Specifiche tecniche per l'interoperabilità tra i sistemi regionali di FSE

Versione 24 Giugno 2014

Indice

Indice delle figure

Indice delle tabelle

Obiettivi del documento

Il presente documento ha l'obiettivo di fornire le specifiche funzionali e tecniche dei servizi a supporto dell'**interoperabilità** tra i sistemi regionali di Fascicolo Sanitario Elettronico (FSE), abilitanti alla realizzazione dei processi di business sovra-regionali.

Le specifiche definite in questo documento sono conformi a quanto indicato nell'Allegato A *"Guida tecnica e modelli di riferimento"* delle *"Linee guida per la presentazione dei piani di progetto regionali per il FSE"*, predisposte dal Tavolo tecnico coordinato dall'Agenzia per l'Italia Digitale e dal Ministero della salute, con rappresentanti del Ministero dell'economia e delle finanze, delle Regioni e Province Autonome (P.A.), nonché del Consiglio Nazionale delle Ricerche e del CISIS (Centro Interregionale per i Sistemi Informatici, Geografici e Statistici).

Il documento è così articolato:

1. La sezione 1 descrive le principali **funzionalità per l'interoperabilità** , sia di base che di supporto, che devono essere offerte dai sistemi regionali di FSE, evidenziando le specifiche tecnico-funzionali da rispettare per la comunicazione con i servizi che le erogano.
2. La sezione 2 illustra i principali **requisiti di sicurezza** da rispettare, con particolare riferimento alla comunicazione interregionale e al controllo degli accessi.
3. La sezione 3 descrive alcune convenzioni esemplificative per la **configurazione su Porta di Dominio** delle operazioni che offrono le funzionalità per l'interoperabilità, da utilizzare per la cooperazione applicativa tra i domini regionali.
4. La sezione 4 descrive le principali **componenti funzionali**, che i sistemi regionali di FSE devono prevedere, propedeutiche a garantire gli aspetti a supporto dell'interoperabilità tra i sistemi regionali di FSE e i requisiti di sicurezza.
5. L'Appendice A mostra alcuni esempi in formato XML delle **asserzioni di sicurezza** da predisporre.
6. L'Appendice B sintetizza un elenco non esaustivo degli **standard tecnologici** da utilizzare per la realizzazione delle funzionalità per l'interoperabilità interregionale.

Acronimi

Di seguito si riporta l'elenco degli acronimi, con le relative estensioni, utilizzati in questo documento.

Acronimo	Estensione
AIC	**A**utorizzazione all'**I**mmissione in **C**ommercio di un farmaco
ANA	**A**nagrafe **N**azionale degli **A**ssistiti
ATC	Classificazione **A**natomica **T**erapeutica **C**himica
CISIS	**C**entro **I**nterregionale per i **S**istemi **I**nformatici, Geografici e **S**tatistici
CRUD	**C**reate, **R**ead, **U**pdate, **D**elete
DPCM	**D**ecreto del **P**residente del **C**onsiglio dei **M**inistri
FSE	**F**ascicolo **S**anitario **E**lettronico
HL7 CDA Rel. 2	**H**ealth **L**evel **7** **C**linical **D**ocument **A**rchitecture **R**elease **2**
ICD9-CM	**I**nternational **C**lassification of **D**iseases, **N**inth **R**evision, **C**linical **M**odification
IPA	**I**ndice della **P**ubblica **A**mministrazione
LOINC	**L**ogical **O**bservation **I**dentifiers **N**ames and **C**odes
MIME	**M**ultipurpose **I**nternet **M**ail **E**xtensions
P.A.	**P**rovincia **A**utonoma
PDD	**P**orta **d**i **D**ominio
PDF	**P**ortable **D**ocument **F**ormat
RCD	**R**egione **C**ontenente un **D**ocumento
RDA	**R**egione **d**i **A**ssistenza
RDE	**R**egione **d**i **E**rogazione
RPDA	**R**egione **P**recedente **d**i **A**ssistenza
SAML	**S**ecurity **A**ssertion **M**arkup **L**anguage
SPC	**S**istema **P**ubblico di **C**onnettività
TLS	**T**ransport **L**ayer **S**ecurity
TS	**T**essera **S**anitaria
XML	e**X**tensible **M**arkup **L**anguage
XSPA	**C**ross-**E**nterprise **S**ecurity and **P**rivacy **A**uthorization

Tabella 1. Elenco degli acronimi

1 Funzionalità a supporto dell'interoperabilità

Questa sezione illustra le principali funzionalità a supporto dell'interoperabilità che i domini regionali devono offrire per la realizzazione dei processi di business sovra-regionali, evidenziati nell'Allegato A delle *"Linee guida per la presentazione dei piani di progetto regionali per il FSE"* e descritti in dettaglio nel documento *"Processi di business sovra-regionali relativi ai sistemi regionali di FSE"*.

Le funzionalità sono state raggruppate in due classi:

- *funzionalità di base*: funzionalità che i servizi a supporto dell'interoperabilità devono offrire per consentire l'interscambio delle informazioni sanitarie in un contesto interregionale, conformemente a quanto indicato nel paragrafo 6.3 del disciplinare tecnico del DPCM attuativo sul FSE.
- *funzionalità di supporto*: funzionalità propedeutiche o di sostegno a quelle di base.

La comunicazione tra un sistema di FSE ed un servizio esposto da un altro dominio regionale che eroga le funzionalità descritte in precedenza deve avvenire rispettando il protocollo **SOAP v1.2**.

1.1 Funzionalità di base

Le funzionalità di base sono descritte di seguito:

- **Ricerca dei documenti del FSE:** permette alla RDE (Regione di Erogazione) che eroga una prestazione sanitaria ad un cittadino assistito da un dominio regionale differente di ottenere dalla RDA (Regione di Assistenza) dell'assistito un elenco di metadati relativi ai documenti che soddisfano i criteri di ricerca indicati e le politiche di accesso stabilite dall'assistito a cui essi fanno riferimento.
- **Recupero di un documento del FSE**: consente alla RDE di recuperare un documento presente in un dominio regionale diverso da quello di assistenza del paziente (RCD, Regione Contenente un Documento), a partire da un riferimento al documento da recuperare, ottenuto dopo aver usufruito della funzionalità di ricerca dei documenti del FSE.
- **Comunicazione dei metadati dei documenti del FSE:** permette alla RDE di trasmettere un elenco di metadati (comprensivi di informazioni su oscuramento e politiche di visibilità) relativi a un documento prodotto nel proprio dominio regionale alla RDA del paziente cui il documento si riferisce.

Di seguito si presentano le specifiche tecnico-funzionali da rispettare per la comunicazione con i servizi che erogano le funzionalità di base.

1.1.1 Ricerca dei documenti

Messaggio di richiesta

L'header del messaggio di richiesta nella transazione deve comprendere una **asserzione** in grado di attestare specifici attributi (come descritto nella sezione successiva).

Il body del messaggio di richiesta nella transazione deve contenere i **parametri di ricerca** per la query, presentati nella tabella successiva.

Nome	Descrizione
Identificativo paziente	Il parametro specifica l'identificativo del paziente (codice fiscale).
Stato documento	Il parametro indica lo stato del documento (approvato, obsoleto, ecc.).
Tipo documento	Il parametro indica il tipo di documento secondo la codifica LOINC.
Intervallo temporale di ricerca	Rappresenta i limiti inferiore e superiore della data di creazione dei documenti.

Tabella 2. Parametri di richiesta per la ricerca dei documenti

Messaggio di risposta

Il servizio che riceve il messaggio di richiesta deve verificare che l'utente che ha effettuato la richiesta possiede i diritti di accesso sulla base di diversi attributi, quali il ruolo professionale che l'utente ricopre, i consensi forniti dal paziente, l'eventuale autorizzazione puntuale fornita all'operatore. Nel caso in cui l'utente possiede i privilegi di accesso, il messaggio di risposta deve essere strutturato come descritto nello scenario A. In caso contrario, o in caso di eventuali ulteriori anomalie, il messaggio di risposta deve riportare le informazioni illustrate nello scenario B.

