

GATEFIRE

Integrazione “Gateway di Firma Digitale e Archiviazione” - Applicativi Regionali

Requisiti di integrazione

Versione 08

INDICE

1	SCOPO DEL DOCUMENTO	3
1.1	Riferimenti	3
2	GLOSSARIO	3
3	DESCRIZIONE DELLA SOLUZIONE	3
4	GATEWAY DI FIRMA	5
5	GATEWAY REPOSITORY	5
6	SERVIZI FRUIBILI TRAMITE INTEGRAZIONE CON IL SISTEMA GATEFIRE	6
7	TECNOLOGIA DEI SERVIZI ESPOSTI	9

VERIFICHE E APPROVAZIONI

VERSIONE	REDAZIONE		CONTROLLO APPROVAZIONE		AUTORIZZAZIONE EMISSIONE	
	NOME	DATA	NOME	DATA	NOME	DATA
V08	CSI PIEMONTE	31/08/2025	CSI PIEMONTE	31/08/2025	CSI PIEMONTE	31/08/2025
V07	CSI PIEMONTE	07/10/2025	CSI PIEMONTE	07/10/2025	CSI PIEMONTE	07/10/2025
V06	CSI PIEMONTE	08/04/2025	CSI PIEMONTE	08/04/2025	CSI PIEMONTE	08/04/2025
V05	CSI PIEMONTE	19/06/2024	CSI PIEMONTE	19/06/2024	CSI PIEMONTE	19/06/2024
V04	CSI PIEMONTE	10/11/2023	CSI PIEMONTE	10/11/2023	CSI PIEMONTE	10/11/2023
V03	CSI PIEMONTE	16/01/2023	CSI PIEMONTE	16/01/2023	CSI PIEMONTE	16/01/2023
V02	CSI PIEMONTE	08/11/2022	CSI PIEMONTE	08/11/2022	CSI PIEMONTE	08/11/2022
V01	CSI PIEMONTE	02/09/2022	CSI PIEMONTE	02/09/2022	CSI PIEMONTE	02/09/2022

STATO DELLE VARIAZIONI

VERSIONE	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
V08	Tutto il documento	Aggiunta CA Uanataca
V07	Paragrafo 4	Indicazione dei domini di firma supportati
V06	Paragrafo 5	Inserito riferimento al documento di specifiche dettagliato
V05	Paragrafo 5	Correzione refuso
V04	Paragrafo 4	Correzione refuso
V03	Paragrafo 4 e 5	Approfondimento funzioni di firma e funzioni di conferimento
V02	Paragrafo 4	Indicazione per CA Infocert o Aruba
V01	Tutto il documento	Versione iniziale del documento

1 Scopo del documento

Il presente documento è finalizzato a descrivere i requisiti per gestire l'integrazione di un applicativo regionale con la soluzione "Gateway di Firma Digitale e Archiviazione" di seguito denominato GATEFIRE.

1.1 Riferimenti

Num	Riferimento	Autore	Descrizione
[1]	https://www.servizi.piemonte.it/srv/fascicolo-sanitario-elettronico/	CSI Piemonte	Specifiche di Integrazione Sistema Regionale GATEFIRE - Repository Clinico Documentale Aziendale

2 Glossario

Sigla	Acronimo di
FSE	Fascicolo Sanitario Elettronico
DCE	Documento Clinico Elettronico
OTP	One Time Password. Password valida per una singola sessione di accesso o una transazione
XSD.b	Cross Enterprise Document Sharing version b
RCD	Repository Clinico Documentale
PAdES	PDF Advanced Electronic Signature
XAdES	XML Advanced Electronic Signature
CADES	Cryptographic Message Syntax Advanced Electronic Signature

3 Descrizione della soluzione

Il sistema GATEFIRE è una soluzione "middleware" open source facente parte **dell'Ecosistema Sanitario Digitale della Regione Piemonte**, orientata all'orchestrazione di processi di gestione della **firma digitale** e di **conferimento** dei documenti digitali nei **Repository Clinici Documentali Aziendali / Regionali**.

