[1 Introduzione 2](#_Toc187239916)

[2 Identity and Access Management 2](#_Toc187239917)

[3 API Management 3](#_Toc187239918)

[4 Firma Digitale 4](#_Toc187239919)

[5 Interoperabilità AgID tra Enti 4](#_Toc187239920)

[6 Monitoraggio processi e procedimenti (BAM) 5](#_Toc187239921)

# Introduzione

Si riporta, nel seguito, una descrizione sintetica delle componenti architetturali che coprono i requisiti non ancora del tutto soddisfatti dalla soluzione.

L’integrazione tra la soluzione e le piattaforme trasversali che implementano le componenti architetturali permette di garantire la aderenza minima alla architettura di riferimento dell’Ente.

# Identity and Access Management

La componente di Identity and Access Management (IAM) è il sistema che permette di gestire complessivamente le identità dei soggetti e le proprie autorizzazioni all'interno del sistema informativo.

Il sistema IdM è in grado di garantire e gestire:

• **Autenticazione**: verifica che un soggetto è chi/quello che dice di essere utilizzando una password, una smart card, una credenziale biometrica, come un'impronta digitale, o altro.

• **Autorizzazione**: è il processo mediante il quale ad un soggetto già autenticato si garantisce o si nega l'accesso ad un servizio in base all’identità ed ai ruoli che lo identificano.

• **Ruoli**: i ruoli sono gruppi di attività e/o di altri ruoli. Agli utenti vengono attributi ruoli legati a un particolare lavoro o mansione.

• **Delega**: con il concetto di delega un utente può svolgere attività per nome e per conto di altro utente, con medesimi ruoli.

• **Interoperabilità**: utilizzo del protocollo SAML, standard internazionale utilizzato per lo scambio di informazioni sulle identità tra domini distinti.

Il modello di riferimento regionale per l’identificazione ed autenticazione degli operatori, in linea con i principali sistemi analoghi realizzati in altri domini, prevede le seguenti componenti logiche:

* **Identity Provider (IP)**, componente che consente di gestire le identità digitali degli utenti (operatori) abilitati ad utilizzare i sistemi informativi del dominio interessato (aziendale e regionale).
* **Componente di IP** deve gestire una o più soluzioni di autenticazione (es.: Username/password + OTP, Username/password + postazione certificata);
* **Attribute Authority (AA)**, componente che certifica il possesso di determinati attributi (profili, requisiti …) basandosi sull’identità dell’utente (operatore) certificata dall’IP e finalizzata a definire le autorizzazioni utilizzabili dai Service Provider (SP).
* **Service Provider (SP)**, componente che fornisce servizi applicativi e informativi (aziendali e regionali) basandosi sull’identità dell’utente (operatore) certificata dal IP e dagli attributi dello stesso utente certificati dal AA.

L'infrastruttura di autorizzazione e autenticazione federata è realizzata utilizzando il framework open source Shibboleth basato su standard di interoperabilità SAML 2.0 implementato da Internet2.

Nell’infrastruttura di access management di CSI Piemonte anche SPID e CIE confluiscono in un unico sistema di autenticazione integrato nel sistema Shibboleth2, già in uso in consorzio, attraverso la predisposizione di service provider dedicati. È stato predisposto un Identity Provider Proxy SPID, denominato GASP (Gateway Autenticazione SPID), e i Service Provider CSI, per usare SPID, effettuano il trust con tale Identity Provider. I SP dispiegati possono essere usati solo dagli applicativi rivolti ad utenti cittadini e/o imprese.

# API Management

L’API Management va utilizzato tutte le volte che occorre realizzare una API trasversale, ovvero, utilizzabile da differenti soluzioni verticali, da piattaforme trasversali o da applicazioni dispiegate su sistemi informativi esterni.

È valido per tutti i casi d’uso di integrazione che non appartengono a quelli legati all’interoperabilità tra enti della PA, ovvero, quelli vincolai al modello di interoperabilità AgID.

Permette di introdurre un layer di astrazione tra i servizi che espongono funzionalità (API Providers) e le applicazioni che li consumano (API Consumers) semplificando gli sviluppi e favorendone il disaccoppiamento tra i due livelli.

L’Api Manager è la soluzione più utilizzata al giorno d’oggi per far fronte a questa necessità senza però perdere di vista gli obiettivi di gestione del traffico, della gestione della sicurezza, della gestione del ciclo di vita delle API e dell’audit del sistema.