Scenario A: Successo

L'header del messaggio di risposta nella transazione deve contenere una **asserzione di autorizzazione** che permette l'accesso, in una successiva richiesta di recupero, ai documenti soddisfacenti i criteri indicati e le politiche di visibilità stabilite dall'assistito.

Il body del messaggio di risposta deve contenere lo stato della risposta ed una serie di **metadati** per ciascun documento soddisfacente i parametri di ricerca indicati e le politiche di visibilità stabilite dall'assistito, come indicato nella tabella successiva.

Nome	Descrizione
Stato risposta	Il parametro indica l'esito della ricerca (successo).
MIME type	Il parametro indica il MIME type (CDA, PDF).
Codice Regione / P.A.	Il parametro è utilizzato per indicare l'identificativo del dominio regionale.
Codice struttura sanitaria	Il parametro è utilizzato per indicare l'identificativo della struttura sanitaria all'interno del dominio regionale.
Identificativo documento	Il parametro indica l'identificativo utilizzato per il documento.
Tipo documento	Il parametro indica il tipo di documento, rappresentato con un codice LOINC.
Identificativo paziente	Il parametro indica l'identificativo del paziente (codice fiscale) a cui il documento fa riferimento.
Data creazione documento	Il parametro indica la data di creazione del documento.

Tabella 3. Parametri di risposta per la ricerca dei documenti in caso di successo

Scenario B: Errore

L'header del messaggio di risposta non deve comprendere asserzioni.

Il body del messaggio di risposta deve contenere lo **stato della risposta** che indica il fallimento con un codice di errore specifico.

Nome	Descrizione
Stato risposta	Il parametro indica l'esito dell'operazione (fallimento).
Codice errore	Il parametro rappresenta un codice che indica l'errore occorso.

Tabella 4. Parametri di risposta per la ricerca dei documenti in caso di errore

1.1.2 Recupero di un documento

Messaggio di richiesta

L'header del messaggio di richiesta nella transazione deve contenere l'**asserzione di autorizzazione** ricevuta a valle dalla funzionalità di ricerca dei documenti.

Il body del messaggio di richiesta della transazione deve contenere i **riferimenti del documento** da recuperare, elencati nella prossima tabella.

Nome	Descrizione
Codice Regione / P.A.	Il parametro esprime l'identificativo del dominio regionale dove è presente il documento richiesto.
Codice struttura sanitaria	Il parametro è utilizzato per indicare l'identificativo della struttura sanitaria all'interno del dominio regionale.
Identificativo documento	Il parametro indica l'identificativo utilizzato per il documento.

Tabella 5. Parametri di richiesta per il recupero di un documento

Messaggio di risposta

Il servizio che riceve il messaggio di richiesta deve verificare che l'asserzione di autorizzazione ricevuta sia valida. In caso di esito positivo, il messaggio di risposta deve essere strutturato come descritto nello scenario A. In caso contrario, o in caso di eventuali ulteriori anomalie, il messaggio di risposta deve riportare le informazioni illustrate nello scenario B.

Scenario A: Successo

L'header del messaggio di risposta della transazione non deve contenere asserzioni.

Il body del messaggio di risposta della transazione deve contenere il **documento** incapsulato in formato binario (Base64). Nella prossima tabella è riportato l'elenco delle informazioni presenti nel body del messaggio di risposta.

Nome	Descrizione
Stato risposta	Il parametro indica l'esito dell'operazione (successo).
Documento	Rappresenta il documento richiesto, in formato binario Base64.
Mime type	Il parametro indica il MIME type del documento (CDA, PDF).
Codice Regione / P.A.	Il parametro esprime l'identificativo del dominio regionale dove è presente il documento richiesto.
Codice struttura sanitaria	Il parametro è utilizzato per indicare l'identificativo della struttura sanitaria all'interno del dominio regionale.
Identificativo documento	Il parametro indica l'identificativo utilizzato per il documento.

Tabella 6. Parametri di risposta per il recupero di un documento in caso di successo

Scenario B: Errore

L'header del messaggio di risposta della transazione non deve contenere asserzioni.

Il body del messaggio di risposta deve contenere lo **stato della risposta** che indica il fallimento con un codice di errore specifico.

Nome	Descrizione
Stato risposta	Il parametro indica l'esito dell'operazione (fallimento).
Codice errore	Il parametro rappresenta un codice che indica l'errore occorso.

Tabella 7. Parametri di risposta per il recupero di un documento in caso di errore

1.1.3 Comunicazione dei metadati

Messaggio di richiesta

L'header del messaggio di richiesta nella transazione deve comprendere una **asserzione** in grado di attestare specifici attributi (come descritto nella sezione successiva).

I parametri che devono essere presenti nel body del messaggio, relativi ai **metadati** da trasmettere, sono mostrati di seguito. Si sottolinea che, nel caso in cui il documento a cui i metadati da comunicare fanno riferimento aggiorna un documento precedentemente, l'elenco dei parametri deve comprendere anche il riferimento al documento aggiornato.

Nome	Descrizione
MIME type	Il parametro indica il MIME type del documento a cui i metadati fanno riferimento (CDA, PDF).
Oscuramento	Il parametro, valorizzato secondo le indicazioni del paziente, indica se il paziente ha stabilito di oscurare il documento.
Policy di visibilità	Il parametro indica l'insieme dei ruoli che possono accedere al documento. Tale lista è specificata dal paziente.
Codice Regione / P.A.	Il parametro esprime l'identificativo del dominio regionale dove è presente il documento richiesto.
Codice struttura sanitaria	Il parametro è utilizzato per indicare l'identificativo della struttura sanitaria all'interno del dominio regionale.
Identificativo documento	Il parametro indica l'identificativo utilizzato per il documento.
Tipo documento	Il parametro indica il tipo di documento, rappresentato mediante un codice LOINC valido
Identificativo paziente	Il parametro indica l'identificativo utilizzato del paziente (codice fiscale) a cui i metadati fanno riferimento.
Riferimento documento aggiornato	Il parametro rappresenta il riferimento al documento aggiornato. Esso deve essere valorizzato unicamente in caso di aggiornamento di un documento.

Tabella 8. Parametri di richiesta per la comunicazione dei metadati

Messaggio di risposta

Il servizio che riceve il messaggio di richiesta deve verificare che l'utente che ha effettuato la richiesta possiede i diritti di accesso sulla base di diversi attributi, quali il ruolo professionale che l'utente ricopre, i consensi forniti dal paziente, l'eventuale autorizzazione puntuale fornita all'operatore. Nel caso in cui l'utente possiede i privilegi di accesso, il messaggio di risposta deve essere strutturato come descritto nello scenario A. In caso contrario, o in caso di eventuali ulteriori anomalie, il messaggio di risposta deve riportare le informazioni illustrate nello scenario B.

Scenario A: Successo

L'header del messaggio non deve contenere asserzioni.

Il body del messaggio di risposta della transazione deve contenere lo **stato della risposta**.

Nome	Descrizione
Stato risposta	Il parametro indica lo stato dell'operazione (successo).

Tabella 9. Parametri di risposta per la comunicazione dei metadati in caso di successo

Scenario A: Errore

L'header del messaggio di risposta della transazione non deve contenere asserzioni.

Il body del messaggio di risposta deve contenere lo **stato della risposta** che indica il fallimento con un codice di errore specifico.

Nome	Descrizione
Stato risposta	Il parametro indica l'esito dell'operazione (fallimento).
Codice errore	Il parametro rappresenta un codice che indica l'errore occorso.