L'istituzione di un sistema unico di firma digitale regionale presenta alcuni peculiari vantaggi:

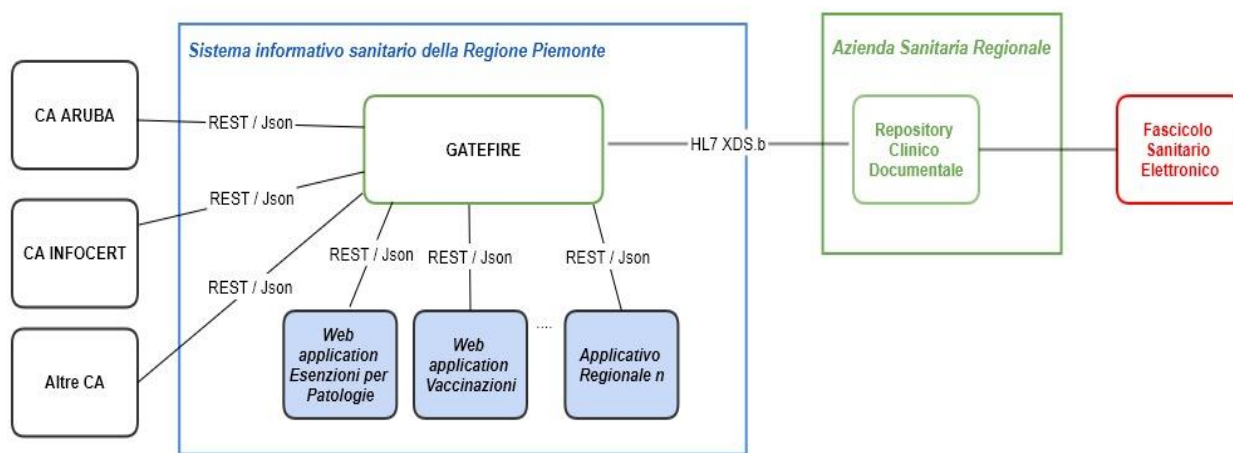
- consente di dare **efficacia probatoria** ai documenti informatici firmati digitalmente, favorendo così i processi di dematerializzazione e consentendo l'automazione e l'ottimizzazione dei processi aziendali.
- favorisce i **processi di dematerializzazione** e consente l'automazione e l'ottimizzazione dei processi aziendali;
- **conformità alla normativa vigente** in materia di firme digitali (CAD d.lgs. 82 del 7 marzo 2005 e successive modifiche);

- **semplifica l'applicazione del servizio di firma digitale** non prevedendo l'uso di dispositivi quali smart card o chiavi USB;
- consente agli operatori di utilizzare le applicazioni regionali e di apporre, dalle applicazioni stesse, la firma digitale attraverso il certificato di firma di cui l'azienda sanitaria ha dotato il professionista previa configurazione del dominio di firma.

Il sistema è attualmente integrato con le Certification Authority ARUBA, INFOCERT e UANATACA consentendo di firmare attraverso le attuali firme in dotazione alle aziende sanitarie locali e agli ospedali piemontesi già configurate.

La scelta dei fornitori è stata dettata dalle dotazioni in essere presso le Aziende Sanitarie pubbliche ad avvio del progetto.

Il sistema è inoltre integrato con i Repository Clinici Documentali delle Aziende Sanitarie Regionali per il conferimento e la gestione dei documenti clinici.



GATEFIRE

Il sistema è composto logicamente da due componenti, rispettivamente denominate “**gateway di firma**” e “**gateway dei repository**” come di seguito descritto.

4 Gateway di firma

La componente logica “**gateway di firma**” consente l’apposizione della firma digitale sui documenti, nonché la verifica della firma e della marca temporale. Il sistema supporta le firme digitali nei formati **PAdES**, per i documenti in formato PDF, **XAdES**, per i documenti in formato XML, e **CAdES**, applicabile a qualsiasi tipologia di documento. Il sistema consente l’utilizzo delle credenziali di firma in possesso delle Aziende Sanitarie Locali e delle Aziende Sanitarie Ospedaliere piemontesi già integrate con GATEFIRE. Si precisa che il sistema **non gestisce firme automatiche ARUBA**. Per la CA **Uanataca**, le firme automatiche prevedono tre fattori di firma, mentre le firme remote prevedono quattro fattori.

