Specifiche di Integrazione
Sistema Regionale GATEFIRE -
Repository Clinico Documentale Aziendale

Versione 07

VERIFICHE E APPROVAZIONI

VERSIONE	REDAZIONE		CONTROLLO APPROVAZIONE		AUTORIZZAZIONE EMISSIONE	
	NOME	DATA	NOME	DATA	NOME	DATA
V07	CSI PIEMONTE	11/11/2025	CSI PIEMONTE	11/11/2025	CSI PIEMONTE	25/09/2025
V06	CSI PIEMONTE	22/09/2025	CSI PIEMONTE	22/09/2025	CSI PIEMONTE	22/09/2025
V05	CSI PIEMONTE	05/03/2025	CSI PIEMONTE	05/03/2025	CSI PIEMONTE	05/03/2025
V04	CSI PIEMONTE	28/10/2024	CSI PIEMONTE	28/10/2024	CSI PIEMONTE	28/10/2024
V03	CSI PIEMONTE	28/02/2024	CSI PIEMONTE	28/02/2024	CSI PIEMONTE	28/02/2024
V02	CSI PIEMONTE	29/11/2023	CSI PIEMONTE	29/11/2023	CSI PIEMONTE	29/11/2023
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
V07	Paragrafo 3.8, 3.9, 3.10, 3.11	Inseriti esempi di slot custom Aggiornate specifiche Autenticazione Security Token Service
V06	Paragrafo 3.7	Indicazione relativa alla obbligatorietà per l'idAura del paziente
V05	Tutto il documento	Revisione documento
V04	Paragrafo 3.1	Aggiornata immagine transazioni attori

V03	Paragrafo 3.9, 3.10, 3.11	Aggiunta sezione autenticazione, gestione errori, censimento nuovo repository
V02	Paragrafo 3.7 e 3.8	Aggiunti gli attributi per adeguamento FSE affinity domain 2.4.1
V01	Tutto il documento	Versione iniziale del documento

Indice generale

1 Scopo e riferimenti del documento

1.1 Scopo del documento

Scopo del presente documento è descrivere le Specifiche di integrazione del Sistema Regionale GATEFIRE con i Repository Clinici Documentali delle Aziende Sanitarie Regionali.

1.1 Riferimenti

Num.	Riferimento	Data	Autore	Descrizione
[1]	http://www.hl7italia.it/hl7italia_D7/hl7it_publications	n.a.	HL7-Italia	Specifiche HL7 Italia
[2]	http://www.sistemapiemonte.it/eXoRisorse/dwd/servizi/FascicoloSanitarioOperatori/2023/Linee_guida_per_la_gestione_di_un_DCE_V11.pdf	Ottobre 2023	CSI Piemonte	Linee guida per la gestione di un Documento Clinico Elettronico finalizzata alla pubblicazione su FSE e ROL
[3]	https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2015-11-11&atto.codiceRedazionale=15G00192&atto.articolo.numero=0&atto.articolo.sottoArticolo=1&atto.articolo.sottoArticolo1=10&qId=98af9a3f-5e25-4113-8c51-3469c77b4439&tabID=0.14144806886991423&title=lbl.dettaglioAtto	Settembre 2015	Ministero della salute	Regolamento in materia di Fascicolo sanitario elettronico – Decreto n.178 29 settembre 2015
[4]	Affinity domain Italia	Febbraio 2023	Agid	https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2023/02/10/interoperabilita-sistemi-regionali-fse-online-versione-241-specifiche-tecniche
[5]	http://www.sistemapiemonte.it/eXoRisorse/dwd/servizi/FascicoloSanitarioOperatori/2023/DMA-CL-SRS-15-V38-Specifica_protocollo_interoperabilita_CL_dip_con_e_senza_invio_referti-XML.pdf	Novembre 2023	CSI Piemonte	Specifiche del protocollo di interoperabilità via Web Service XML/SOAP
[6]	https://profiles.ihe.net/ITI/TF/Volume2/index.html#3	n.a.	IHE International	Infrastructure Technical Framework, Volume 2b (ITI TF-2b): Transactions Part B".
[7]	https://profiles.ihe.net/ITI/TF/Volume3/index.html	n.a.	IHE International	Specifiche dei metadata
[8]	http://www.hl7italia.it/hl7italia_D7/hl7it_publications	n.a.	HL7 Italia	Implementation Guide CDA-R2

1.2 Glossario

Di seguito sono elencati acronimi o termini utilizzati nel presente documento.

ASR	Aziende Sanitarie Regionali
FSE	Fascicolo Sanitario Elettronico
DCE	Documento Clinico Elettronico
HL7	Health Level 7
IHE	Integrating Healthcare Enterprise
Web app	Web Application
RCD	Repository Clinico Documentale
XDS.b	Cross Entreprise Document Sharing version b

2 Introduzione

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

Il **Documento Clinico Elettronico** conferito sul **Repository** della Azienda Sanitaria Regionale dovrà essere inviato al **Fascicolo Sanitario Elettronico** dalla ASR stessa secondo le modalità di invio già previste.