Tabella 10. Parametri di risposta per la comunicazione dei metadati in caso di errore

1.2 Funzionalità di supporto

Le funzionalità di supporto propedeutiche o di sostegno a quelle di base sono le seguenti:

- **Identificazione di un assistito:** permette ad un dominio regionale differente da quello di assistenza di un paziente (RDE) di identificare quest'ultimo mediante l'interazione con un opportuno sistema anagrafe. L'identificazione può essere effettuata indicando alcuni parametri relativi al paziente (quali codice fiscale o un insieme di elementi quali nome, cognome e data di nascita) e ricevendo in risposta i dati anagrafici necessari alla identificazione. L'identificazione deve avvenire interagendo con l'**Anagrafe Nazionale Assistiti** (ANA). Nelle more di una eventuale indisponibilità dell'ANA, l'identificazione può essere eseguita mediante l'interazione con il **Sistema Tessera Sanitaria** (TS).
- **Trasmissione dei dati di audit**: consente alla RCD, che riceve una richiesta di recupero di un documento relativo ad un assistito di un altro dominio regionale, di trasmettere alla RDA del paziente una traccia di audit contenente informazioni relative all'accesso al documento.
- **Trasferimento del FSE**: consente alla RPDA (Regione Precedente di Assistenza) di trasferire l'intero indice del FSE di un paziente alla nuova RDA.
- **Recupero dei consensi**: consente alla nuova RDA di recuperare le informazioni relative ai consensi che un paziente ha precedentemente fornito alla RPDA.

Di seguito si presentano le specifiche tecnico-funzionali da rispettare per la comunicazione con i servizi che erogano le funzionalità di supporto.

1.2.1 Identificazione di un assistito

L'identificazione di un paziente assistito da un altro dominio regionale deve avvenire secondo le regole funzionali e tecniche dell'opportuno sistema anagrafe da contattare (ANA o Sistema TS). Pertanto, le informazioni fornite di seguito sono puramente indicative.

L'identificazione di un assistito extra-regionale dovrebbe avvenire fornendo il codice fiscale oppure un insieme di dati anagrafici (quali il nome, il cognome e la data di nascita) del paziente.

Messaggio di richiesta

L'header del messaggio di richiesta dell'operazione non dovrebbe contenere asserzioni.

Il body del messaggio di richiesta dell'operazione dovrebbe contenere uno o più **dati anagrafici** indicati nella tabella successiva.

Nome	Descrizione
Identificativo paziente	Il parametro specifica l'identificativo del paziente, ovvero il codice fiscale.
Nome paziente	Il parametro indica il nome del paziente.
Cognome paziente	Il parametro indica il cognome del paziente.
Data di nascita paziente	Il parametro specifica la data di nascita del paziente.

Tabella 11. Parametri di richiesta per l'identificazione di un assistito

Messaggio di risposta

Il servizio che riceve il messaggio di richiesta dovrebbe verificare che la propria banca dati sia in possesso delle informazioni richieste. In caso di esito positivo, il messaggio di risposta dovrebbe essere strutturato come descritto nello scenario A. In caso contrario, o in caso di eventuali ulteriori anomalie, il messaggio di risposta dovrebbe riportare le informazioni illustrate nello scenario B.

Scenario A: Successo

L'header del messaggio di risposta dell'operazione non dovrebbe contenere asserzioni.

Il body del messaggio di risposta dovrebbe contenere le **informazioni anagrafiche del paziente**, nel caso in cui quest'ultimo sia identificato, come riportato nella tabella successiva.

Nome	Descrizione
Stato risposta	Il parametro indica se il paziente è stato identificato.
Identificativo paziente	Il parametro specifica l'identificativo del paziente, ovvero il codice fiscale.
Cognome (alla nascita)	Il parametro specifica il cognome alla nascita del paziente.
Nome	Il parametro rappresenta il nome del paziente.
Sesso	Il parametro rappresenta il sesso del paziente.
Data di nascita	Il parametro indica la data di nascita del paziente.
Comune di nascita	Il parametro indica il comune di nascita del paziente.
Provincia di nascita	Il parametro indica la provincia di nascita del paziente.
Indirizzo di residenza	Il parametro indica l'indirizzo di residenza del paziente.
Azienda sanitaria di assistenza	Il parametro indica l'azienda sanitaria di assistenza del paziente.
Azienda sanitaria di residenza	Il parametro indica l'azienda sanitaria di residenza del paziente.

Tabella 12. Parametri di risposta per l'identificazione di un assistito in caso di successo

Scenario B: Errore

L'header del messaggio di risposta dell'operazione non dovrebbe contenere asserzioni.

Il body del messaggio di risposta dovrebbe contenere lo **stato della risposta** che indica il fallimento con un codice di errore specifico.

Nome	Descrizione
Stato risposta	Il parametro indica l'esito dell'operazione (fallimento).
Codice errore	Il parametro rappresenta un codice che indica l'errore occorso.

Tabella 13. Parametri di risposta per l'identificazione di un assistito in caso di errore

1.2.2 Trasmissione dei dati di audit

Messaggio di richiesta

L'header del messaggio di risposta della transazione non deve contenere asserzioni.

I parametri che devono essere presenti nel body del messaggio, relativi alla **traccia di audit** da trasmettere, sono mostrati di seguito.

Nome	Descrizione
Identificativo paziente	Il parametro rappresenta l'identificativo del paziente, ovvero il codice fiscale
Ruolo utente	Il parametro indica il ruolo assunto dall'utente che ha richiesto l'accesso al documento.

Contesto operativo	Il parametro indica il contesto operativo all'atto della richiesta di accesso al documento.
Codice Regione / P.A.	Il parametro esprime l'identificativo del dominio regionale dove è presente il documento richiesto.
Codice struttura sanitaria	Il parametro è utilizzato per indicare l'identificativo della struttura sanitaria all'interno del dominio regionale.
Identificativo documento	Il parametro indica l'identificativo utilizzato per il documento.
Tipo documento	Il parametro indica il tipo di documento, rappresentato attraverso un codice LOINC.
Data e ora accesso	Il parametro indica la l'istante di tempo in cui è stato richiesto l'accesso al documento.
Identificativo operatore	Il parametro rappresenta l'identificativo dell'operatore (codice fiscale).

Tabella 14. Parametri di richiesta per la trasmissione dei dati di audit

Messaggio di risposta

Il servizio che riceve il messaggio di richiesta deve verificare che quest'ultimo contiene informazioni relative all'accesso ad un documento di un proprio assistito. In caso di esito positivo, il messaggio di risposta deve essere strutturato come descritto nello scenario A. In caso contrario, o in caso di eventuali ulteriori anomalie, il messaggio di risposta deve riportare le informazioni illustrate nello scenario B.

Scenario A: Successo

L'header del messaggio non deve contenere asserzioni.

Il body del messaggio di risposta della transazione deve contenere lo **stato della risposta**.

Nome	Descrizione
Stato risposta	Il parametro indica lo stato dell'operazione (successo).

Tabella 15. Parametri di risposta per la trasmissione dei dati di audit in caso di successo

Scenario A: Errore

L'header del messaggio di risposta della transazione non deve contenere asserzioni.

Il body del messaggio di risposta deve contenere lo **stato della risposta** che indica il fallimento con un codice di errore specifico.

Nome	Descrizione
Stato risposta	Il parametro indica l'esito dell'operazione (fallimento).
Codice errore	Il parametro rappresenta un codice che indica l'errore occorso.

Tabella 16. Parametri di risposta per la trasmissione dei dati di audit in caso di errore

1.2.3 Trasferimento del FSE

Messaggio di richiesta

L'header del messaggio di richiesta nella transazione deve comprendere una **asserzione** in grado di attestare specifici attributi (come descritto nella sezione successiva).

Il body del messaggio di richiesta nella transazione deve contenere l'**identificativo del paziente** che ha richiesto il trasferimento del proprio FSE.