Di seguito sono elencate le singole funzionalità previste dal sistema:

- apposizione di firma digitale remota PAdES
- apposizione di firma digitale remota massiva PAdES
- apposizione di firma digitale remota automatica PAdES (non disponibile per CA ARUBA)
- apposizione di firma digitale remota XAdES
- apposizione di firma digitale remota massiva XAdES
- apposizione di firma digitale remota automatica XAdES (non disponibile per CA ARUBA)
- apposizione di firma digitale remota CAdES
- apposizione di firma digitale remota massiva CAdES
- apposizione di firma digitale remota automatica CAdES (non disponibile per CA ARUBA)
- apposizione della marca temporale
- richiesta OTP
- verifica della validità della firma digitale
- verifica della validità della marca temporale
- apertura sessione remota (solo CA ARUBA)
- chiusura sessione remota (solo CA ARUBA)

5 Gateway repository

La componente logica “**gateway dei repository**” consente di gestire l’interazione con i repository clinici documentali delle aziende sanitarie regionali. Il sistema mette a disposizione le seguenti funzionalità:

- archiviazione dei documenti negli RCD delle ASR
- recupero dei documenti dagli RCD delle ASR
- modifica metadati relativi ai documenti già inviati agli RCD delle ASR

Per quanto riguarda l'integrazione con i RCD delle ASR per l'archiviazione dei documenti, il sistema supporta le transazioni previste dal profilo **XDS.b**. I casi prevedono l'invio di un nuovo documento e relativi metadati, l'aggiornamento dei metadati di un documento già inviato, la ricerca e recupero di un documento e relativi metadati e la sostituzione di un documento già inviato.

Rispetto a tale profilo il sistema GATEFIRE interpreta gli attori Document Source e Document Consumer nei rispettivi casi di invio e recupero documento dal Repository Aziendale; Document Administrator nel caso di modifica dei metadati di un documento già inviato. Il Repository Aziendale interpreta gli attori Document Registry e Document Repository.

A seguito del buon esito dell'invio del documento firmato digitalmente da parte di GATEFIRE al Repository, non è prevista l'archiviazione del documento all'interno del sistema né all'interno dell'applicativo verticale chiamante.

L'applicativo verticale dovrà conservare le informazioni strettamente necessarie al recupero dello stesso per le successive consultazioni.

Il dettaglio relativo delle specifiche di integrazione del sistema GATEFIRE con i Repository Clinici Documentali delle aziende si trova in [1].

6 Servizi fruibili tramite integrazione con il sistema GATEFIRE

Di seguito l'elenco dei servizi esposti dal sistema.

Servizio	Obiettivo
Apposizione remota firma digitale PAdES	Permette di apporre una firma digitale remota di tipo PAdES ad un file utilizzando la Certification Authority richiesta dall'applicativo chiamante (che può essere Aruba, Infocert o Unataca). Modalità di esecuzione: sincrona.
Apposizione remota firma digitale massiva PAdES	Permette di apporre una firma digitale remota di tipo PAdES, ad un gruppo di file, in modo simultaneo, utilizzando la Certification Authority richiesta dall'applicativo chiamante(che può essere Aruba, Infocert o Unataca)). Restituisce un file zip contenente tutti i file firmati. Modalità di esecuzione: sincrona.