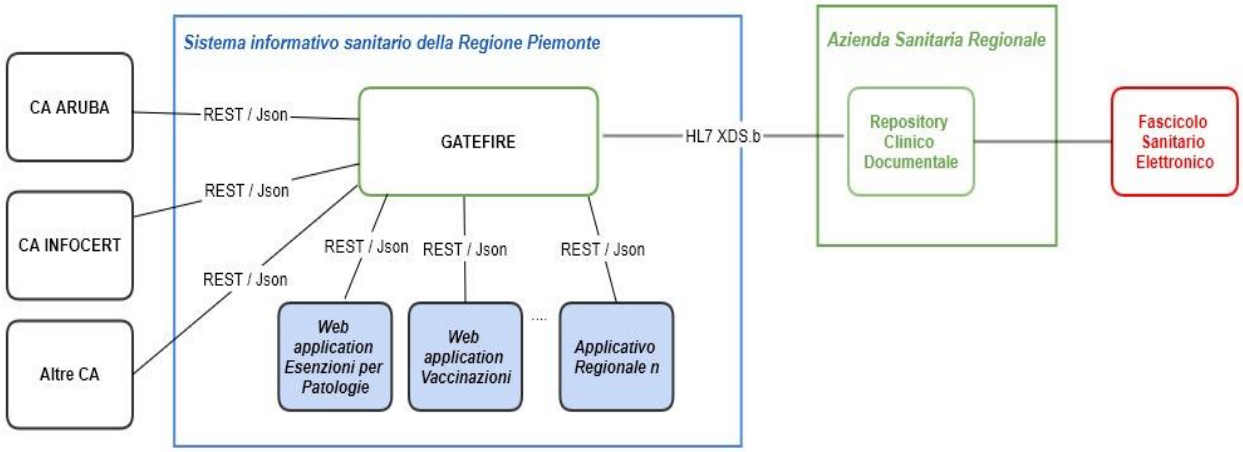

Diagramma di Contesto sistema GATEFIRE

La creazione dei documenti clinici e l'invio ai Repository dovrà essere conforme alle "**Linee guida per la gestione di un Documento Clinico Elettronico**" descritte in [2] all'interno delle regole definite nell'**Affinity Domain** di riferimento per l'interoperabilità dei sistemi di Fascicolo Sanitario Elettronico (FSE) tra le Regioni e Province Autonome italiane attraverso l'Infrastruttura Nazionale per l'Interoperabilità (INI). [4]

Il modello descritto prevede l'utilizzo del profilo XDS.b.

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 dell'applicativo verticale chiamante né all'interno del sistema GATEFIRE. L'applicativo verticale dovrà conservare le informazioni strettamente necessarie al recupero dello stesso per le successive consultazioni.

3 Produzione del documento clinico e integrazione con Repository Clinico Documentali delle ASR

3.1 Transazioni IHE

Il sistema realizza l'interazione con i Repository Clinici Documentali attraverso il profilo di integrazione XDS.b come di seguito descritto.

Attori XDS

Document Source Il produttore di documenti è il sistema applicativo regionale che mette a disposizione i documenti prodotti su PDF/A-2 contenente il CDA-R2 e firmato PAdES/BES.

Document Repository - Responsabile dell'immagazzinamento delle informazioni in modo trasparente, sicuro, affidabile e persistente e si occupa della risposta alle richieste di documenti.

Document Registry - Componente responsabile dell'immagazzinamento di documenti in modo che quelli che sono di interesse per la cura del paziente possano essere facilmente trovati, selezionati e recuperati indipendentemente dal luogo in cui sono effettivamente memorizzati.

PIX Patient Identity Source - Il sistema di gestione dell'anagrafe aziendale AULA che deve mantenersi allineato con il sistema di anagrafe regionale (AURA).

Document Consumer - Il fruitore di documenti può essere l'applicativo che ha creato il documento o un applicativo diverso, con lo scopo di visualizzare il documento richiesto (prodotto su PDF/A-2 contenente il CDA-R2 e firmato PAdES/BES).

Document Administrator – Responsabile dell'aggiornamento dei metadati relativi ad un documento.

Il sistema **GATEFIRE** supporta le transazioni previste dal profilo XDS.b per:

- l'invio di un nuovo documento e relativi metadati nel repository aziendale,
- l'aggiornamento dei metadati di un documento già inviato,
- la ricerca e recupero di un documento e relativi metadati,
- l'annullamento di un documento già inviato.

Transazione [ITI-41] Provide and Register Document Set-b

La transazione [ITI-41] Provide and Register Document Set-b permette di pubblicare un documento nel repository trasmettendo contestualmente i metadati ad esso associati. Per la struttura dei messaggi si faccia riferimento a [6].

Gli attori coinvolti sono il sistema GATEFIRE come Document Producer ed il Repository Aziendale che valida i metadati ricevuti, li completa e provvede alla registrazione sul Document Registry.

Transazione [ITI-57] Update Document Set

La transazione [ITI-57] Update Document Set è utilizzata per effettuare l'update di uno o più metadati associati ad un documento precedentemente inviato. Per la struttura dei messaggi si faccia riferimento a [6].

Gli attori coinvolti sono il sistema GATEFIRE come Document Administrator ed il Registry dell'Azienda Sanitaria.

Transazione [ITI-18] Registry Stored Query

La transazione [ITI-18] Registry Stored Query è utilizzata dal sistema GATEFIRE per ricercare un documento all'interno del Repository. Per la struttura dei messaggi si faccia riferimento a [6].

Gli attori coinvolti sono il sistema GATEFIRE come Document Consumer ed il Registry dell'Azienda Sanitaria, è possibile ricercare il documento recuperandone i metadati ed i riferimenti al Document Repository dove è disponibile.

Transazione [ITI-43] Retrieve Document Set-b

La transazione [ITI-43] Retrieve Document Set-b è utilizzata per recuperare uno o più documenti dal repository. Per la struttura dei messaggi si faccia riferimento a [6].

Gli attori coinvolti sono il sistema GATEFIRE come Document Consumer ed il Repository dell'Azienda Sanitaria. Il Document Consumer ha già ottenuto il XDSDocumentEntry UniqueID e il repository di Document Repository UniqueId dal Registry tramite la transazione ITI-18.

3.2 Casi d'Uso supportati dal Sistema

Di seguito vengono descritti i casi d'utilizzo del sistema e le transazioni IHE coinvolte.

Un applicativo regionale tramite l'integrazione con il sistema GATEFIRE può prevedere i seguenti casi di gestione del documento verso il Repository Clinico Documentale dell'Azienda Sanitaria di riferimento:

- invio di un nuovo documento;
- ricerca e recupero di un documento;
- aggiornamento dei metadati relativi ad un documento già inviato;
- annullamento di un documento già inviato.

Invio di un nuovo documento

L'invio di un nuovo documento prevede l'invio del documento stesso insieme ai metadati previsti dall'Affinity Domani di riferimento. Il sistema GATEFIRE prevede anche l'invio di alcuni slot custom necessari per l'integrazione con il Fascicolo Sanitario Elettronico come descritto al paragrafo 3.8.