Nome	Descrizione
Identificativo paziente	Il parametro rappresenta l'identificativo del paziente (codice fiscale) che ha richiesto il trasferimento del proprio FSE.

Tabella 17. Parametri di richiesta per il trasferimento del FSE

Messaggio di risposta

Il servizio che riceve il messaggio di richiesta deve verificare che quest'ultimo contiene informazioni relative ad un proprio assistito. In caso di esito positivo, il messaggio di risposta deve essere strutturato come descritto nello scenario A. In caso contrario, o in caso di eventuali ulteriori anomalie, il messaggio di risposta deve riportare le informazioni illustrate nello scenario B.

Scenario A: Successo

L'header del messaggio di risposta nella transazione non deve contenere asserzioni.

Il body del messaggio di risposta deve contenere l'intero **indice del FSE di un paziente**, che comprende, per ogni singolo documento, l'insieme dei metadati di indicizzazione, delle informazioni di oscuramento e delle politiche di visibilità (elenco dei ruoli professionali abilitati).

Nome	Descrizione
Stato risposta	Il parametro specifica se il paziente è stato identificato o meno.
Elenco metadati di indicizzazione	Rappresenta l'insieme dei metadati di indicizzazione dei documenti del FSE di un dato paziente.
Elenco riferimenti ai documenti oscurati	Indica l'elenco di tutti i documenti oscurati.
Elenco policy di visibilità	Rappresenta l'insieme dei ruoli abilitati all'accesso di ogni documento da parte dell'assistito.
Elenco accessi al FSE	Il parametro rappresenta l'elenco degli accessi che sono stati effettuati al FSE di un dato paziente (insieme dei dati di audit log).

Tabella 18. Parametri di risposta per il trasferimento del FSE in caso di successo

Scenario B: Errore

L'header del messaggio di risposta nella transazione non deve contenere asserzioni.

Il body del messaggio di risposta deve contenere lo **stato della risposta** che indica il fallimento con un codice di errore specifico.

Nome	Descrizione
Stato risposta	Il parametro indica l'esito dell'operazione (fallimento).
Codice errore	Il parametro rappresenta un codice che indica l'errore occorso.

Tabella 19. Parametri di risposta per il trasferimento del FSE in caso di errore

1.2.4 Recupero dei consensi

Messaggio di richiesta

L'header del messaggio di richiesta nella transazione deve comprendere una **asserzione** in grado di attestare specifici attributi (come descritto nella sezione successiva).

Il body del messaggio di richiesta nella transazione deve contenere l'**identificativo del paziente** i cui consensi si intendono recuperare.

Nome	Descrizione
Identificativo paziente	Il parametro rappresenta l'identificativo del paziente (codice fiscale) a cui si riferiscono i consensi da recuperare.

Tabella 20. Parametri di richiesta per il recupero dei consensi

Messaggio di risposta

Il servizio che riceve il messaggio di richiesta deve verificare che quest'ultimo contiene informazioni relative ad un assistito che ha usufruito del FSE nel proprio dominio regionale. In caso di esito positivo, il messaggio di risposta deve essere strutturato come descritto nello scenario A. In caso contrario, o in caso di eventuali ulteriori anomalie, il messaggio di risposta deve riportare le informazioni illustrate nello scenario B.

Scenario A: Successo

L'header del messaggio di risposta nella transazione non deve contenere asserzioni.

Il body del messaggio di risposta deve contenere le informazioni relative allo stato dei **consensi** forniti dal paziente.

Nome	Descrizione
Stato risposta	Il parametro specifica se il paziente è stato identificato o meno.
Consenso all'alimentazione	Il parametro rappresenta l'insieme delle informazioni che il paziente ha fornito inerenti al consenso all'alimentazione del FSE (quali lo stato del consenso e le eventuali restrizioni generali sull'alimentazione del FSE).
Consenso alla consultazione	Il parametro rappresenta l'insieme delle informazioni che il paziente ha fornito inerenti al consenso alla consultazione del FSE (quali lo stato del consenso e le eventuali restrizioni generali sulla consultazione del FSE).

Tabella 21. Parametri di risposta per il recupero dei consensi in caso di successo

Scenario B: Errore

L'header del messaggio di risposta nella transazione non deve contenere asserzioni.

Il body del messaggio di risposta deve contenere lo **stato della risposta** che indica il fallimento con un codice di errore specifico.

Nome	Descrizione
Stato risposta	Il parametro indica l'esito dell'operazione (fallimento).
Codice errore	Il parametro rappresenta un codice che indica l'errore occorso.

Tabella 22. Parametri di risposta per il recupero dei consensi in caso di errore

2 Aspetti di sicurezza

Questa sezione presenta i principali requisiti di sicurezza da rispettare, con particolare riferimento alla comunicazione interregionale e al controllo degli accessi.

2.1 Comunicazione sicura

I principali requisiti da rispettare nella comunicazione interregionale tra i sistemi regionali di FSE sono sintetizzati di seguito:

- *Integrità dei messaggi*: garantisce che i messaggi scambiati non siano alterati nella trasmissione o che vi sia evidenza di una eventuale modifica dei messaggi scambiati.
- *Confidenzialità dei messaggi*: assicura che solo il destinatario dei messaggi sia in grado di interpretarne il contenuto.
- *Non ripudio dei messaggi*: garantisce che il mittente ed il destinatario dei messaggi non possano negare, rispettivamente, di aver trasmesso e ricevuto i messaggi.
- *Autenticità degli attori*: assicura l'identità degli attori coinvolti nella comunicazione dei messaggi.

Il rispetto dei requisiti di sicurezza è garantito da una parte dall'utilizzo delle infrastrutture tecnologiche del **Sistema Pubblico di Connettività** per la cooperazione applicativa tra i sistemi regionali di FSE, in grado di assicurare una comunicazione sicura tra le Porte di Dominio (PDD), dall'altra dal ricorso a specifiche **asserzioni di sicurezza** contenute nei messaggi scambiati.

I requisiti di **autenticità** dei nodi regionali, di **integrità** e di **non ripudio** dei messaggi sono assicurati dalla firma digitale dei messaggi scambiati tra i domini regionale di FSE a livello di Porta di Dominio, prevista dalle infrastrutture del Sistema Pubblico di Connettività (SPC) mediante l'adozione dello standard **Transport Layer Security** (TLS) con modalità di mutua autenticazione. Allo stesso modo, il protocollo TLS è utilizzato per garantire anche il requisito di *confidenzialità* dei messaggi scambiati.

La verifica delle identità degli attori coinvolti nelle transazioni interregionali (*autenticità*) può essere effettuata dalla preesistenza di relazioni di trust mutue tra i domini attraverso un **Circle of Trust** gestito da una autorità centrale fidata, avente il compito di rilasciare i certificati digitali alle Regioni / P.A. e di provvedere alla loro manutenzione.

L'**autorizzazione** all'accesso alle funzionalità offerte dai sistemi regionali di FSE deve essere svolta analizzando le asserzioni di sicurezza contenute nei messaggi scambiati, di cui le Regioni/P.A. richiedenti garantiscono l'autenticità.

2.2 Controllo degli accessi

Il controllo degli accessi ai servizi offerti dai sistemi regionali deve essere effettuato dai sistemi di queste ultime attraverso la verifica di opportune attestazioni in forma di asserzioni di sicurezza che devono essere contenute nei messaggi trasmessi.

Nello specifico, ad ogni richiesta interregionale devono essere predisposte opportune asserzioni, a seconda dello specifico processo sovra-regionale. Le possibili tipologie di asserzioni da predisporre sono le seguenti:

- *Asserzione di attributo*: provvede a garantire il ruolo dell'utente ed ulteriori attributi.
- *Asserzione di autorizzazione*: contiene l'autorizzazione ad accedere ai documenti identificati a valle di una ricerca.

