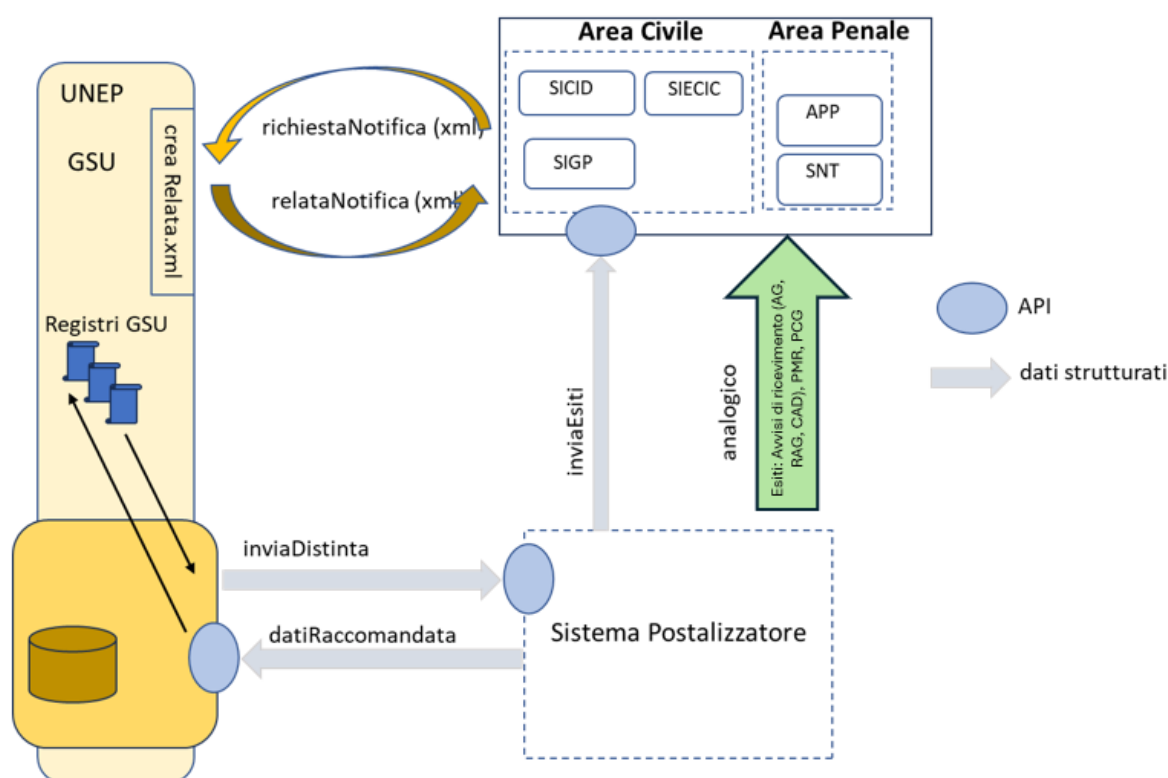


Figura 1: Schema flussi applicativi

### 3. Flussi e funzionalità

Si riporta di seguito una descrizione di maggior dettaglio dei flussi (sotto forma di sequence diagram) e delle principali funzionalità proposte per la realizzazione di quanto descritto nel precedente capitolo.

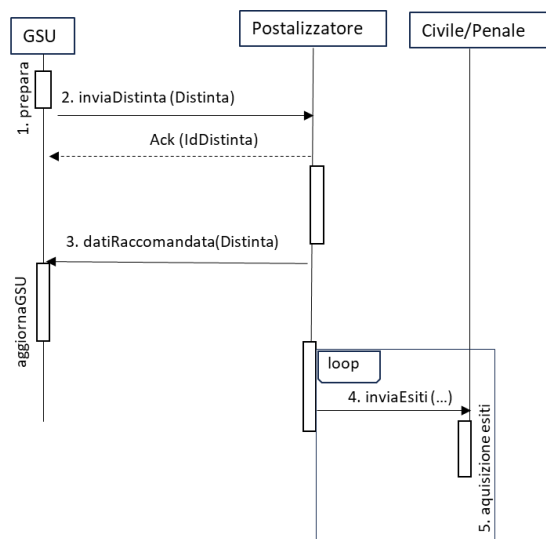


Figura 2: Diagramma interazioni tra sistemi

Per ogni attività è indicato il soggetto a carico del quale si pone la realizzazione. Gli interventi a carico del Fornitore ed oggetto della gara sono riportati in *corsivo*.