All'invio di un nuovo documento il sistema applicativo regionale non tiene copia del documento inviato al Repository memorizzando solo i dati necessari al recupero dello stesso. Il documento inviato al Repository viene inviato al FSE dell'assistito secondo le modalità di integrazione tra RCD dell'ASR e FSE già previste.

Ricerca e recupero di un documento

Il recupero del documento avviene in due fasi, la chiamata al XDS Document Registry per il recupero dei riferimenti del documento e la chiamata al XDS Document Repository per il recupero del documento.

Aggiornamento metadati di un documento inviato

È possibile aggiornare i metadati relativi ad un documento inviato effettuando una chiamata di Registry Stored Query per il recupero dei riferimenti e dei metadati del documento ed una chiamata di Update Document Set inviando i metadati aggiornati.

Annullamento di documento inviato

In caso di invio errato di un documento è possibile inviare un documento annullativo. In questo caso è necessario effettuare il recupero dei riferimenti del documento dal XDS Document Registry tramite una chiamata di Registry Stored Query e successivamente effettuare un invio di REPLACE di un documento annullativo al XDS Document Repository tramite una chiamata di Provide and Register Document Set-b di REPLACE per annullamento.

Nel caso di invio di REPLACE di un documento annullativo il documento annullato non dovrà essere più visibile sul Fascicolo Sanitario Elettronico dell'assistito.

Caso d'uso	Transazioni coinvolte	Riferimenti
Invio nuovo documento e relativi metadati	ITI-41 per l'invio	https://profiles.ihe.net/ITI/TF/Volume2/ITI-41.html
Ricerca e Recupero documento	ITI-18 per recupero riferimenti documento	https://profiles.ihe.net/ITI/TF/Volume2/ITI-18.html
	ITI-43 per recupero documento	https://profiles.ihe.net/ITI/TF/Volume2/ITI-43.html
Aggiornamento metadati relativi ad un documento già inviato	ITI-18 per recupero riferimenti documento	https://profiles.ihe.net/ITI/TF/Volume2/ITI-18.html
	ITI-57 di update metadata	https://profiles.ihe.net/ITI/TF/Volume2/ITI-57.html
Annullamento di un documento già inviato	ITI-18 per recupero riferimenti documento	https://profiles.ihe.net/ITI/TF/Volume2/ITI-18.html
	ITI 41 di REPLACE per annullamento	https://profiles.ihe.net/ITI/TF/Volume2/ITI-41.html

3.3 Il Documento Clinico Elettronico

I documenti clinici elettronici realizzati tramite gli applicativi regionali integrati con il sistema GATEFIRE dovranno essere realizzati seguendo le linee guida descritte in [2], in particolare il processo di produzione del documento dovrà prevedere i seguenti passi:

- **Produrre il CDA-R2** - La parte di CDA-R2 è elaborata seguendo le indicazioni di HL7 Italia che dipendono dalla tipologia di documento realizzato e sono pubblicate in [7];
- **Produrre il PDF** - Il documento PDF prodotto è originato dalla produzione del CDA-R2 nella versione PDF/A-2 (basato sullo standard PDF 1.7 (ISO 32000-1:2008)) che prevede la possibilità di iniettare l'XML nella struttura XFA;

- **Preparazione dei Metadati** - I metadati, ovvero la parte di indicizzazione del documento contenuta nella parte Registry della soluzione, devono anche contenere informazioni di utilità all'Interoperabilità dei documenti richiesti dall'adozione delle regole dell'INI.

3.4 XDSDocumentEntry.uniqueId

Al fine di adeguarsi al modello di interoperabilità nazionale, l'attributo XDSDocumentEntry.uniqueId è codificato con un OID univoco all'interno della Regione Piemonte, definito secondo il seguente formato:

- una stringa fissa uguale "2.16.840.1.113883.2.9.2.10.4.4" (porzione di codice comune a tutti i documenti della Regione Piemonte);
- <.10> (codice che identifica le strutture pubbliche);
- <000> (applicativi della Regione Piemonte);
- <AAA > (identificativo del sistema verticale regionale inviante (ad esempio 010 per Esenzioni per patologie));
- <BBB> (codice identificativo della ASL di riferimento);
- <NNNNNNNNNNNNNNNNNNNNN> progressivo numerico, che renda univoco l'OID del documento e con un numero di 22 caratteri numerici.

Di seguito un esempio: 2.16.840.1.113883.2.9.2.10.4.4.1000001021100000000000000000000028

L'identificativo univoco del documento (OID) viene generato al momento della creazione del documento, seguendo le specifiche nazionali e quindi rimanendo univoco a livello nazionale e regionale.

3.5 XDSSubmissionSet.uniqueId

L'attributo XDSSubmissionSet uniqueId è l'indentificatore univoco assegnato dall'attore che richiede lo stesso SubmissionSet (identificativo univoco della Submission assegnato dal XDS Document Source). Il dato è implementato dal sistema GATEFIRE secondo le seguenti specifiche:

- una stringa fissa uguale "2.16.840.1.113883.2.9.2.10" (Ramo OID Regione Piemonte);
- <.4.3>;
- <X>, dove X è valorizzato come:
  - <10000> =struttura inviante (10= struttura pubblica e 000=CSI Piemonte);
  - <010> = identificativo dell'applicativo verticale regionale che si occupa della creazione del documento (ad esempio 010 per Esenzioni per patologie);
  - <timestamp>.