Il formato delle asserzioni di sicurezza contenute nei messaggi SOAP scambiati tra i servizi interregionali deve essere conforme allo standard OASIS **Security Assertion Markup Language** (SAML) v2.0, con particolare riferimento al profilo **Cross-Enterprise Security and Privacy Authorization** (XSPA) per il settore sanitario.

Una trattazione più dettagliata di tali tipologie di asserzioni è fornita nei sottoparagrafi seguenti.

2.2.1 Asserzione di attributo

L'asserzione di attributo consente al dominio regionale di asserire specifici **attributi** (tra cui il ruolo professionale) associati ad un proprio utente e dipendenti dal contesto relativo alla richiesta. A valle dell'identificazione e dell'autenticazione dell'utente, il sistema regionale di FSE deve attestare che esso ricopre effettivamente un determinato ruolo e possiede specifici attributi. L'asserzione di attributo è emessa dal nodo del dominio regionale, in grado di certificare tale informazione per l'utente registrato. L'asserzione di attributo attesta gli attributi riportati nella tabella successiva.

Attribute ID	URN	Descrizione
SubjectId	*urn:oasis:names:tc:xacml:1.0:subject: subject-id*	Identificativo dell'utente (codice fiscale).
OrganizationId	*urn:oasis:names:tc:xspa:1.0:subject: organization-id*	Identificativo del dominio regionale presso cui l'utente è in carico.
Organization	*urn:oasis:names:tc:xspa:1.0:subject: organization*	Descrizione del dominio regionale presso cui l'utente è in carico.
EnvironmentLocality	*urn:oasis:names:tc:xspa:1.0: environment:locality*	Eventuale posizione dalla quale l'utente opera (ospedale, studio medico, casa del paziente).
SubjectRole	*urn:oasis:names:tc:xacml:2.0:subject: role*	Ruolo dell'utente.
SubjectPurposeOfUse	*urn:oasis:names:tc:xspa:1.0:subject: purposeofuse*	Contesto operativo della richiesta: trattamento di cura ordinario; trattamento in emergenza.
ResourceType	*urn:oasis:names:tc:xspa:1.0:resource: hl7:type*	Eventuale tipo di documento a cui si intende accedere (es. codice LOINC Patient Summary).
ResourceId	*urn:oasis:names:tc:xacml:1.0: resource:resource-id*	Identificativo univoco dell'assistito (codice fiscale) il cui documento si intende accedere.
PatientConsent	*urn:oasis:names:tc:xspa:1.0:resource: patient:consent*	Manifestazione del consenso puntuale ricevuto dal paziente: consenso fornito (ad es. per il trattamento di cura ordinario); consenso non fornito (ad es. in caso di trattamento in emergenza).
ResourceAction	*urn:oasis:names:tc:xacml:1.0:action: action-id*	Azione CRUD (Create, Read, Update, Delete) che l'utente intende effettuare nell'ambito dell'interazione con il FSE.

Tabella 23. Formato dell'asserzione di attributo

L'intera asserzione è firmata dal nodo regionale che in questo modo si assume la responsabilità di quanto asserito. L'asserzione di attributo deve essere firmata utilizzando il certificato digitale che fa riferimento al Circle of Trust.

2.2.2 Asserzione di autorizzazione

L'asserzione di autorizzazione è generata dal sistema di FSE della Regione di Assistenza di un paziente che, dopo aver ricevuto una richiesta inerente alla ricerca di documenti relativi a quest'ultimo, fornisce o meno l'asserzione per l'**autorizzazione** al successivo recupero dei documenti, in base alle politiche di visibilità e di oscuramento espresse dal paziente. Essa è emessa dall'amministrazione erogante sulla base di politiche prestabilite. Un'asserzione di autorizzazione attesta gli attributi riportati nella tabella successiva.

Attribute ID	URN	Descrizione
SubjectId	*urn:oasis:names:tc:xacml:1.0:subject: subject-id*	Identificativo dell'utente (codice fiscale) a cui viene fornita l'autorizzazione.
Role	*urn:oasis:names:tc:xacml:2.0:subject: role*	Ruolo dell'utente a cui viene fornita l'autorizzazione.

Tabella 24. Formato dell'asserzione di autorizzazione

L'intera asserzione è firmata dal nodo regionale che in questo modo si assume la responsabilità di quanto autorizzato. L'asserzione di autorizzazione deve essere firmata utilizzando il certificato digitale che fa riferimento al Circle of Trust.

2.2.3 Errori relativi alla verifica delle asserzioni

Ogni richiesta di interazione con un servizio per l'interoperabilità da parte di un dominio regionale deve essere preliminarmente analizzata dal sistema regionale che offre il servizio al fine di effettuare il controllo degli accessi. Le principali verifiche da eseguire riguardano:

- la correttezza del formato di ogni asserzione;
- la verifica della firma digitale di ogni asserzione;
- la verifica della coerenza dell'asserzione di attributo con il messaggio applicativo;
- la verifica del ruolo dell'utente e del *purpose of use* (contesto operativo);
- la verifica dell'esistenza dell'autorizzazione concessa dal paziente ad un operatore extra-regionale;

Ulteriori verifiche da effettuare prima di concedere l'accesso al servizio richiesto riguardano la manifestazione dei consensi da parte del cittadino, mediante l'interazione con il sistema di gestione del consenso del proprio dominio regionale.

Eventuali errori inerenti alla verifica delle asserzioni di sicurezza devono essere opportunamente segnalati, come mostrato in maniera esemplificativa in Tabella 25.

Messaggio di errore	Descrizione
Permesso negato	Le politiche di accesso non consentono l'accesso al servizio richiesto da parte del soggetto richiedente.
Asserzioni assenti o non valide	Nel messaggio non vengono individuate le asserzioni.
Formato dell'asserzione di attributo non valido	La struttura dell'asserzione di attributo non è corretta (ad es. attributi assenti).
Formato dell'asserzione di autorizzazione non valido	La struttura dell'asserzione di autorizzazione non è corretta (ad es. attributi assenti).
Firma dell'asserzione di attributo non valida	La verifica della firma dell'asserzione di attributo non è andata a buon fine.
Firma dell'asserzione di autorizzazione non valida	La verifica della firma dell'asserzione di autorizzazione non è andata a buon fine.
Costruzione dell'asserzione di autorizzazione errata	Non è stato possibile costruire l'asserzione di autorizzazione.
Ruolo non valido	Il ruolo dell'utente non è presente tra quelli previsti.
Contesto operative non valido	Il valore del *purpose of use* non è presente tra quelli previsti.
Consenso all'alimentazione assente	Il paziente non ha fornito il consenso all'alimentazione del FSE con riferimento al ruolo.
Consenso alla consultazione assente	Il paziente non ha fornito il consenso alla consultazione del FSE con riferimento al ruolo.
Identificativo paziente non valido	L'identificativo del paziente indicato nell'header non coincide con quello indicato nel body.
Identificativo documento non valido	L'identificativo del documento indicato nell'header non coincide con quello indicato nel body.
Asserzione scaduta	Periodo di validità dell'asserzione scaduta.
Destinatario errato	Il messaggio è stato inviato ad un dominio regionale errato.

Tabella 25. Messaggi di errore inerenti alla verifica delle richieste di accesso

3 Configurazione delle operazioni su Porta di Dominio

Questa sezione descrive alcune **convenzioni esemplificative** per la configurazione su Porta di Dominio delle operazioni che offrono le funzionalità descritte, da utilizzare per la cooperazione applicativa tra i domini regionali. In particolare, ogni funzionalità per l'interoperabilità viene esposta adottando la modalità **transparent proxy**. Si noti che l'elemento <*codice regione*> deve essere codificato come indicato al paragrafo 6.2 del disciplinare tecnico del DPCM attuativo sul FSE.

