SIELTE

Carta dei servizi

RAO Pubblico

Sommario

1 Premessa

1.1 Cos'è il RAO Pubblico

Sielte, in qualità di Identity Provider (di seguito IdP) accreditato in AgID, offre una modalità fortemente proiettata a venire incontro alle necessità degli Enti pubblici che necessitano di una soluzione di erogazione nell'ambito del sistema di rilascio dell'identità digitale.

Tale soluzione, denominata RAO (Registration Authority Officer) Pubblico, permette all'Ente di:

- essere autonomo dal punto di vista del rilascio dell'identità e nella gestione degli appuntamenti;
- rilasciare l'identità digitale contestualmente agli altri servizi;
- semplificare il rilascio dell'identità per il cittadino.

1.2 L'offerta di Sielte

Il servizio è fornito in modalità SaaS.

Sielte si impegna a:

- Garantire Evoluzione, Scalabilità e Sicurezza della piattaforma.
- Erogare la Configurazione e la Formazione.
- Offrire il Supporto tecnico.
- Garantire un valore di Uptime in linea o superiore agli standard di Sielte.

1.3 In breve: il processo di identificazione tramite RAO Pubblico

Il Cittadino si reca presso una delle Pubbliche amministrazioni accreditate in AgID, consultabili tramite il seguente link: https://www.spid.gov.it/cos-e-spid/come-attivare-spid/le-pa-per-attivare-spid/.

Fornisce quindi i suoi dati anagrafici all'operatore preposto e mostra i suoi documenti; successivamente l'operatore inserisce a sistema le informazioni comunicate dal Cittadino e necessarie al rilascio dell'identità digitale.

Una volta completata la fase di inserimento ed invio dati, l'operatore consegna al Cittadino un documento cartaceo contenente la prima parte di una password. Contestualmente, il Cittadino riceve via e-mail la seconda parte della password ed un pacchetto (token) di attivazione in formato testuale. Conclusa la fase di riconoscimento presso l'ente pubblico, il Cittadino deve ultimare la procedura di richiesta recandosi sul sito di un IdP abilitato alla modalità di identificazione Sportello Pubblico, dove inserisce il proprio Codice Fiscale, scarica il token ricevuto via e-mail e lo carica nell'apposito form, facendo attenzione ad inserire anche la prima parte della password, ricevuta brevi manu, e la seconda parte ricevuta via e-mail. Se le due password sono corrette, il sistema chiede la verifica dei dati di contatto inseriti e, successivamente, il Cittadino può concludere la procedura attivando l'identità e cambiando la password.

2 Principi fondamentali della Carta dei Servizi

La Carta dei Servizi garantisce la trasparenza dei servizi che Sielte S.p.A. fornisce ai propri Clienti. Il documento riporta dettagliatamente le informazioni riguardanti i diritti di cui godono i Clienti e il livello e la qualità del servizio che Sielte S.p.A. si assume nell'ambito del RAO Pubblico.

La Carta dei Servizi è disponibile al link: https://www.sielte.it/images/documents/carta-servizi-rao-pubblico.pdf

3 Generalità

3.1 Scopo del documento

Il presente documento riassume le modalità di erogazione del servizio RAO Pubblico.

3.2 Il ruolo di Sielte e le sue responsabilità

Sielte S.p.A. fornisce il servizio RAO Pubblico in modalità SaaS rivolgendosi alle pubbliche amministrazioni che vogliono accreditarsi in AgID come RAO Pubblici. Sielte, in questo scenario, si occupa di sviluppare, gestire e manutenere la piattaforma e l'applicativo e fornire relativa formazione dedicata, supporto ed assistenza. Offre, inoltre, formazione e supporto alle PA lungo tutto il percorso di accreditamento con l'AgID.

3.3 Quadro normativo di riferimento

Le caratteristiche del servizio RAO Pubblico di Sielte sono conformi a quanto previsto dalle *Linee Guida per la realizzazione di un modello di RAO Pubblico,* emanate da AgID con Determinazione n. 344/2019.

Il servizio è erogato in conformità alle norme di certificazione ISO/IEC 27001:2022 (Sicurezza delle Informazioni) e Linee Guida ISO/IEC 27017/2015 (Sicurezza delle Informazioni nell'ambito di erogazione dei servizi cloud) e ISO/IEC 27018:2019 (protezione dei dati personali nell'ambito di erogazione dei servizi cloud).

Pertanto, nel trattamento di dati e informazioni, vengono applicati i seguenti fondamentali principi:

➢ *Riservatezza:* le informazioni vengono rese disponibili solo agli individui e alle entità autorizzate.

➢ *Integrità:* le informazioni devono essere protette per quanto riguarda la loro accuratezza e completezza.

➢ *Disponibilità:* le informazioni sono accessibili solo agli individui e alle entità autorizzate, laddove necessario.