3.6 XDSSubmissionSet.sourceId

L'attributo XDSSubmissionSet.sourceId è l'identificatore univoco assegnato dall'attore Document Source che produce ed inserisce il documento. Il dato è implementato dal sistema GATEFIRE secondo le seguenti specifiche:

- una stringa fissa uguale "2.16.840.1.113883.2.9.2.10" (Ramo OID Regione Piemonte);
- <.4.5>;
- <X>, dove X è valorizzato come:
  - <10000> =struttura inviante (10= struttura pubblica e 000=CSI Piemonte);
  - <010> = identificativo dell'applicativo verticale regionale che si occupa della creazione del documento (ad esempio 010 Esenzioni per patologie);

Esempio: 2.16.840.1.113883.2.9.2.10.4.5.1000010

3.7 Specifiche dei metadati dei documenti XDS-DocumentEntry XDS SubmissionSet

I metadati devono essere implementati e valorizzati secondo le specifiche definite in [7].

Di seguito si riporta l'elenco dei metadati con le relative descrizioni e con l'indicazione dell'obbligatorietà di ciascuno.

Attributo di XDSDocumentEntry	(sotto-attributo)	Document Entry - - XDSDocumentEntry: descrizione attributi	Submission Set -- XDSSubmissionSet: descrizione degli attributi	Obbligatorietà
author		Rappresenta la persona e/o la macchina che ha scritto il documento. Questo attributo definisce una struttura di classificazione ebRIM contenente i seguenti sottoattributi: · authorPerson – zero o più · authorRole – zero o più · authorSpecialty – zero o più · authorInstitution – zero o più · authorTelecommunication – zero o più Devono essere presenti almeno un sotto-attributo di authorPerson, authorTelecommunication o authorInstitution, quando l'attributo dell'author è incluso nei metadati.	Rappresenta la persona e/o la macchina che autorizza il SubmissionSet. Quest'attributo definisce una struttura di classificazione ebRIM contenente i seguenti sottoattributi: · authorPerson – zero o più · authorRole – zero o più · authorSpecialty – zero o più · authorInstitution – zero o più · authorTelecommunication – zero o più	sì
	authorPerson (sotto-attributo di author)	Rappresenta l'umano e/o la macchina che ha scritto il documento all'interno del authorInstitution. L'autore può essere il paziente stesso. Se l'autore è una persona fisica, allora l'identificatore corrisponderà al numero del codice fiscale. Il cognome, nome e prefisso vengono aggiunti al codice fiscale..	Rappresenta la persona e/o la macchina autore del documento all'interno dell'authorInstitution. Se l'autore è una persona fisica, l'identificativo deve corrispondere al codice fiscale (CF) Al Codice Fiscale sono aggiunti Cognome, Nome e Prefisso.	sì
	authorRole (sotto-attributo di author)	Ruolo dell'autore del documento	Ruolo dell'autore del documento	no
	authorSpecialty (sotto-attributo di author)	Specialità all'interno della struttura sanitaria nella quale è prodotto il documento.	Specialità all'interno della struttura sanitaria nella quale è prodotto il documento.	no

	authorInstitution (sotto-attributo di author)	Struttura sanitaria in base alla quale l'uomo e/o le macchine siano gli autori del documento. L'elenco dei codici ammessi sono definiti in [4].		sì
	authorTelecommunication (sotto-attributo di author)	Indirizzo telecomunicazioni (es. e-mail), del documento o dell'autore di SubmissionSet.	Indirizzo di telecomunicazione (e.g., e-mail) del documento o dell'autore del SubmissionSet.	no
classCode		Classificazione del tipo di documento. I valori possibili per l'attributo di classCode sono definiti in [4]		sì
confidentialityCode		Livello di riservatezza del documento: i tag di sicurezza e di privacy del documento. L'elenco dei codici ammessi sono definiti in [4].		sì
entryUUID		UUID	Identifier globalmente univoco.	sì
eventCodeList		Rappresenta i principali atti clinici che vengono documentati. Utilizzato anche per specificare la visibilità del documento I valori utilizzabili sono definiti in [4].		no
formatCode		Formato del documento. Assieme al metadato typeCode permette di capire la tipologia del documento. I valori utilizzabili sono definiti in [4].		sì
hash		Hash del documento calcolato usando l'algoritmo SHA 1.		no
healthcareFacilityTypeCode		Modalità organizzativa che ha portato alla creazione del documento. I valori utilizzabili sono definiti in [4].		sì
languageCode		Valore costante: "it-IT"		sì
legalAuthenticator		Rappresenta l'operatore all'interno dell autorInstitution che ha legittimamente certificato o attestato il documento.		no
legalAuthenticatorTime		Data/ora della firma digitale.		no
mimeType		Il MIME type del documento nel Repository.		sì
patientId		Il patientId rappresenta il soggetto principale del documento. All'interno di una richiesta di submission, il valore del patientId del DocumentEntry coincide con quello del SubmissionSet. L'eventuale valorizzazione con l'identificativo univoco locale del paziente all'interno dell'azienda (idAULA) è a carico del Repository.	Il patientId è il soggetto principale della cura del SubmissionSet	sì
practiceSettingCode		Specialità clinica in cui è stato eseguito l'atto che ha portato alla creazione del documento I valori utilizzabili sono definiti in [4].		sì
referenceIdList	Inseriamo NRE ad esempio	Lista contenete zero o più Identificatori (Identifiers).		no

		.		
repositoryUniqueId		Identifica in maniera univoca a livello nazionale il Repository che custodisce il documento che deve essere indicizzato.		no
serviceStartTime		Data e ora di inizio prestazione che viene documentata o data inizio episodio.		no
serviceStopTime		Data e ora di fine prestazione che viene documentata o data fine episodio.		no
sourcePatientId		Identificativo del paziente all'interno del dominio in cui è avvenuto l'evento che ha portato alla creazione di un documento. Codice Fiscale e idAura se presente (l'id aura potrebbe non essere presente ad esempio per cittadini assistiti fuori regione Piemonte) CF^^^&2.16.840.1.113883.2.9.4.3.2&ISO 12345678^^^&2.16.840.1.113883.2.9.2.10&ISO		sì
sourcePatientInfo		Metadato che permette di veicolare informazioni anagrafiche relative al paziente titolare del documento. Esempio: PID-3|CF ^^^&2.16.840.1.113883.2.9.4.3.2&ISO PID-5|PROVA^PROVA^^^ PID-7|19278901 PID-8|F PID-11 PID-11|^^PIANAVIA^^^100^N^^008828 PID-11 à N per nascita (999xxx nati estero) PID-11 à L per residenza PID-11 à H per domicilio		no
typeCode		Codice che specifica il tipo di documento. I valori utilizzabili sono definiti in [4].		sì
uniqueId		Identificativo univoco e globale assegnato al documento da parte del Document Source. Vedi paragrafo 3.4.		sì
URI		URI del documento		no

3.8 Slot Custom per Fascicolo Sanitario Elettronico Regione Piemonte

Il sistema, all'interno delle transazioni, gestisce alcuni slot custom definiti per supportare le valorizzazioni di alcuni campi richiesti dal Fascicolo Sanitario Elettronico della Regione Piemonte.