La piattaforma che realizza le principali funzioni dell’API Management, si compone di:

* **Publisher**, applicazione web che permette agli API Providers di creare e pubblicare le API. Nel Publisher si definiscono tutti gli aspetti di configurazione dell'API, compresi endpoint dei servizi di back-end e politiche di throttling e rate limiting
* **API Store**, catalogo dedicato agli sviluppatori e alle terze parti che intendono integrare le API nelle loro applicazioni, monitorare l’utilizzo delle API nonché accedere ad altri strumenti di comunicazione e condivisione
* **API Gateway**, componente di runtime dell’API Manager che ha come finalità essenziale di esporre i servizi messi a disposizione dall'intero sistema in maniera sicura, facilmente fruibile e controllata. L'API Gateway, dal punto di vista architetturale, è un proxy dei servizi esposti dai sistemi di back-end, in modo tale che tutti i sistemi fruitori debbano effettuare l'accesso a servizi e risorse attraverso questo componente. Dal punto di vista funzionale, il Gateway, riceve le richieste per accedere alle API ed attua le politiche di controllo di accessi, applica le regole di rate limiting e throttling e instrada le richieste verso i sistemi di back-end.
* **Key Manager**, componente che ha il compito di gestire tutte le questioni relative alla sicurezza e alle chiavi. Tutte le richieste di generazione di nuovi access token sono gestite da questo componente che effettua la validazione di tutti i parametri inviati nella richiesta (client\_id, client\_secret, username, password, ecc...)
* **Traffic Manager**, componente che si occupa di regolare il traffico di ciascuna API secondo le politiche che sono state definite in fase di definizione dell'API e in fase di sottoscrizione alla stessa. Il motore di elaborazione del Traffic Manager elabora le politiche di throttling in real time, incluse le politiche di rate limiting delle chiamate alle API.

# Firma Digitale

La componente permette ad applicativi fruitori di disporre di servizi inerenti alle firme elettroniche. In pratica sono rese disponibili funzioni nei seguenti macro-ambiti funzionali:

* Verifica di firme elettroniche apposte su documenti digitali (file)
* Firma elettronica sui documenti digitali (file)
* Marcatura temporale dei documenti (apposizione e verifica)

Queste macro-funzionalità sono ovviamente articolate in servizi a grana più fine che implementano elaborazioni di natura crittografica, legata alle chiavi di firma nonché delle policy o profili di conformità legati ai criteri di apposizione e validazione delle firme e dei rispettivi certificati, come la validità del certificato e della CA emittente, la verifica delle liste di revoca (CRL), controllo dei formati delle buste crittografiche (PADES, XADES, CADES-BES, …).

Il componente svolge ruolo di mediazione verso i provider dei servizi di firma remota (normale, automatica, o di sigillo digitale) e di marcatura temporale, esposti dai certificatori accreditati che erogano servizi di identità digitale in veste di fornitori (o appaltatori) dell’ente.

La piattaforma che implementa la componente di firma digitale è denominata DoSign.

# Interoperabilità AgID tra Enti

Consente l'Interoperabilità tra enti implementando il nuovo Modello di AgID (MoDI) e l’integrazione con la Piattaforma Digitale Nazionale Dati (PDND).

Il nuovo Modello di Interoperabilità rende possibile la collaborazione tra Pubbliche amministrazioni e tra queste e soggetti terzi, per mezzo di soluzioni tecnologiche che assicurano l’interazione e lo scambio di informazioni senza vincoli sulle implementazioni, evitando integrazioni ad hoc.

Gli obiettivi del nuovo modello AgID sono:

* Costituire un punto unico per dichiarare la disponibilità di servizi e informazioni della PA
* Normalizzare il processo di autenticazione e autorizzazione all’accesso ai servizi
* Instaurare sempre un canale di comunicazione sicuro
* Evitare la proliferazione di duplicati di servizi omologhi
* Adottare un modello di interoperabilità (MoDI) che definisce le modalità tecniche con cui le PA possono condividere i dati con i soggetti o processi che ne hanno diritto
* Abilitare lo sviluppo di nuove applicazioni per gli utenti della PA

L’uso di questa componente è obbligatorio per normativa in tutti gli scenari di interoperabilità tra enti della PA e le piattaforme dati nazionali.