4 Qualità del servizio

4.1 Risk Assessment

Il risk assessment consente l'analisi delle minacce che impattano sui processi che Sielte utilizza per erogare servizi ai propri Clienti. Con cadenza almeno annuale o quando si verificano cambiamenti significativi, le minacce ed i relativi rischi vengono analizzati, aggiornati e correlati ai processi aziendali. Le minacce che generano rischi a impatto per il Cliente vengono trattate secondo programmazione aziendale ovvero incluse nel piano di miglioramento.

4.2 Monitoring

Sielte utilizza tecniche proattive e preventive di monitoraggio dell'infrastruttura e dei servizi erogati. Tutti i componenti dell'infrastruttura sono monitorati attraverso trigger opportunamente configurati.

4.2.1 *Generici tipi di Allarmi*

- Allarme rientrato.
- Allarme di livello informativo: non impatta sulle prestazioni, solo per alcuni tipi di metriche.
- Allarme di livello basso: non impatta sulle prestazioni e sulla fruibilità del servizio.
- Allarme di livello alto: pregiudica le prestazioni o la fruibilità del servizio.
- Allarme di livello disastro: interruzione di servizio.

Il Service Desk verifica tutti gli allarmi del monitoraggio e garantisce copertura lunedì-venerdì dalle 07:30 alle 18:30 e il sabato dalle 08:30 alle 17:30.

4.3 Incident Management

L'Incident Management è gestito dal Service Desk. Il processo di gestione degli Incident, mira a ripristinare la normalità di servizio nella maniera più veloce possibile, con la minima interruzione di servizio al business, assicurando che i migliori livelli di servizio e disponibilità siano mantenuti. Sono considerati incident tutte le segnalazioni di anomalie effettuate dai Clienti, rilevate internamente e/o dai sistemi di monitoring.

Il Service Desk ha principalmente il compito di:

- Raccogliere le segnalazioni provenienti dagli utenti, e dopo aver stabilito se si tratti o meno di un incidente, effettuare le operazioni di categorizzazione, classificazione e assegnazione priorità sul sistema di ticketing.
- Dare supporto iniziale agli utenti e fare il primo tentativo di offrire una soluzione workaround.
- Mantenere gli utenti aggiornati sullo stato delle loro richieste.
- Coinvolgere le parti interessate in base alla tipologia di incidente, inoltrando tutte le richieste che non possono essere risolte direttamente ai gruppi di secondo livello e monitorarne lo stato.
- Fornire informazioni sulle necessità formative degli utenti dei servizi IT e dei servizi Cloud rispetto ai servizi stessi.
- Confermare agli utenti l'effettiva risoluzione degli incidenti.

È possibile segnalare un incident chiamando dal lunedì al venerdì dalle 7:30 alle 18:30 e il sabato dalle 08:30 alle 17:30 al numero di telefono 095.2291711 oppure scrivendo una mail a supporto@sielte.it.

Funzione	Giorni	Festivi	Orario
Helpdesk	LUN/VEN	NO	07:30-18:30
Helpdesk	SAB	NO	08:30-17:30

Sulla base della valutazione di impatto che l'incidente potrebbe avere sui sistemi ICT e sull'erogazione dei servizi di Sielte, gli incidenti di sicurezza delle informazioni sono classificati su 4 livelli di criticità:

Valore	Criticità dell'incidente	tipologia impatto
1	POCO SIGNIFICATIVA	Impatto irrilevante o modesto, possibilità di incontrare piccoli inconvenienti, superabili senza alcun problema
2	QUASI SIGNIFICATIVA	Impatto moderato, ma che richiede interventi mirati da parte dell'Organizzazione, possibilità di incontrare inconvenienti significativi, che dovrebbero essere superabili a dispetto di alcuni problemi (costi aggiuntivi, impossibilità di accesso a servizi, ecc.)
3	SIGNIFICATIVA	Impatto significativo, con possibili conseguenze rilevanti che dovrebbero essere superabili anche se con gravi difficoltà (inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, ecc.)
4	MOLTO SIGNIFICATIVA	Impatto molto significativo, compromesso con necessità di interventi immediati, con conseguenze irreversibili, quindi potrebbero non essere superabili

Il grado di urgenza dell'incidente è valutato sulla base di quanto a lungo un incidente abbia un impatto sull'erogazione dei servizi.