Di seguito l'elenco dei campi supportati. Per approfondimenti si faccia riferimento a [2] e [5].

Attributo	Descrizione	Slot
creationTime	Rappresenta l'instante in cui l'autore crea il documento nel Document Source, nel formato "YYYYMMDDhhmmss", dove "hh" è codificato sulle 24 ore.	<ns2:Slot name="creationTime"> <ns2:ValueList> <ns2:Value>20251007220000</ns2:Value> </ns2:ValueList>

		</ns2:Slot>
firmatoDigitalmente	True/False	<ns2:Slot name="firmatoDigitalmente"> <ns2:ValueList> <ns2:Value>true</ns2:Value> </ns2:ValueList> </ns2:Slot>
mediciValidatori	vedi legalAuthenticator se presente nei metadati (o author)	
dataOraFirmaDocumento	vedi legalAuthenticatorTime se presente nei metadati	<rim:Slot name="dataOraFirmaDocumento">
mediciRedattori	vedi author	
documentoAnnullativo	true/false	<rim:Slot name="documentAnnullativo">
codiceLuogoAccettazione	codice MUP ARPE	<rim:Slot name="codiceLuogoAccettazione">
codiceLuogoDimissione	codice MUP ARPE	<rim:Slot name="codiceLuogoDimissione">
codiceCentroPrelievi		<rim:Slot name="codiceCentroPrelievi">
tipoFirma	PB Pades	<ns2:Slot name="tipoFirma"> <ns2:ValueList> <ns2:Value>PB</ns2:Value> </ns2:ValueList> </ns2:Slot>
codicePIN	obbligatorio se previsto Ritiro On Line	
codiceDocumentoScaricabile	obbligatorio se previsto Ritiro On Line	
dataDisponibilitaReferto	data in cui sarà disponibile il referto per lo scarico on-line	
pagatoTicket	Indica lo stato di pagamento del ticket - obbligatorio se invioFSE=1	
importoTicketDaPagare	se previsto Ritiro On Line	
importoTicketPagato	se previsto Ritiro On Line	
privacyDocumento		<rim:Slot name="privacyDocumento">
oscuraScaricoCittadino		<rim:Slot name="oscuraScaricoCittadino">
scaricabileDalCittadino		<rim:Slot name="scaricabileDalCittadino">
soggettoALeggiSpeciali		<rim:Slot name="soggettoALeggiSpeciali">
invioFSE	0 documento da NON inviare a FSE / 1 documento da inviare a FSE	<ns2:Slot name="invioFSE"> <ns2:ValueList> <ns2:Value>1</ns2:Value> </ns2:ValueList> </ns2:Slot>
invioCLS	0 da NON inviare in conservazione / 1 da inviare in conservazione	<ns2:Slot name="invioCLS"> <ns2:ValueList> <ns2:Value>0</ns2:Value> </ns2:ValueList> </ns2:Slot>
tipoEpisodio (O/I/E)		<rim:Slot name="tipoEpisodio">
codiceApplicativo		<rim:Slot name="codiceApplicativo">
tokenConservazione	valorizzato dal Sistema di Conservazione Legale, post conservazione	
tipoEpisodioOriginanteRichiesta	opzionale e solo per episodi I o E	<rim:Slot name="tipoEpisodioOriginanteRichiesta">
regime		<rim:Slot name="urn:ita:2022:administrativeRequest"> <rim:ValueList> <rim:Value> SSN^Regime SSN</rim:Value> </rim:ValueList> </rim:Slot>
SubjectApplication	Stringa che riporta codice applicativo, codice fornitore e versione	<ns2:Slot name="SubjectApplication"> <ns2:ValueList> <ns2:Value>ESENPAT^CSI Piemonte^1.0.0</ns2:Value> </ns2:ValueList> </ns2:Slot>

3.9 Autenticazione Security Token Service

Il servizio di conferimento di **Gatefire** utilizza un meccanismo di autenticazione basato su **Security Token Service (STS)**, in conformità agli standard **OASIS WS-Trust 1.2**:
http://docs.oasis-open.org/ws-sx/ws-trust/v1.2/ws-trust.html

La piattaforma dell'Azienda Sanitaria deve pertanto esporre un servizio STS per il rilascio di un **Security Token (asserzione SAML 2.0)** necessario per l'accesso ai servizi dedicati alla gestione delle transazioni ITI.

Per ogni informazione non esplicitamente contenuta nel presente documento si rimanda alla documentazione dello standard WS-Trust sopra citato.

Il servizio STS deve rispettare i seguenti criteri:

- L'elemento <wst:KeyType> specifica il tipo di chiave utilizzata per il rilascio del token.
  Il valore supportato è **SymmetricKey**.
  In questo profilo il token deve essere firmato utilizzando una chiave simmetrica derivata dal "entropy" condiviso tra client e STS.
- L'**algoritmo di firma** utilizzato per la generazione dell'asserzione SAML deve essere basato su **SHA1**, in particolare:
  - http://www.w3.org/2000/09/xmldsig#hmac-sha1 per firme **simmetriche**, oppure
  - http://www.w3.org/2000/09/xmldsig#rsa-sha1 per firme **asimmetriche**, nel caso in cui si utilizzi una chiave pubblica con certificato X.509.
    L'utilizzo di algoritmi **SHA256 (es. RSA-SHA256)** non è supportato dalla policy WS-Security configurata nel sistema Gatefire (**Basic256**) e causa l'esito negativo della validazione CXF.
- L'elemento <wsp:AppliesTo> deve indicare l'endpoint applicativo al quale il token rilasciato verrà presentato.