Servizio	Obiettivo
Apposizione remota firma digitale automatica PAdES	Operazione adatta per sessioni di firma batch, senza l'intervento esplicito di un operatore. Le credenziali sono fisse e non è necessario utilizzare un OTP generato al momento (disponibile solo per Infocert e Uanataca e non per Aruba) . Modalità di esecuzione: sincrona.
Apposizione remota firma digitale XAdES	Permette di apporre una firma digitale remota di tipo XAdES ad un file utilizzando la Certification Authority richiesta dall'applicativo chiamante (che può essere Aruba, Infocert o Uanataca). Modalità di esecuzione: sincrona.
Apposizione remota firma digitale massiva XAdES	Permette di apporre una firma digitale remota di tipo XAdES, ad un gruppo di file, in modo simultaneo, utilizzando la Certification Authority richiesta dall'applicativo chiamante.(che può essere Aruba, Infocert o Uanataca) Restituisce un file zip contenente tutti i file firmati. Modalità di esecuzione: sincrona.
Apposizione remota firma digitale automatica XAdES	Operazione adatta per sessioni di firma batch, senza l'intervento esplicito di un operatore. Le credenziali sono fisse e non è necessario utilizzare un OTP generato al momento (disponibile solo per Infocert e Uanataca e non per Aruba)) . Modalità di esecuzione: sincrona.
Apposizione remota firma digitale CAdES	Permette di apporre una firma digitale remota di tipo CAdES ad un file utilizzando la Certification Authority richiesta dall'applicativo chiamante (che può essere Aruba, Infocert o Uanataca). Modalità di esecuzione: sincrona.
Apposizione remota firma digitale massiva CAdES	Permette di apporre una firma digitale remota di tipo CAdES, ad un gruppo di file, in modo simultaneo, utilizzando la Certification Authority richiesta dall'applicativo chiamante (che può essere Aruba, Infocert o Uanataca) Restituisce un file zip contenente tutti i file firmati. Modalità di esecuzione: sincrona.

Servizio	Obiettivo
Apposizione remota firma digitale automatica CAdES	Operazione adatta per sessioni di firma batch, senza l'intervento esplicito di un operatore. Le credenziali sono fisse e non è necessario utilizzare un OTP generato al momento (disponibile solo per Infocert e Uanataca e non per Aruba)). Modalità di esecuzione: sincrona.
Apposizione remota marca temporale	Permette di apporre una marca temporale di tipo tsr e tsd ad un file, utilizzando la Certification Authority richiesta dall'applicativo chiamante (che può essere Aruba, Infocert o Uanataca). Opzionalmente, permette il conferimento nei repository. Modalità di esecuzione: sincrona.
Verifica remota firma digitale	Permette di verificare le informazioni relative alla firma digitale presente su un file. Restituisce un set di informazioni relative alla firma digitale. Modalità di esecuzione: sincrona.
Verifica remota marca temporale	Permette di verificare le informazioni relative alla marca temporale presente su un file. Restituisce un set di informazioni relative alla marca temporale. Modalità di esecuzione: sincrona.
Richiesta OTP	Consente di richiedere un OTP per la firma remota. Restituisce l'OTP all'utente secondo le modalità previste dalla CA (infocert via SMS, Aruba via SMS o Arubacall e Uanataca via SMS) Modalità di esecuzione: sincrona.
Apertura remota sessione	Permette di aprire una sessione remota presso una Certification Authority (al momento solo supportata da Aruba). L'apertura della sessione viene eseguita utilizzando la Certification Authority richiesta dall'applicativo chiamante. Restituisce un identificativo della sessione che può essere utilizzato per l'esecuzione della firma digitale massiva. Modalità di esecuzione: sincrona.

Servizio	Obiettivo
Chiusura remota sessione	Permette la chiusura di una sessione remota presso una Certification Authority (al momento solo supportata da Aruba) utilizzando la Certification Authority richiesta dall'applicativo chiamante. Modalità di esecuzione: sincrona.
Conferimento documento su RCD della ASR	Permette il conferimento di un file ricevuto in input da un'applicazione chiamante presso l' RCD della ASR. Modalità di esecuzione: sincrona.
Recupero documento su RCD della ASR	Permette di recuperare un documento dal RCD della ASR. Modalità di esecuzione: sincrona.
Modifica metadati relativi ad un documento conferito su RCD della ASR	Permette di modificare i metadati di un documento archiviato sul RCD della ASR. Modalità di esecuzione: sincrona.

7 Tecnologia dei servizi esposti

I servizi esposti dal sistema sono realizzati in tecnologia web services SOAP e API/REST.