- **Soggetto SPC**
  - *Nome*: FSE<codice regione>
  - *Codice IPA*: c=it, o=fse_<codice regione>
  - *Connettore*: URL specifico della PDD erogatore

- **Ricerca dei documenti**
  - *Accordo di servizio parte comune*
    - Nome Accordo AS: AS_RicercaDocumenti_<codice regione>
  - *Info servizio*
    - Nome servizio: RicercaDocumenti
    - Profilo: sincrono
  - *Info azione*
    - Nome: ricercaDocumenti
  - *Accordo di servizio parte specifica*
    - *Accordo:* AS_RicercaDocumenti_<codice regione>
    - *Servizio:* RicercaDocumenti
    - *Nome:* RicercaDocumenti
  - *Servizio applicativo*
    - *Nome:* SA_RicercaDocumenti_<codice regione>
    - *Modalità di autenticazione:* basic
    - *Username:* fse_<codice regione>
    - *Password:* *****

- **Recupero di un documento**
  - *Accordo di servizio parte comune*
    - *Nome Accordo AS:* AS_RecuperoDocumento_<codice regione>
  - *Info servizio*
    - *Nome servizio:* RecuperoDocumento
    - *Profilo:* sincrono
  - *Info azione*
    - *Nome:* recuperoDocumento
  - *Accordo di servizio parte specifica*
    - *Accordo:* AS_RecuperoDocumento_<codice regione>
    - *Servizio:* RecuperoDocumento
    - *Nome:* RecuperoDocumento
  - *Servizio applicativo*
    - *Nome:* SA_RecuperoDocumento_<codice regione>
    - *Modalità di autenticazione:* basic
    - *Username:* fse_<codice regione>
    - *Password:* *****

- **Comunicazione dei metadati**
  - *Accordo di servizio parte comune*
    - *Nome Accordo AS:* AS_ComunicazioneMetadati_<codice regione>
  - *Info servizio*
    - *Nome servizio:* ComunicazioneMetadati
    - *Profilo:* sincrono
  - *Info azione*
    - *Nome:* comunicazioneMetadati

- *Accordo di servizio parte specifica*
  - *Accordo:* AS_ComunicazioneMetadati_<codice regione>
  - *Servizio:* ComunicazioneMetadati
  - *Nome:* ComunicazioneMetadati
- *Servizio applicativo*
  - *Nome:* SA_ComunicazioneMetadati_<codice regione>
  - *Modalità di autenticazione:* basic
  - *Username:* fse_<codice regione>
  - *Password:* *****

- **Identificazione di un assistito**
  - *Accordo di servizio parte comune*
    - *Nome Accordo AS:* AS_IdentificazioneAssistito_<codice regione>
  - *Info servizio*
    - *Nome servizio:* IdentificazioneAssistito
    - *Profilo:* sincrono
  - *Info azione*
    - *Nome:* identificazioneAssistito
  - *Accordo di servizio parte specifica*
    - *Accordo:* AS_IdentificazioneAssistito_<codice regione>
    - *Servizio:* IdentificazioneAssistito
    - *Nome:* IdentificazioneAssistito
  - *Servizio applicativo*
    - *Nome:* SA_IdentificazioneAssistito_<codice regione>
    - *Modalità di autenticazione:* basic
    - *Username:* fse_<codice regione>
    - *Password:* *****

- **Trasmissione dei dati di audit**
  - *Accordo di servizio parte comune*
    - *Nome Accordo AS:* AS_TrasmissioneDatiAudit_<codice regione>
  - *Info servizio*
    - *Nome servizio:* TrasmissioneDatiAudit
    - *Profilo:* sincrono
  - *Info azione*
    - *Nome:* trasmissioneDatiAudit
  - *Accordo di servizio parte specifica*
    - *Accordo:* AS_TrasmissioneDatiAudit_<codice regione>
    - *Servizio:* TrasmissioneDatiAudit
    - *Nome:* TrasmissioneDatiAudit
  - *Servizio applicativo*
    - *Nome:* SA_TrasmissioneDatiAudit_<codice regione>
    - *Modalità di autenticazione:* basic
    - *Username:* fse_<codice regione>
    - *Password:* *****

- **Trasferimento del FSE**
  - *Accordo di servizio parte comune*
    - *Nome Accordo AS:* AS_TrasferimentoFSE_<codice regione>
  - *Info servizio*
    - *Nome servizio:* TrasferimentoFSE
    - *Profilo:* sincrono
  - *Info azione*
    - *Nome:* trasferimentoFSE
  - *Accordo di servizio parte specifica*
    - *Accordo:* AS_TrasferimentoFSE_<codice regione>
    - *Servizio:* TrasferimentoFSE
    - *Nome:* TrasferimentoFSE

- *Servizio applicativo*
  - *Nome:* SA_ TrasferimentoFSE_<codice regione>
  - *Modalità di autenticazione:* basic
  - *Username:* fse_<codice regione>
  - *Password:* *****

- **Recupero dei consensi**
  - *Accordo di servizio parte comune*
    - *Nome Accordo AS:* AS_RecuperoConsensi_<codice regione>
  - *Info servizio*
    - *Nome servizio:* RecuperoConsensi
    - *Profilo:* sincrono
  - *Info azione*
    - *Nome:* recuperoConsensi
  - *Accordo di servizio parte specifica*
    - *Accordo:* AS_RecuperoConsensi_<codice regione>
    - *Servizio:* RecuperoConsensi
    - *Nome:* RecuperoConsensi
  - *Servizio applicativo*
    - *Nome:* SA_RecuperoConsensi_<codice regione>
    - *Modalità di autenticazione:* basic
    - *Username:* fse_<codice regione>
    - *Password:* *****

4 Componenti funzionali

Questa sezione descrive un possibile schema logico delle principali **componenti funzionali** che i sistemi regionali di FSE devono prevedere per garantire gli aspetti a supporto dell'interoperabilità tra i sistemi regionali di FSE e i requisiti di sicurezza descritti nelle sezioni precedenti. Tali componenti sono mostrate nella figura successiva.