Il token rilasciato deve risultare valido alla verifica WS-Security eseguita dal client CXF di Gatefire, che include il controllo del timestamp, della firma digitale e della coerenza del certificato (se presente), secondo le impostazioni della policy Basic256.

L'elemento <wst:Claims> definisce i *claims* supportati:

Claim URI	Descrizione	Obbligatorietà
http://wso2.org/claims/givenname	Nome dell'utente oppure codice applicazione	Opzionale
http://wso2.org/claims/codiceFiscale	Codice fiscale dell'utente	Opzionale
http://wso2.org/claims/lastname	Cognome dell'utente oppure codice applicazione	Opzionale
http://wso2.org/claims/role	Ruoli dell'utente (separati da virgola)	Opzionale

3.9.1 Binding SOAP

Il profilo WS-Trust adottato da Gatefire utilizza binding SOAP 1.2, con namespace:

http://www.w3.org/2003/05/soap-envelope

Tutti i messaggi di richiesta (RequestSecurityToken) e risposta (RequestSecurityTokenResponse) devono essere incapsulati in un envelope SOAP 1.2

È importante che l'STS utilizzi coerentemente SOAP 1.2 sia in richiesta che in risposta, per garantire la corretta validazione del blocco <wsse:Security> e la piena interoperabilità con i client CXF di Gatefire.

3.10 Gestone errori

In caso di esito negativo nella validazione WS-Security o nella fase di autenticazione presso il Security Token Service (STS), Gatefire riceve una risposta SOAP contenente un **fault** conforme alle specifiche WS-Trust.

Di seguito un esempio di messaggio di errore tipico:

```
<soapenv:Body>
    <soapenv:Fault xmlns:axis2ns1="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-
1.0.xsd">
        <faultcode>axis2ns1:FailedAuthentication</faultcode>
        <faultstring>
            The security token could not be authenticated or authorized;
            nested exception is: 102: utente non trovato
        </faultstring>
        <detail/>
    </soapenv:Fault>
</soapenv:Body>
```

Il tag <faultcode> specifica la categoria di errore (es. FailedAuthentication, InvalidSecurityToken, InvalidRequest, ecc.), mentre <faultstring> contiene una descrizione testuale del problema.

Nel caso in cui la response STS non sia conforme alle policy WS-Security configurate nel client (ad esempio firma con algoritmo non supportato o header non validi), CXF genera una WSSecurityException.

org.apache.wss4j.common.ext.WSSecurityException:

```
An error was discovered processing the <wsse:Security> header
    at org.apache.cxf.ws.security.wss4j.WSS4JInInterceptor.handleMessage(WSS4JInInterceptor.java:...)
Caused by: org.apache.xml.security.signature.XMLSignatureException:
Invalid signature or unsupported algorithm (RSA-SHA256 not allowed with Basic256 policy)
```

Questo tipo di errore indica che il messaggio SOAP è formalmente corretto, ma non rispetta la **policy WS-Security attiva** sul client Gatefire.
In questi casi il controllo deve concentrarsi su:

- algoritmo di firma (SignatureMethod);
- tipo di chiave (KeyType);
- coerenza tra versioni di SOAP e WS-Addressing.

3.11 Censimento nuovo Repository

Per l'integrazione con un nuovo repository, il sistema Gatefire ha bisogno di conoscere e configurare al suo interno alcune informazioni.

Le principali informazioni richieste sono:

- Authentication_required→ indica se il repository necessita di autenticazione preventiva con Security Token Se SI il fornitore dovrà fornire a Gatefire le credenziali di autenticazione

- Endpoint servizio STS (se il repository necessita di autenticazione preventiva con Security Token)
- Endpoint delle varie transazioni disponibili sul repository:
  - ITI-18 recupera metadati
  - ITI-41 conferimento documento
  - ITI-41_UNDO replace per annullare documento
  - ITI-43 recupera documento
  - ITI-57 modifica metadati

3.12 Appendice A – Esempio di richiesta ITI-41 (ProvideAndRegisterDocumentSet-b)

Di seguito si riporta un estratto semplificato della richiesta SOAP ITI-41 utilizzata per l'invio di un documento al repository XDS.
L'esempio mostra solo gli elementi principali per facilitare la comprensione della struttura complessiva del messaggio.

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <Action xmlns="http://www.w3.org/2005/08/addressing">
      urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b
    </Action>
    <MessageID xmlns="http://www.w3.org/2005/08/addressing">
      urn:uuid:7b56a2c1-2a86-420e-8a64-9379d733a0bd
    </MessageID>
    <wsse:Security soap:mustUnderstand="true"
      xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                       IssueInstant="2025-10-24T08:43:23.491Z"
                       Version="2.0">
        <saml2:Issuer>GATEFIRE_STS</saml2:Issuer>
        <!-- Firma SAML con algoritmo HMAC-SHA1 -->
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
          </ds:SignedInfo>
        </ds:Signature>
      </saml2:Assertion>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <xdsb:ProvideAndRegisterDocumentSetRequest xmlns:xdsb="urn:ihe:iti:xds-b:2007">
      <lcm:SubmitObjectsRequest xmlns:lcm="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0">
        <rim:RegistryObjectList xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
          <rim:ExtrinsicObject id="Document01" mimeType="application/pdf"
              objectType="urn:uuid:7edca82f-054d-47f2-a032-9b2a5b5186c1">
            <rim:Slot name="creationTime">
              <rim:ValueList>
                <rim:Value>20251023220000</rim:Value>
              </rim:ValueList>
            </rim:Slot>
            <!-- altri metadati documentali (autore, paziente, classificazioni, ecc.) -->
          </rim:ExtrinsicObject>
        </rim:RegistryObjectList>
      </lcm:SubmitObjectsRequest>