Urgenza		Tipologia di incidente
D	Basso	Incidente gestibile. Potenzialmente irritante, ma non incide in modo sostanziale sull'azienda.
C	Medio	Incidente preoccupante. Timori per le scadenze non rispettate e per i modelli di business significativamente modificati.
B	Alto	Incidente critico. Attività seriamente compromessa, scadenze non rispettate; rischio di incorrere in sanzioni.
A	Urgente	Incidente disastroso. Capacità di continuare l'attività seriamente minacciata. Violazione di norme legali e statutarie, danno d'immagine

Dall'intersezione della criticità con il grado di urgenza si definisce la priorità dell'incidente:

Urgenza \ Criticità	Poco significativo	Quasi significativo	Significativo	Molto significativo
Basso	P4	P4	P3	P3
Medio	P4	P3	P3	P2
Alto	P3	P3	P2	P2
Urgente	P3	P2	P2	P1

A seconda della priorità attribuita all'incidente di sicurezza, vengono coinvolte le figure che possiedono delle responsabilità ben definite per la gestione dell'incidente, se ricade nella propria sfera di competenza.

4.4 Segregation, security, Networking Rules

Attraverso l'applicazione di apposite regole di networking, vengono garantiti la segregazione degli ambienti e il filtraggio dei pacchetti. È presente un firewall next generation e la segregazione degli ambienti (istanze) all'interno dell'infrastruttura viene garantita tramite tecnologia di containerizzazione.

I dati vengono immagazzinati su distinti ambienti per ogni Cliente che usufruisce del prodotto in essere. In nessuno scenario i dati di un Cliente saranno visibili da utenti terzi. La profilazione utente garantirà un ulteriore livello di protezione dei dati, rendendo gli stessi accessibili solo da determinati profili utente. Grazie alla compartimentazione logica garantita dal sistema, nessuno tra tutti i dati dei diversi Clienti può in alcun modo entrare in contatto o sovrapporsi.

Nel caso in cui un utente immetta per più di tre volte una password o un PIN errato, l'account viene disattivato e sarà compito dell'amministratore procedere con l'invio di una nuova mail di attivazione.

Viene utilizzato uno strumento di log management per registrare i log di tutte le applicazioni.

4.5 Change Management

Il Cliente, attraverso i canali a sua disposizione, può richiedere una Change Request. Le CR possono essere valutate come manutenzione correttiva del prodotto/servizio o come richiesta di manutenzione evolutiva. La manutenzione correttiva ha la peculiarità di dover essere gestita nella modalità più semplice, efficace e rapida possibile riguardando la rimozione di malfunzionamenti, comunque evidenziati, che sono d'impedimento all'esecuzione o al corretto funzionamento del software applicativo. Nel caso in cui la CR venisse valutata come manutenzione evolutiva, si procede ad avanzare richiesta di autorizzazione al referente del Cliente, al fine di approvare la modifica al sistema e/o ai suoi componenti e la soluzione di massima che è stata individuata in fase di valutazione e di accettare il costo necessario alla sua applicazione.

È possibile richiedere operazioni di Change Management inviando una mail a supporto@sielte.it o chiamando lo 095 2291711.

4.6 User Rights Provisioning

In fase di installazione e configurazione dell'applicativo, Sielte configura la prima utenza, denominata Security Officer, la quale avrà di default i diritti amministrativi della configurazione. Tale utenza potrà quindi, nell'ambito dell'applicativo erogato al singolo Cliente, modificare le varie configurazioni e creare delle utenze di tipo operatore. Quest'ultime utenze avranno soltanto i privilegi necessari per identificare i richiedenti, non avranno quindi la possibilità di modificare la configurazione né di visualizzare le identificazioni degli altri operatori.

4.7 Backup & Restore

Sielte effettua i backup specifici di dati/informazioni/contenuti trattati dal Cliente attraverso tool di backup di livello enterprise.

Vengono effettuati backup delle VM che erogano il servizio.

La crittografia degli stessi viene effettuata direttamente dal software di backup.

La locazione dei backup è su una infrastruttura diversa (storage) rispetto all'ambiente di produzione.

I backup delle VM vengono eseguiti ogni giorno con una schedulazione che prevede un Full Backup settimanale e 6 Incremental Backup nei restanti giorni della settimana.

I backup vengono ogni giorno copiati, sempre tramite lo stesso tool di backup, su un repository locato in una diversa sede remota con retention di 28 giorni, in modo da avere una terza copia dei dati al di fuori del sito di produzione.

È possibile richiedere la variazione della politica di backup o la restore di un servizio attraverso una Change Request inviando una mail a supporto@sielte.it.

L'applicativo garantisce l'integrità del dato e la sua consistenza attraverso delle metodologie e delle logiche proprietarie di backup. Inoltre, due volte l'anno Sielte effettua delle simulazioni di ripristino, al fine di verificare se l'immagine ripristinata sia integra e consistente.

Le tempistiche di ripristino si attestano sulle sei ore circa per l'intera infrastruttura, circa 30 minuti per VM.

4.8 Temporary files

Il prodotto non genera file temporanei.