La nuova piattaforma di interoperabilità PDND-MoDI è un **API Gateway** progettato con l’obiettivo di facilitare l’interoperabilità tra servizi assicurando la conformità alle normative d’interoperabilità italiana ed europea in modo trasparente ai client interni al dominio.

Fornisce, oltre al consueto catalogo API con i relativi flussi di pubblicazione e sottoscrizione, un Gateway MoDI a cui viene delegata l'intera applicazione degli standard di comunicazione AgID.

Esattamente come la piattaforma di APIManagement, permette il disaccoppiamento delle applicazioni. Inoltre, offre la possibilità di configurare diversi profili di Interoperabilità come ad esempio il profilo MoDI.

Il gateway assicura la conformità delle API (sia in fruizione che in erogazione) alle nuove Linee Guida AgID di Interoperabilità, sia per i profili tecnici previsti dal nuovo modello di interoperabilità (ModI), sia per la gestione dei token rilasciati dalla PDND (signed JWT, purposeId, sessionInfo).

Il tutto in maniera trasparente alle applicazioni interne al dominio.

La piattaforma svolge un ruolo di mediazione che permette di semplificare sia le attività di realizzazione dei fruitori di API esterne, che quelle di pubblicazione di proprie API attraverso MODI/PDND.

Si compone di:

• Console di Gestione, è la console utilizzata dagli amministratori della piattaforma per effettuare le configurazioni dei profili MoDI e la pubblicazione delle API.

• Console di monitoraggio, è la console utilizzata dagli amministratori della piattaforma per estrarre i dati di Audit ed è un utile strumento per effettuare il troubleshooting in caso di errori nelle chiamate.

• API Gateway, componente di runtime della piattaforma che ha come finalità essenziale di esporre i servizi messi a disposizione dall'intero sistema in maniera sicura, facilmente fruibile e controllata.

L'API Gateway, dal punto di vista architetturale, è un proxy dei servizi esposti dai sistemi di back-end, in modo tale che tutti i sistemi fruitori debbano effettuare l'accesso a servizi e risorse attraverso questo componente. Dal punto di vista funzionale, il Gateway, riceve le richieste per accedere alle API ed attua le politiche di controllo di accessi, applica le regole di rate limiting e throttling, effettua l’handshake dei certificati per applicare i pattern MoDI e instrada le richieste verso i sistemi remoti.

# Monitoraggio processi e procedimenti (BAM)

La componente offre funzioni per il monitoraggio dei processi/procedimenti (attività svolte, tempi, stato, avanzamento) e di Process Mining.

La componente architetturale permette di costruire una vista chiara dello stato di procedimenti e processi e delle loro performance. In questo modo si intende migliorare il rispetto degli standard di servizio, abilitare un processo decisionale basato sui dati e facilitare la comunicazione interna all’Ente.

Lo strumento che implementa il BAM permette di:

* integrare prodotti e applicativi da cui ottenere i dati necessari al monitoraggio, registrando direttamente dal procedimento o processo via API gli stati e gli eventi o utilizzandone i log;
* avere un modello di gestione dei dati flessibile e scalabile, per ricevere in input informazioni da un parco applicativo vario e da oggetti differenti tra di loro rendendo quanto più facile possibile l’integrazione;
* fornire una vista di business di procedimenti e processi all’interno di una dashboard;
* identificare facilmente e tempestivamente le istanze bloccate o in ritardo;
* integrarsi con le piattaforme di Regione Piemonte, in particolare con l’anagrafica di procedimenti e processi ProceDo e con gli strumenti utilizzati nel quotidiano, come Scrivanie;
* fornire un motore di process mining per analizzare i processi e individuare possibilità di ottimizzazione.

Di seguito in maggiore dettaglio si riporta il set di dati necessari e opzionali per il funzionamento dello strumento:

A screenshot of a computer

Description automatically generated

La modalità di integrazione verso la piattaforma di monitoraggio del BAM avviene in modo asincrono, per evitare una dipendenza diretta rispetto alla disponibilità e alle prestazioni delle funzionalità di business dell’applicazione o della componente trasversale monitorata.

Le modalità con cui i sistemi fruitori potranno fornire le loro informazioni sono:

1. File di log in formato .csv da trasmettere al sistema con cadenza concordata, secondo lo schema di informazioni riportato;
2. Invocazione di API esposta dalla componente MPP di motore di process mining con la trasmissione delle stesse informazioni riportate nello schema sovrastante.