      <!-- Documento PDF codificato Base64 -->
      <xdsb:Document id="Document01">JVBERi0xLjcKJfbk/N8KMSAwIG9iago8PAovVHlwZ...</xdsb:Document>
    </xdsb:ProvideAndRegisterDocumentSetRequest>
  </soap:Body>
</soap:Envelope>
```

3.13 Appendice B – Esempio di richiesta e risposta STS (WS-Trust 1.2)

Di seguito si riporta un esempio di scambio SOAP per l'emissione di un **Security Token SAML 2.0** tramite servizio STS secondo le specifiche **OASIS WS-Trust 1.2**.
L'esempio illustra la richiesta e la relativa risposta così come gestite da Gatefire.

3.13.1 Request – Richiesta token STS

```
<soap:Envelope
    xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
    <soap:Header>
        <wsa:MessageID
            xmlns:wsa="http://www.w3.org/2005/08/addressing">urn:uuid:a8a3c117-e1a4-4945-8b56-86b22efd8b10
        </wsa:MessageID>
        <wsa:Action
            xmlns:wsa="http://www.w3.org/2005/08/addressing">http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT
        </wsa:Action>
        <wsa:To
            xmlns:wsa="http://www.w3.org/2005/08/addressing">https://xx.xx.xx.xx:xx/GetSecurityToken
        </wsa:To>
        <wsa:ReplyTo
            xmlns:wsa="http://www.w3.org/2005/08/addressing">
            <wsa:Address>http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
        </wsa:ReplyTo>
        <wsse:Security
            xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
            xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
soap:mustUnderstand="true">
            <wsu:Timestamp wsu:Id="TS-92542dae-1820-498e-b2c4-d6d4cc8d4938">
                <wsu:Created>2025-11-06T16:35:08.180Z</wsu:Created>
                <wsu:Expires>2025-11-06T16:40:08.180Z</wsu:Expires>
            </wsu:Timestamp>
            <saml2:Assertion
                xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" ID="_eb69b16e-1544-48ab-b79b-317aaa31d8b4" IssueInstant="2025-
11-06T16:35:08.181Z" Version="2.0" xsi:type="saml2:AssertionType">
                <saml2:Issuer>https://xx.xx.xx.xx:xx/GetSecurityToken</saml2:Issuer>
                <saml2:Subject>
                    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
NameQualifier="https://xx.xx.xx.xx:xx/GetSecurityToken">xxxxxx</saml2:NameID>
                    <saml2:SubjectConfirmation Method="http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey"/>
                </saml2:Subject>
                <saml2:Conditions NotBefore="2025-11-06T16:35:08.183Z" NotOnOrAfter="2025-11-06T16:40:08.183Z"/>
                <saml2:AttributeStatement>
                    <saml2:Attribute Name="SubjectApplicationId" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                        <saml2:AttributeValue
                            xmlns:xsd="http://www.w3.org/2001/XMLSchema" xsi:type="xsd:string">ESENPAT
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <saml2:Attribute Name="SubjectApplicationVendor" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                        <saml2:AttributeValue
                            xmlns:xsd="http://www.w3.org/2001/XMLSchema" xsi:type="xsd:string">CSI Piemonte
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                    <saml2:Attribute Name="SubjectApplicationVersion" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
                        <saml2:AttributeValue
                            xmlns:xsd="http://www.w3.org/2001/XMLSchema" xsi:type="xsd:string">1.0.0
                        </saml2:AttributeValue>
                    </saml2:Attribute>
                </saml2:AttributeStatement>
            </saml2:Assertion>
            <wsse:UsernameToken wsu:Id="UsernameToken-18a8eedb-11d6-4796-a22b-5ba7241a81ed">
                <wsse:Username>xxxxx</wsse:Username>
                <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-
1.0#PasswordText">xxxxxxxx</wsse:Password>
            </wsse:UsernameToken>
        </wsse:Security>
    </soap:Header>
    <soap:Body>
        <wst:RequestSecurityToken
            xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust">
            <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</wst:TokenType>
            <wst:RequestType>http://schemas.xmlsoap.org/ws/2005/02/trust/Issue</wst:RequestType>
            <wsp:AppliesTo
                xmlns:wsp="http://www.w3.org/ns/ws-policy">
                <wsa:EndpointReference
                    xmlns:wsa="http://www.w3.org/2005/08/addressing">
                    <wsa:Address>https://10.66.128.19:29090/XDS/repository/ProvideAndRegisterDocumentSet-b</wsa:Address>
                </wsa:EndpointReference>
            </wsp:AppliesTo>
            <wst:Claims Dialect="http://wso2.org/claims">
                <wsid:ClaimType
                    xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity" Optional="true"
Uri="http://wso2.org/claims/codiceFiscale"/>
                    <wsid:ClaimType
                        xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity" Optional="true"
Uri="http://wso2.org/claims/lastname"/>
                        <wsid:ClaimType
                            xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity" Optional="true"
Uri="http://wso2.org/claims/givenname"/>
                            <wsid:ClaimType
                                xmlns:wsid="http://schemas.xmlsoap.org/ws/2005/05/identity" Optional="true"
Uri="http://wso2.org/claims/role"/>
                            </wst:Claims>
                            <wst:Renewing/>
                            <wst:KeyType>http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey</wst:KeyType>
                            <wst:KeySize>256</wst:KeySize>
                            <wst:Entropy>
                                <wst:BinarySecret
Type="http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce">svQxLvQGC+Vq6JENFco1t2PK/a2msOhsBileFsa40=</wst:BinarySecret>
```

```
                        </wst:Entropy>
                        <wst:ComputedKeyAlgorithm>http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1</wst:ComputedKeyAlgorithm>
                    </wst:RequestSecurityToken>
                </soap:Body>
            </soap:Envelope>
```

3.13.2 Response – Risposta STS con SAML Assertion