4.9 Vulnerability Assessment / Penetration Test

Con cadenza almeno annuale, vengono effettuati test di VA/PT su tutti i sistemi dei Clienti. Il Cliente può richiedere, se presente, l'elenco delle vulnerabilità e relativo Mitigation Plan che contiene la descrizione delle attività per il rientro delle vulnerabilità stesse. Le informazioni possono essere richieste attraverso l'apertura di un ticket secondo le modalità concordate contrattualmente.

4.10 Patching

Sielte garantisce ai propri Clienti il patching (SW e OS) secondo best practices dei vendor.

4.11 SLA Management

Gli SLA del servizio RAO Pubblico vengono esplicitati all'interno della Scheda d'Ordine sottoscritta dal Cliente.

4.11.1 *Casi che non fanno parte della garanzia SLA*

- Errata configurazione dell'applicativo da parte del Cliente.
- Manutenzione programmata del datacenter.
- Malfunzionamenti della connettività del Cliente.
- Altri problemi non derivanti da un malfunzionamento dei datacenter del fornitore.

4.11.2 *SLA*

Lo SLA è basato sul servizio ed è valido per tutti i Clienti.

Tipologia SLA	Tipo	TTO (Time to own)	TTR (Time to resolve)
SLA01	Incident *Assistenza per risoluzione di problemi tecnici*	Entro **8** ore lavorative	Entro **3** giorni lavorativi nel 90% dei casi su base annuale
SLA02	Richieste *Assistenza per informazioni*	Entro **3** giorni lavorativi	Entro **5** giorni lavorativi nel 95% dei casi su base annuale

Legenda:

TTO (Time to own): Tempo di presa in carico

TTR (Time to resolve): Tempo di risoluzione

Nota: TTO e TTR misurati dall'istante di apertura dell'incident/richiesta di supporto.

4.11.3 *Uptime*

Come dichiarato all'interno dell'art. 16 della Scheda d'Ordine sottoscritta dal Cliente, dove sono presenti maggiori dettagli e approfondimenti, SIELTE si impegna a mettere in atto la massima disponibilità della sua infrastruttura garantendo una continuità di servizio e rispetto degli SLA in una percentuale non inferiore al 99,7%.

L'Uptime sopra indicato può essere scorporato nei seguenti parametri:

- Alimentazione elettrica e della climatizzazione.
- Accessibilità tramite rete Internet.
- Disponibilità dell'infrastruttura fisica.

4.12 Criptography

Al Cliente viene garantita la crittografia su tutti gli URL pubblicati su internet. Tutti i servizi esposti sono garantiti da certificati SSL.

Sielte garantisce lo scambio crittografato dei dati attraverso il protocollo SSL/TLS.

Il token di identificazione rilasciato all'utente viene crittografato mediante cifratura simmetrica HS256. I dati inseriti per la creazione di una nuova richiesta di identificazione vengono cifrati tramite l'algoritmo di cifratura simmetrico HS256. Le password inserite all'interno del RAO non sono salvate direttamente sul database: è calcolato il loro hash in SHA256 e vengono inserite all'interno di un JWT; dopo 30 giorni, inoltre, sarà necessario aggiornare la password.

4.13 Policy sviluppo sicuro

Sielte stabilisce, documenta, manutiene e applica ai suoi progetti e ai suoi servizi IT i principi per l'ingegnerizzazione dei sistemi sicuri.

Al fine di garantire la massima sicurezza e disponibilità degli ambienti di sviluppo di modifiche ai servizi IT, viene implementata una netta separazione degli ambienti di sviluppo dagli ambienti di test e staging (preproduzione).

In tutte le fasi di pianificazione, progettazione e transizione di servizi IT viene dato particolare peso alla gestione dei dati personali, utilizzando misure e tecniche organizzative per la loro tutela, basandosi sui principi della privacy by design e by default.

- Data Protection by design: valutare e analizzare sin dalle fasi di progettazione gli strumenti e le corrette impostazioni a tutela dei dati personali, al fine di prevenire ogni forma di rischio; utilizzare tecniche di pseudonimizzazione o minimizzazione dei dati.
- Data Protection by default: utilizzare i dati personali solo per le finalità previste; utilizzare i dati personali solo per il periodo necessario alla finalità prevista.

4.14 Gestione dei reclami e delle non conformità

La gestione e delle non conformità viene strutturata e gestita secondo quanto previsto dalle procedure aziendali in materia.

A seconda delle esigenze quali, veicolare i reclami, avere supporto o chiedere informazioni si può scegliere una tra le seguenti modalità di contatto:

- Attraverso il sito istituzionale si possono inoltrare reclami o richieste di informazioni, compilando l'apposito form.
- È a disposizione degli utenti un servizio di Call Center con operatore disponibile dal lunedì al venerdì, dalle ore 7:30 alle ore 18:30 e il sabato dalle 08:30 alle 17:30, raggiungibile al numero 095 2291711.