**a. Identificazione degli atti da consegnare al Fornitore per la notifica (Responsabile: Ministero della Giustizia)**

Il sistema GSU individua i dati specifici degli atti giudiziari da notificare che saranno inoltrati al Fornitore aggiudicatario e al FSU. L'individuazione avverrà tramite indicazione di numero cronologico, numero di registro e qualsiasi altra informazione utile. Per ogni atto dovranno essere presenti tutti i dati di dettaglio descrittivi dell'atto e tutti i singoli destinatari: il sistema GSU memorizza, quindi, tutte le informazioni utili per la singola notificazione.

Il sistema raggrupperà le notificazioni individuate dall'operatore GSU in unità logiche (distinta degli AAGG e delle RAG) caratterizzate da un identificativo univoco (IdUnivoco).

**b. Ricezione delle distinte da parte del Fornitore (Responsabile: Fornitore)**

Il sistema GSU invierà i dati strutturati che formano le 'distinte' al sistema informatico del Fornitore utilizzando un apposito ***servizio web esposto dal Fornitore***. L'interfaccia del servizio web è definita dall'Amministrazione unitamente allo schema di organizzazione dei dati strutturati. Lo schema dei dati che saranno trasferiti dal GSU al sistema del Fornitore è riportato al paragrafo 'Strutture dati'.

**c. Ritorno dei numeri di raccomandata (Responsabile: Fornitore)**

Allo scopo di permettere al Fornitore di comunicare i numeri di raccomandata associati alla singola notifica, il GSU esporrà un servizio web che dovrà essere ***invocato dal Fornitore***; i numeri di raccomandata saranno comunicati al GSU utilizzando la stessa struttura dati (distinta) di cui al precedente punto b, arricchita dei numeri di raccomandata e di altre informazioni utili.

**d. Invio degli esiti delle notifiche (Responsabilità: Fornitore)**

L'invio dei dati relativi agli esiti delle notificazioni avverrà su iniziativa del sistema del Fornitore che dovrà trasmettere all'Amministrazione, alla conclusione dell'attività di notificazione, *copia per immagine della cartolina contenente l'esito della notifica*, nonché i dati strutturati associati a ciascuna cartolina. L'immagine in formato pdf deve essere chiaramente leggibile e non deve superare la dimensione massima di 500 KB. Il sistema informatico del Fornitore ***invocherà il servizio web esposto dal dominio Giustizia*** di cui al successivo punto e.

**e. Acquisizione degli esiti delle notifiche (Responsabilità: Ministero della Giustizia)**

Per la comunicazione degli esiti di ogni singola attività di notifica eseguita dal Fornitore, il dominio Giustizia esporrà un servizio web di ricezione dei dati strutturati relativi agli esiti di notifica (le informazioni riportate sugli avvisi di ricevimento); il servizio potrà essere unico per gli ambiti civile e penale oppure potranno essere realizzate API differenti per civile e penale. Le informazioni inviate dal Fornitore permetteranno di indirizzare gli esiti della notifica verso il corretto fascicolo gestito dall'ufficio giudiziario.

**f. Esposizione delle copie per immagine degli esiti di notificazione (Responsabilità: Fornitore)**

Il Fornitore ***metterà a disposizione nel sistema informatico e nel sito web*** della copia per immagine delle 'cartoline', utilizzando come criterio di ricerca il numero di raccomandata, l'ambito (civile/penale), il ruolo e il numero del fascicolo, nonché qualsiasi altro dato presente nella cartolina.

Il servizio dovrà essere accessibile agli operatori degli uffici giudiziari accreditati sul sistema del Fornitore; la modalità di accesso e di accreditamento sarà quella proposta dal Fornitore secondo le indicazioni di sicurezza descritte al successivo capitolo 6. Il sistema dovrà garantire l'implementazione di specifiche regole di consultazione in modo da permettere la visualizzazione solo dei dati a cui il soggetto ha diritto.

## **4. Sistema informatico del fornitore**

Il fornitore dovrà mettere a disposizione dell'Amministrazione un sistema informatico in grado di soddisfare tutte le esigenze conoscitive descritte nel capitolato tecnico e negli atti di gara, il cui accesso dovrà essere garantito, ai fini della tracciabilità delle spedizioni, anche via web.