```
<env:Envelope
    xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Header>
        <wsse:Security
            xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" env:mustUnderstand="true">
            <wsu:Timestamp
                xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="43ddffd3-8573-
4b2d-aa46-735b63440166">
                <wsu:Created>2025-11-06T16:35:22.110Z</wsu:Created>
                <wsu:Expires>2025-11-06T16:40:22.110Z</wsu:Expires>
            </wsu:Timestamp>
        </wsse:Security>
        <wsa:To

xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing">http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
        </wsa:To>
        <wsa:MessageID
            xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing">urn:uid:f732a46e-27b4-479d-a1ec-9058169f5cb1
        </wsa:MessageID>
        <wsa:Action
            xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing">http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue
        </wsa:Action>
        <wsa:RelatesTo
            xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing">urn:uuid:a8a3c117-e1a4-4945-8b56-86b22efd8b10
        </wsa:RelatesTo>
    </env:Header>
    <env:Body>
        <wst:RequestSecurityTokenResponse
            xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust">
            <wst:TokenType>http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</wst:TokenType>
            <wst:KeySize>256</wst:KeySize>
            <wst:RequestedAttachedReference>
                <wsse:SecurityTokenReference
                    xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
                    <wsse:Reference URI="#541da87f-0bf2-4cc0-b98b-153f5b123f3e" ValueType="http://docs.oasis-open.org/wss/oasis-wss-
saml-token-profile-1.1#SAMLV2.0"/>
                </wsse:SecurityTokenReference>
            </wst:RequestedAttachedReference>
            <wst:RequestedUnattachedReference>
                <wsse:SecurityTokenReference
                    xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
                    <wsse:Reference URI="541da87f-0bf2-4cc0-b98b-153f5b123f3e" ValueType="http://docs.oasis-open.org/wss/oasis-wss-
saml-token-profile-1.1#SAMLV2.0"/>
                </wsse:SecurityTokenReference>
            </wst:RequestedUnattachedReference>
            <wsp:AppliesTo
                xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
                <wsa:EndpointReference
                    xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"/>
                </wsp:AppliesTo>
                <wst:Lifetime>
                    <wsu:Created
                        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2025-11-
06T16:35:22.110Z
                    </wsu:Created>
                    <wsu:Expires
                        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">2025-11-
06T16:40:22.110Z
                    </wsu:Expires>
                </wst:Lifetime>
                <wst:RequestedSecurityToken>
                    <saml2:Assertion
                        xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" ID="541da87f-0bf2-4cc0-b98b-153f5b123f3e"
IssueInstant="2025-11-06T16:35:18.867Z" Version="2.0"
                        xmlns:xs="http://www.w3.org/2001/XMLSchema">
                        <saml2:Issuer>xxxxx</saml2:Issuer>
                        <ds:Signature
                            xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                            <ds:SignedInfo>
                                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
                                <ds:Reference URI="#541da87f-0bf2-4cc0-b98b-153f5b123f3e">
                                    <ds:Transforms>
                                        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                                        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                            <ec:InclusiveNamespaces
                                                xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList="xs"/>
                                            </ds:Transform>
                                        </ds:Transforms>
                                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                        <ds:DigestValue>Je4FoxHHzmlEnfd4MdfRaptJmaE=</ds:DigestValue>
```

```
                                    </ds:Reference>
                                </ds:SignedInfo>
                                <ds:SignatureValue>RnZKfY8w2zpmvR0/+hvno8kAgpg=</ds:SignatureValue>
                            </ds:Signature>
                            <saml2:Subject>
                                <saml2:NameID>xxxxx</saml2:NameID>
                                <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
                                    <saml2:SubjectConfirmationData NotBefore="2025-11-06T16:35:18.867Z" NotOnOrAfter="2025-11-
06T17:05:18.867Z"
                                        xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
                                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="saml2:KeyInfoConfirmationDataType"/>
                                    </saml2:SubjectConfirmation>
                                </saml2:Subject>
                                <saml2:Conditions NotBefore="2025-11-06T16:35:18.867Z" NotOnOrAfter="2025-11-06T17:05:18.867Z"/>
                                <saml2:AuthnStatement AuthnInstant="2025-11-06T16:35:18.867Z" SessionIndex="541da87f-0bf2-4cc0-b98b-
153f5b123f3e" SessionNotOnOrAfter="2025-11-06T17:05:18.867Z">
                                    <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</saml2:AuthnContextClassRef>
                                    </saml2:AuthnContext>
                                </saml2:AuthnStatement>
                                <saml2:AttributeStatement>
                                    <saml2:Attribute Name="http://wso2.org/claims/role" NameFormat="http://wso2.org/claims/role">
                                        <saml2:AttributeValue
                                            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"/>
                                        </saml2:Attribute>
                                        <saml2:Attribute Name="http://wso2.org/claims/lastname"
NameFormat="http://wso2.org/claims/lastname">
                                            <saml2:AttributeValue
                                                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"/>
                                            </saml2:Attribute>
                                            <saml2:Attribute Name="http://wso2.org/claims/codiceFiscale"
NameFormat="http://wso2.org/claims/codiceFiscale">
                                                <saml2:AttributeValue
                                                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"/>
                                                </saml2:Attribute>
                                                <saml2:Attribute Name="http://wso2.org/claims/givenname"
NameFormat="http://wso2.org/claims/givenname">
                                                    <saml2:AttributeValue
                                                        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string"/>
                                                    </saml2:Attribute>
                                                </saml2:AttributeStatement>
                                            </saml2:Assertion>
                                        </wst:RequestedSecurityToken>
                                        <wst:RequestedProofToken>
                                            <wst:ComputedKey>http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1</wst:ComputedKey>
                                        </wst:RequestedProofToken>
                                        <wst:Entropy>
                                            <wst:BinarySecret
Type="http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce">ODNhMDE3OTItYTUxMC00OTJmLWFlNWQtYzgzMzc1ODg4NWRi</wst:BinarySecret>
                                        </wst:Entropy>
                                    </wst:RequestSecurityTokenResponse>
                                </env:Body>
                            </env:Envelope>
```