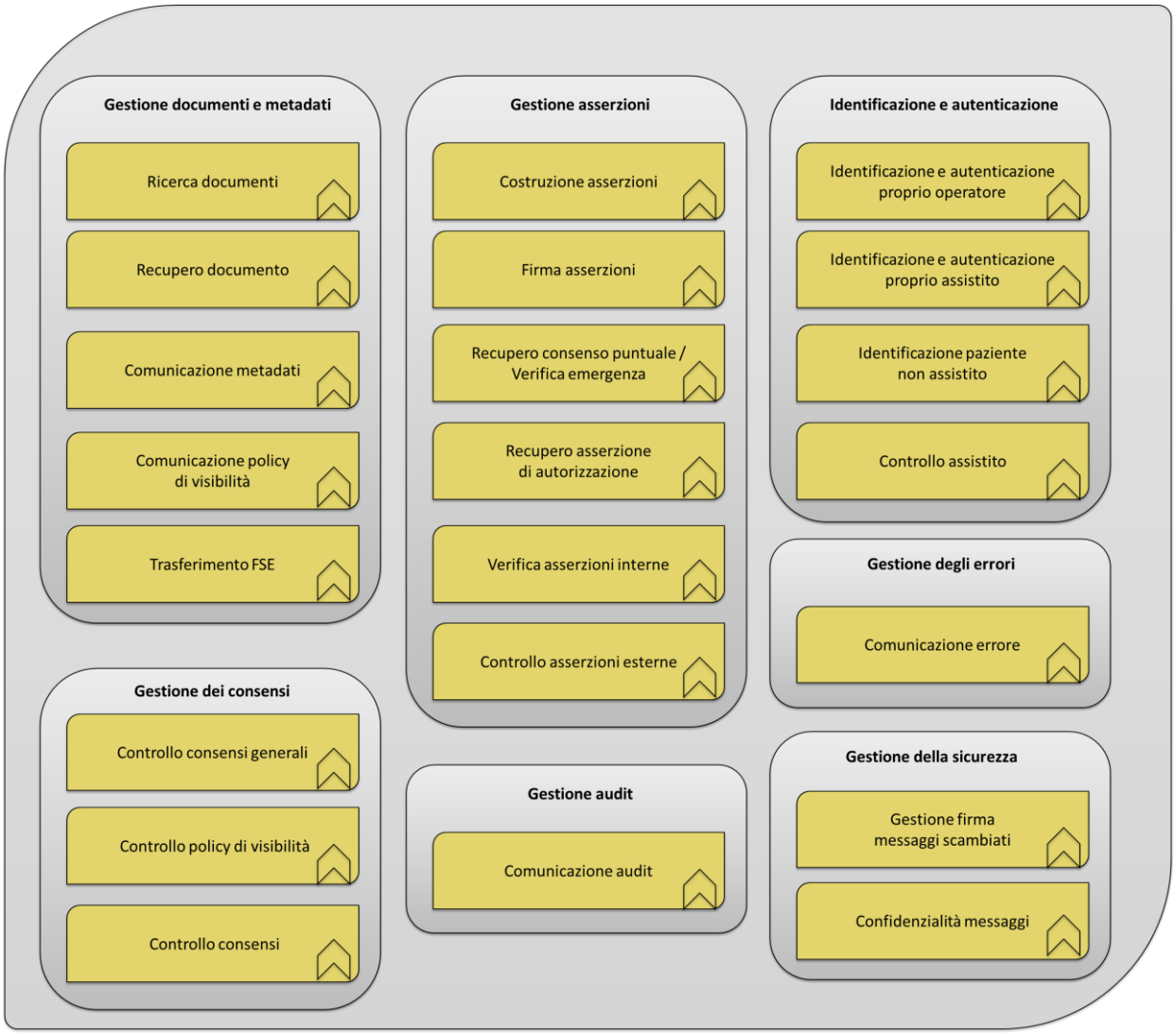

Figura 1. Componenti funzionali per l'interoperabilità tra i sistemi regionali di FSE

Le principali componenti funzionali da offrire, conformemente al modello funzionale indicato nell'Allegato A delle *"Linee guida per la presentazione dei piani di progetto regionali per il FSE"*, sono raggruppate in classi, come descritto di seguito.

- **Identificazione e autenticazione**
  - ***Identificazione e autenticazione proprio operatore***
    Questa componente funzionale permette l'identificazione e l'autenticazione di un operatore sanitario che opera all'interno del dominio regionale e che intende usufruire di un servizio offerto da un altro dominio regionale. Consente inoltre l'individuazione del ruolo attivo e di ulteriori attributi dell'operatore sanitario.
  - ***Identificazione e autenticazione proprio assistito***
    Questa componente funzionale consente l'identificazione e l'autenticazione di un paziente assistito nel proprio dominio regionale.

- ***Identificazione paziente non assistito***
  Questa componente funzionale permette di identificare un paziente non assistito nel proprio dominio regionale. La componente prevede l'inoltro di una richiesta di identificazione all'ANA o, in sua assenza, al Sistema TS.

- ***Controllo assistito***
  Questa componente funzionale permette al dominio regionale di verificare se il codice fiscale di un paziente fa riferimento ad un proprio assistito o meno.

- **Gestione asserzioni**

  - ***Costruzione asserzioni***
    Questa componente funzionale consente di costruire le asserzioni in modo opportuno in base al processo sovra-regionale.

  - ***Firma asserzioni***
    Questa componente funzionale consente al sistema regionale di firmare digitalmente le asserzioni.

  - ***Recupero consenso puntuale / Verifica emergenza***
    Questa componente funzionale permette di recuperare il consenso puntuale espresso dal paziente ad un operatore sanitario extra-regionale per l'accesso al FSE. La richiesta è trasmessa dal sistema del dominio regionale a cui l'operatore afferisce alla RDA del paziente. In caso di assenza di tale consenso, la componente consente di verificare se la richiesta è inviata in regime di emergenza.

  - ***Recupero asserzione di autorizzazione***
    Questa componente funzionale consente il recupero della asserzione di autorizzazione ricevuta in risposta alla ricerca dei documenti e di usarla per il recupero di uno specifico documento.

  - ***Verifica asserzioni interne***
    Questa componente funzionale consente di verificare le asserzioni costruite all'interno del dominio regionale prima che esse siano inoltrate ad un dominio esterno.

  - ***Controllo asserzioni esterne***
    Questa componente funzionale permette di controllare la struttura e la validità delle asserzioni trasmesse da altri domini regionali.

- **Gestione degli errori**

  - ***Comunicazione errore***
    Questa componente funzionale consente di comunicare un messaggio di errore al sistema regionale di FSE che ha richiesto di usufruire di una funzionalità offerta dal proprio sistema.

- **Gestione della sicurezza**

  - ***Gestione firma messaggi scambiati***
    Questa componente funzionale permette di firmare i messaggi in uscita e controllare le firme dei messaggi in entrata nella comunicazione con altri sistemi regionali attraverso le infrastrutture tecnologiche del Sistema Pubblico di Connettività, allo scopo di offrire caratteristiche di sicurezza.

  - ***Confidenzialità messaggi***
    Questa componente funzionale permette l'utilizzo di protocolli sicuri per la cifratura e decifratura dei messaggi scambiati attraverso le infrastrutture tecnologiche di SPC.

- **Gestione audit**
    - ***Comunicazione audit***
      Questa componente funzionale consente di inoltrare e ricevere una traccia di audit a/da un altro sistema regionale di FSE. È utilizzata in particolare nel caso di recupero di un documento presente in un dominio regionale differente da quello di assistenza del paziente a cui il documento fa riferimento. Il dominio regionale contenente il documento deve inoltrare la traccia di audit (che fornisce informazioni relative all'accesso al documento) alla RDA del paziente cui si riferisce il documento, la quale deve gestire adeguatamente le tracce ricevute (rendendo noti gli accessi al proprio assistito).
- **Gestione documenti e metadati**
    - ***Ricerca documenti***
      Questa componente funzionale consente di inviare e ricevere una richiesta di ricerca di documenti. Il messaggio di richiesta è trasmesso dalla RDE alla RDA del paziente.
    - ***Recupero documento***
      Questa componente funzionale consente di inviare e ricevere una richiesta di recupero di un documento. Il messaggio di richiesta è trasmesso dalla RDE alla RCD.
    - ***Comunicazione metadati***
      Questa componente funzionale consente di inviare e ricevere un elenco di metadati relativi ad un documento prodotto nel proprio dominio regionale. La componente, ad esempio, è utilizzata in caso di creazione di un documento sanitario in un dominio regionale diverso da quella di assistenza del paziente a cui esso fa riferimento. In questo caso, il sistema di FSE deve inoltrare i metadati relativi al documento alla RDA del paziente.
    - ***Comunicazione policy di visibilità***
      Questa componente funzionale consente di inviare e ricevere le policy di visibilità stabilite da un paziente relativamente ai propri documenti. È utilizzata, ad esempio, nel caso di creazione di un nuovo documento in un dominio regionale di FSE diverso da quello di assistenza. In questo caso, il sistema deve inoltrare le policy di visibilità indicate dal paziente al sistema di FSE della RDA di quest'ultimo.
    - ***Trasferimento FSE***
      Questa componente funzionale permette il trasferimento dell'intero indice del FSE di un paziente alla sua nuova RDA.
- **Gestione dei consensi**
    - ***Controllo consensi generali***
      Questa componente funzionale permette di verificare i consensi generali espressi dall'assistito, ovvero verificare il consenso alla alimentazione e quello alla consultazione del FSE.
    - ***Controllo policy di visibilità***
      Questa componente funzionale consente di verificare le policy di visibilità espresse dall'assistito relative ai propri documenti sanitari. La componente consente, ad esempio, di filtrare i documenti che un operatore può ricevere a valle di una ricerca di documenti.
    - ***Comunicazione consensi***
      Questa componente funzionale consente di comunicare con un altro sistema di FSE per inviare e ricevere i consensi generali (all'alimentazione e alla consultazione) espressi dal paziente. Essa è utilizzata, ad esempio, quando il paziente, cambiata la propria RDA, chiede di recuperare i consensi forniti alla RPDA prima di fornire i nuovi consensi.