In particolare (senza pretesa di esaustività), il citato sistema informatico, dovrà garantire, oltre alle funzionalità già descritte nel presente documento e negli atti di gara:

- esposizione dei servizi per la ricezione delle distinte delle raccomandate;
- invocazione dei servizi web esposti dal dominio Giustizia e documentati nelle API che saranno rese disponibili nella fase di progettazione di dettaglio (successiva all'aggiudicazione). Il pattern

di interazione sarà di tipo ‘non bloccante’ e il pattern di sicurezza sarà in linea con gli standard di sicurezza definiti dall’Amministrazione (si veda quanto indicato nel successivo capitolo 6);

- creazione dell’esito di notifica come oggetto nativo digitale, secondo la struttura dati descritta al capitolo 5-Strutture dati;
- memorizzazione, in conformità con le “Linee guida sulla formazione, gestione e conservazione dei documenti informatici” adottate dall’Agenzia per l’Italia Digitale con determinazione n. 407 del 9 settembre 2020, delle distinte delle raccomandate provenienti dall’ufficio NEP e degli esiti di notifica comprensivi di copie per immagine delle cartoline restituite agli uffici giudiziari;
- consultazione dei dati memorizzati (sia C2A che A2A) per almeno 5 anni dopo la conclusione del contratto;
- creazione e gestione dei log e delle informazioni utili al tracciamento degli eventi di processo (**giornale degli eventi**). Il giornale deve risultare ricostruibile in maniera semplice in base ad eventi significativi (es: ricezione distinte, invio dati raccomandate, invio esiti, accessi utente accreditato e operazioni compiute, ecc,...);
- retry delle invocazioni ai servizi esposti dal dominio Giustizia, di cui ai punti c. ed e. del precedente elenco, nel caso in cui non si riceva la notifica di presa in carico (ack) da parte dei sistemi del dominio Giustizia. La politica di retry dovrà essere concordata con l’Amministrazione;
- possibilità di elaborazione di statistiche/estrazione di dati aggregati relative al processo di notificazione;
- servizi di manutenzione correttiva, adeguativa ed evolutiva del software a seguito di adeguamenti o miglioramenti implementati sui sistemi informatici del dominio Giustizia;
- aggiornamento dei sistemi informatici per garantire riservatezza e integrità dei dati personali trattati nonché conformità ai requisiti di sicurezza di cui al capitolo 6;
- disponibilità dei servizi applicativi e del sito web non inferiore al 99,95% su base mensile.

## 5. Strutture dati

Di seguito le strutture dati (descritte ad alto livello e con linguaggio naturale) che definiscono il contenuto informativo delle interazioni tra i sistemi del dominio Giustizia e il sistema informatico del Fornitore. Si precisa che i dati potranno essere soggetti a raffinamenti e modifiche nella fase di disegno di dettaglio della soluzione, nonché nel corso dell’esecuzione contrattuale.

**Distinta degli AAGG e delle raccomandate:** informazioni strutturate inviate dal GSU al sistema del Fornitore; tali informazioni saranno quelle utilizzate per la compilazione delle buste ‘verdi’ e delle cartoline relative agli esiti. Come specificato nei precedenti paragrafi, la struttura dati viene creata dal GSU e di seguito elaborata dal Fornitore e arricchita dei dati indicati in **grassetto**; quindi restituita al GSU nella fase di invio dati Raccomandate.

Le informazioni tra parentesi indicano l’obbligatorietà del dato (*obb*) e la cardinalità.

1. Id\_Distinta (*obb, 1*) --*identificativo univoco della distinta*
2. progrInvio (*obb, 1*) --*progressivo invio della stessa distinta utilizzato per correzioni di una distinta già inviata. Al primo invio sarà 1 e sarà incrementato nel caso di reinvii di una stessa distinta con correzioni*



3. dataDistinta
4. ModelloGSU
5. TotaleAtti (*obb, 1*)
6. **TotaleSpesaPostale** - *--valorizzata da Fornitore*
7. ItemNotifica <progressivo> (*obb, 1-unbounded*)
  - a. CronologicoGSU
  - b. numeraleCronologicoGSU
  - c. AnnoCronologicoGSU
  - d. RegistroGSU
  - e. Atto-Avviso, con valori Artt. 139, 140 e 660 c.p.c. e 157 c.p.p. *--permette di distinguere se si tratta di un atto o di un avviso*) - *obb, 1*
  - f. Richiedente
    - i. Ufficio
      1. Cod Ufficio
      2. DenomUfficio
      3. civile/penale
      4. caricoErario (opz) con valori FunzDeleg o Ministero
    - ii. privato
      1. Cognome
      2. Nome
      3. Indirizzo
      4. Civico
      5. CAP
      6. Località/Città
      7. Provincia
      8. PEC
      9. CaricoPagamento
        - a. parte
        - b. erario
  - g. DatiRegistroRichiedente (*opz, 0-1*)
    - i. Registro (SNT, SICID, SIECIC, SIGP,...) *-- codifica condivisa*
    - ii. Ruolo
    - iii. Numero RG
    - iv. Anno RG
    - v. dataUdienza/Scadenza
    - vi. Sezione o Collegio (*opz*)
    - vii. Giudice
  - h. ListaDestinatari (*obb*)
    - i. Destinatario <progrDest> (*obb, 1-unbounded*)
      1. Anagrafica
        - a. Cognome
        - b. Nome
        - c. CodiceFiscale
        - d. Indirizzo
        - e. Civico

- f. Località
- g. CAP
- h. Provincia
- i. Nazione
- 2. **Raccomandata** (*opz*) --*valorizzata da Fornitore*
  - a. **Numero**
  - b. **spesaPostale**
- 3. **metadata** (*opz*) -- *utilizzati per informazioni di comodo*

**Esito atto notificato:** informazioni strutturate che il sistema del Fornitore invia al dominio Giustizia per la successiva associazione al fascicolo di pertinenza (vedere par 5.4 e 5.5 del Capitolato tecnico)

- 1. IdDistinta --*referimento alla distinta*
- 2. progrInvio --*progressivo della distinta a cui si fa riferimento*
- 3. Richiedente
  - a. CodUfficio
  - b. DenomUfficio
  - c. civile/penale
- 4. DatiRegistroRichiedente (*opz, 0-1*)
  - a. Registro (SNT, SICID, SIECIC, SIGP,...) --*codifica condivisa*
  - b. Ruolo
  - c. Numero RG
  - d. Anno RG
  - e. dataUdienza
  - f. Giudice
- 5. Destinatario
  - a. anagrafica
    - i. Cognome
    - ii. Nome
    - iii. CodiceFiscale
    - iv. Indirizzo
    - v. Civico
    - vi. Località/Città
    - vii. CAP
    - viii. Provincia
- 6. NumeroRaccomandata
- 7. Pdf immagine della cartolina degli esiti della notificazione (base64)
- 8. datiNotificaPostale (*obb, 1-n*)
  - a. EsitoAvvenutaConsegna
    - i. dataConsegnaNotifica
    - ii. Ricevente <tipologia fisica/giuridica>
      - 1. Cognome
      - 2. Nome

3. Qualità (destinatario, familiare convivente, addetto alla casa, legale rappresentante, curatore fallimentare,.....)
4. SpecificaQualità
5. DatiFirma (analfabeta, imposs firmare, firmato registro consegna)
- iii. ComAvvenutaNotifica (CAN)
  1. NumeroRaccomandataAvvenutaNotifica
  2. dataRaccomandata
  3. dataConsegnaRaccomandata (*opz*)
- b. EsitoMancataConsegna
  - i. TipoMancataConsegna (rifiuto, assenza temporanea, irreperibilità, destinatario sconosciuto, trasferito, ecc)
  - ii. dataRifiuto
  - iii. nominativoRifiuto
    1. Cognome
    2. Nome
    3. Qualità
    4. SpecificaQualità
  - iv. affissoAvviso (porta/cassetta)
  - v. DepositoPressoUfficio
    1. DataDeposito
    2. NumeroRaccomandataAvvenutoDeposito (CAD)
    3. dataRaccomandata
    4. dataConsegnaRaccomandata (*opz*)
- c. EsitoRitiro
  - i. dataRitiro
  - ii. nominativoRitiro
    1. Cognome
    2. Nome
    3. Qualità
    4. SpecificaQualità

## 6. Sicurezza e modalità di connessione

Il sistema informatico del Fornitore dovrà essere realizzato tramite metodologie che integrino la sicurezza in ogni fase del ciclo di sviluppo, dalla progettazione iniziale all'esercizio, secondo tecniche di SDLC (Secure Development Lifecycle) e Security/Privacy by Design.