Appendice A

Questa appendice mostra alcuni esempi in formato XML delle asserzioni di sicurezza.

A.1 Asserzione di attributo

Di seguito è riportato un esempio di una possibile asserzione di attributo.

```
<saml:Assertion
 xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 ID="ID_12345"
 IssueInstant="2011-11-11T09:18:01.000Z"
 Version="2.0"
 xmlns:xs="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:assertion saml-schema-assertion-
 2.0.xsd">
   <saml:Issuer>Issuer</saml:Issuer>
   <saml:Subject>
       <saml:NameID>XXXXXXXXXXXXXXXX</saml:NameID>
   </saml:Subject>
   <saml:Conditions
    NotBefore="2012-11-11T09:18:01.012Z"
    NotOnOrAfter="2012-11-11T09:48:01.017Z"/>
   <saml:AuthnStatement AuthnInstant="2011-11-11T09:18:01.000Z">
       <saml:AuthnContext>
           <saml:AuthnContextDecl>
               urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
           </saml:AuthnContextDecl>
           <saml:AuthenticatingAuthority>Issuer</saml:AuthenticatingAuthority>
       </saml:AuthnContext>
   </saml:AuthnStatement>
   <saml:AttributeStatement>
       <saml:Attribute
         Name="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
           <saml:AttributeValue xsi:type="xs:string">
                   XXXXXXXXXXXXXXXX
           </saml:AttributeValue>
       </saml:Attribute>
       <saml:Attribute
         Name="urn:oasis:names:tc:xacml:1.0:action:action-id"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
           <saml:AttributeValue xsi:type="xs:string">READ</saml:AttributeValue>
       </saml:Attribute>
       <saml:Attribute
         Name="urn:oasis:names:tc:xspa:1.0:environment:locality"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
           <saml:AttributeValue xsi:type="xs:string">H</saml:AttributeValue>
       </saml:Attribute>
       <saml:Attribute
         Name="urn:oasis:names:tc:xspa:1.0:resource:hl7:type"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
           <saml:AttributeValue xsi:type="xs:string">
                   CodiceDocumento
           </saml:AttributeValue>
       </saml:Attribute>
       <saml:Attribute
         Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse"
         NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
           <saml:AttributeValue xsi:type="xs:string">
                   HEALTHCARE TREATMENT
           </saml:AttributeValue>
       </saml:Attribute>
       <saml:Attribute
         Name="urn:oasis:names:tc:xspa:1.0:subject:organization"
```

```
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
              <saml:AttributeValue xsi:type="xs:string">
                      DescrizioneDominio
              </saml:AttributeValue>
          </saml:Attribute>
          <saml:Attribute
            Name="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
              <saml:AttributeValue xsi:type="xs:string">
                      YYYYYYYYYYYYYYY
              </saml:AttributeValue>
          </saml:Attribute>
          <saml:Attribute
            Name="urn:oasis:names:tc:xspa:1.0:resource:patient:consent"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
              <saml:AttributeValue xsi:type="xs:string">true</saml:AttributeValue>
          </saml:Attribute>
          <saml:Attribute
            Name="urn:oasis:names:tc:xacml:2.0:subject:role"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
              <saml:AttributeValue xsi:type="xs:string">MMG</saml:AttributeValue>
          </saml:Attribute>
          <saml:Attribute
            Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
              <saml:AttributeValue xsi:type="xs:string">
                      IdentificativoDominio
             </saml:AttributeValue>
          </saml:Attribute>
    </saml:AttributeStatement>
    <ds:Signature>...</ds:Signature>
</saml:Assertion>
```

A.2 Asserzione di autorizzazione

Di seguito è riportato un esempio di una possibile asserzione di autorizzazione.

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID=" ID_12345"
  IssueInstant="2010-01-18T16:16:00.499Z"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:assertion saml-schema-assertion-
  2.0.xsd">
    <saml:Issuer>Issuer</saml:Issuer>
    <saml:Subject>
        <saml:NameID>XXXXXXXXXXXXXXXX</saml:NameID>
    </saml:Subject>
    <saml:Conditions
      NotBefore="2012-11-11T09:17:00.499Z"
      NotOnOrAfter="2012-11-11T09:32:00.499Z"/>
    <saml:AuthzDecisionStatement Decision="Permit" Resource="IdentificativoRCD">
        <saml:Action Namespace="URN_Servizio_Recupero_RCD">
             IdentificativoDocumento
        </saml:Action>
    </saml:AuthzDecisionStatement>
    <saml:AttributeStatement>
        <saml:Attribute
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          Name="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
            <saml:AttributeValue xsi:type="xs:string">
                    XXXXXXXXXXXXXXXX
             </saml:AttributeValue>
        </saml:Attribute>
        <saml:Attribute
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          Name="urn:oasis:names:tc:xacml:2.0:subject:role">
```

```
            <saml:AttributeValue xsi:type="xs:string">MMG</saml:AttributeValue>
        </saml:Attribute>
    </saml:AttributeStatement>
    <ds:Signature>...</ds:Signature>
</saml:Assertion>
```

Appendice B

La tabella successiva sintetizza un elenco non esaustivo degli standard tecnologici da utilizzare per la realizzazione delle funzionalità per l'interoperabilità interregionale.

Standard tecnologici di riferimento	
Incapsulamento dei messaggi	I messaggi da scambiare con i servizi per l'interoperabilità esposti dai sistemi regionali di FSE devono essere incapsulati in una busta conforme alla specifica **SOAP versione 1.2**.
Cooperazione applicativa	Le operazioni offerte dai servizi a supporto dell'interoperabilità devono essere esposte su **Porta di Dominio** adottando la modalità **transparent proxy** e comunicare attraverso **SPC**.
Comunicazione sicura	La comunicazione tra i servizi mediante PDD deve avvenire mediante l'utilizzo del protocollo **TLS con mutua autenticazione**, per garantire i requisiti di autenticità del mittente e del ricevente e di integrità, non ripudio e confidenzialità dei dati scambiati.
Formato delle asserzioni	Il formato delle asserzioni di sicurezza contenute nei messaggi SOAP scambiati tra i servizi interregionali deve essere conforme al profilo standard **OASIS XSPA of SAML v2.0 for Healthcare v1.0**. Tali asserzioni devono essere contenute nella sezione header dei messaggi SOAP conformemente alle specifiche **Web Services Security**.
Circle of Trust	Le relazioni di trust tra i domini regionali vengono gestite da una **Certification Authority fidata** su base nazionale che rilascia i certificati digitali a tutte le Regioni e Province Autonome. Tali certificati possono essere utilizzati per la firma delle asserzioni da parte dei domini regionali.
Identificazione di un assistito	L'identificazione di un paziente assistito da un altro dominio regionale deve avvenire mediante l'interazione con l'**ANA** oppure, in alternativa, con il **Sistema TS**.
Protocolli di comunicazione	I protocolli di comunicazione con i servizi a supporto dell'interoperabilità tra i sistemi di FSE devono essere conformi ad adeguati standard internazionali.
Formato dei documenti scambiati	I documenti scambiati nell'ambito delle transazioni interregionali devono essere strutturati secondo lo standard **HL7 CDA Rel. 2** oppure essere in formato **PDF**.
Codifiche terminologiche	Il contenuto clinico dei documenti deve essere codificato utilizzando i sistemi di codifica **LOINC**, **ICD9-CM**, **ATC** e **AIC**.

Tabella 26. Standard tecnologici di riferimento