Nello specifico, dovrà essere garantito un approccio di *security by design*, in *compliance* con gli aspetti relativi al trattamento dei Dati personali, e che garantisca adeguati livelli di sicurezza relativi a:

- **Autenticazione e autorizzazione:** il sistema dovrà garantire la possibilità di abilitare una autenticazione forte per gli utenti e per gli amministratori e implementare modelli di controllo

delle autorizzazioni basati sul principio di “least-privilege” per mezzo di privilegi relativi a ruoli (RBAC) o su attributi (ABAC);

- **Comunicazioni:** il sistema dovrà supportare l'utilizzo di protocolli sicuri (HTTPS con TLS 1.2 o superiore) per tutte le comunicazioni;
- **Gestione dei dati:** il sistema dovrà supportare l'utilizzo di cifrari forti che utilizzino algoritmi raccomandati all'interno delle Linee Guida ACN (“Linee Guida funzioni crittografiche”, “Codici di autenticazione di messaggi”, “Funzioni di Hash”, “Cifrari a blocchi e modalità di funzionamento”);
- **Sicurezza del software:** il sistema dovrà essere resiliente rispetto alle vulnerabilità note nell'ambito applicativo (come SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) e Remote Code Execution (RCE)), indicate nell'OWASP Top 10;
- **Applicativo up-to-date:** tutti i sistemi utilizzati nell'ambito della fornitura (applicativi, librerie e sistemi operativi) devono essere aggiornati allo stato dell'arte al momento della consegna;
- **Logging e monitoraggio:** il sistema dovrà garantire la possibilità di logging ed inoltre log verso il sistema SIEM (Security Information and Event Management) dell'Amministrazione;
- **Manutenzione:** il fornitore dovrà garantire l'applicazione tempestiva di aggiornamenti e patch di sicurezza necessari per il corretto funzionamento del sistema.

Nell'ambito dei Web Services e dell'API Security, il fornitore dovrà garantire l'utilizzo di strumenti adeguati a:

- **Autenticazione delle API:** l'applicativo dovrà utilizzare standard utili all'autenticazione per utenti e client quali standard come OAuth2.0 o token JWT se utilizzato il paradigma REST ed implementare WS-Security se utilizzato il paradigma SOAP. Dovrà inoltre essere garantita l'integrazione con l'API Gateway e/o con il sistema IAM presente presso l'Amministrazione;
- **Autorizzazione su paradigma “least-privilege”:** l'applicativo dovrà implementare il principio del minimo privilegio per limitare l'accesso delle risorse API ed i token utilizzati dovranno avere una scadenza prevedendo meccanismi di revoca;
- **Sicurezza delle comunicazioni:** l'applicativo dovrà utilizzare protocolli con crittografia adeguata per proteggere i dati in transito disabilitando le connessioni non sicure (es: http). Laddove possibile, dovranno essere predisposti strumenti per l'autenticazione machine-to-machine (mTLS);
- **Protezione delle informazioni:** l'applicativo dovrà ridurre al minimo le informazioni contenute nelle risposte secondo il paradigma di “least data exposure” implementando la crittografia degli elementi sensibili;
- **Protezione API:** l'applicativo dovrà integrarsi con soluzioni di API Gateway o altre soluzioni (WAF/AntiBot) già presenti atte a limitare il numero di richieste per utente o per IP per prevenire attacchi DoS/DDoS e a gestire le interazioni tra i Web Services interessati;

- **Validazione input:** l'applicativo dovrà essere sviluppato secondo il paradigma di security by design comprendendo data validation utile a verificare e validare gli input delle API. Nell'ambito del paradigma REST devono essere utilizzate librerie per la validazione dei payload (es: JSON), nell'ambito del paradigma SOAP dovrà essere utilizzata una validazione per tramite di uno stringente XSD;
- **Protezione da vulnerabilità note:** l'applicativo dovrà essere sviluppato per essere resiliente by design – nei limiti del possibile – ad attacchi di tipo applicativo, tra i quali CSRF (Cross-Site Request Forgery), CORS (Cross-Origin Resource Sharing), XEE (XML External Entity);
- **Monitoraggio:** l'applicativo dovrà registrare le richieste e garantire la possibilità di inoltro dei log verso il SIEM;
- **Manutenzione ed aggiornamento:** il fornitore dovrà prevedere il supporto di manutenzione correttiva atta a garantire l'applicazione tempestiva di aggiornamenti e patch di sicurezza per l'applicativo comprensivo dei test di regressione;
- **Test e validazione:** il fornitore, assieme alla documentazione contrattuale, dovrà fornire i risultati di test di sicurezza effettuati sull'applicativo che dimostri l'assenza di problematiche di sicurezza o vulnerabilità.