Sistema SIRPED
Dematerializzazione delle prescrizioni nella Regione Piemonte

Accesso ai servizi delle ricette dematerializzate mediante autenticazione forte

Specifiche tecniche

Versione 5.0

STATO DELLE VARIAZIONI

VERSIONE	DATA	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
V01	22/10/2025	Tutto il documento	Prima stesura del documento
V02	10/12/2025	4.2.1-Servizio di richiesta dell'Id-Sessione	Spostato la restituzione dei permessi dalla sezione "info" alla sezione "comunicazioni"
V03	27/01/2026	4.2.1-Servizio di richiesta dell'Id-Sessione 4.2.2-Servizio di verifica dell'Id-Sessione 4.2.3-Servizio di revoca dell'Id-Sessione	Precisazione sul pincode
V04	02/03/2026	4.2.1-Servizio di richiesta dell'Id-Sessione	Precisazione comportamento in ambiente di test
V05	10/04/2026	4.3.1-Servizio di Autorizzazione dell'Utente (Authorization Endpoint) 4.3.2-Servizio Token 4.2.1-Servizio di richiesta dell'Id-Sessione 4.2.2-Servizio di verifica dell'Id-Sessione 4.2.3-Servizio di revoca dell'Id-Sessione 4.2.5-Utilizzo dell'Id-Sessione con i servizi della ricetta dematerializzata 4.3.5 Servizio di revoca del token	Precisazione sulla valorizzazione del campo client_id Precisazione sulla valorizzazione del campo infoAggiuntive Precisazione sulla modalità di autenticazione ai servizi di gestione dell'id-Sessione con mail certificata Precisazione sulla valorizzazione del campo X-Gestionale Correzione esempio request

INDICE

1. Scopo e riferimenti del documento

1.1 Scopo del documento

Il presente documento descrive le nuove modalità di autenticazione a due o più fattori per l'accesso ai servizi regionali della ricetta dematerializzata a carico del SSN alle quali devono attenersi i gestionali che comunicano con il sistema SIRPED.

1.2 Riferimenti

[JWT-STD] JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens

https://oauth.net/2

https://datatracker.ietf.org/doc/html/rfc9068

[DEC-08-06-2023] DECRETO 8 giugno 2023 - Modifica al decreto 30 dicembre 2020, concernente l'adozione delle modalita' di accesso al Sistema TS mediante l'autenticazione a due o più fattori.

https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2023-06-15&atto.codiceRedazionale=23A03402&elenco30giorni=false

[DEC-27-02-2025] DECRETO 27 febbraio 2025 - Modifiche al decreto 2 novembre 2011 - Estensione dell'autenticazione a due o piu' fattori alle funzionalita' della ricetta dematerializzata a carico del Servizio sanitario nazionale.

https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2025-03-10&atto.codiceRedazionale=25A01494&elenco30giorni=false

[**A2F TS**] *Modalità di autenticazione a due fattori Sistema TS (aggiornato al 20/04/2025)*

Pubblicato al link https://sistemats1.sanita.finanze.it/portale/documenti-e-specifiche-tecniche6

[**A2F WS**] *Specifiche per l'autenticazione a due fattori per web services (aggiornato al 03/06/2025)*

Pubblicato al link https://sistemats1.sanita.finanze.it/portale/documenti-e-specifiche-tecniche6

[**A2F_STWS**] Web Service per la gestione dell'Id-Sessione utilizzato nell'autenticazione forte ai servizi del Sistema TS, reperibile nel kit di sviluppo

Manuale_utilizzo_WS_2Fattori.pdf, versione 1.1 del 04 giugno 2025

pubblicato al link https://sistemats1.sanita.finanze.it/portale/documenti-e-specifiche-tecniche6

1.3 Glossario

Termine	Definizione
A2F	Autenticazione a due fattori
Authorization Server	Sistema che governa autenticazione, autorizzazione e rilascio dei token di accesso.
challenge PKCE	Estensione di sicurezza del protocollo OAuth 2.0 (RFC 7636) che previene attacchi di intercettazione del codice di autorizzazione
CIL	Componente di Integrazione Locale, resa disponibile alle Aziende pubbliche, per il colloquio con il SAR
Client	Applicazione fruitrice che richiede le autorizzazioni per conto dell'utente.
Configuratore Regionale	Consente, ai Titolari al trattamento dati delle strutture sanitarie pubbliche e private, di gestire le abilitazioni degli utenti all'accesso ai servizi sanitari della Regione Piemonte.
GASP-RP	È la piattaforma regionale che mette a disposizione il sistema di autenticazione con SPID, CIE, TS-CNS e CNS. Nel documento è spesso definita anche come GASP-RP Salute; in generale, si intende l'area logica di appartenenza nella quale sussiste il Single Sign On.
Gestionale	Applicativo utilizzato dagli utenti per colloquiare con il sistema SIRPED
JWT	JSON Web Token
MMG	Medico di medicina generale
PLS	Pediatra di libera scelta
PUA	Punto Unico di Accesso degli operatori
SAC	Sistema di accoglienza centrale delle ricette dematerializzate ed elettroniche
SAR	Sistema di accoglienza regionale delle ricette dematerializzate ed elettroniche
SistemaTS	Sistema Tessera Sanitaria del Ministero dell'Economia e delle Finanze
SSN	Servizio Sanitario Nazionale
Prescrizione	Operazione di redazione delle ricette dematerializzate
Presa in carico	Operazione che permette di bloccare le ricette dematerializzate in modo esclusivo presso una regione/Azienda/struttura. Se non esplicitamente indicata, nel presente documento, si intende compresa nel termine più generico di "erogazione".
Erogazione	Operazione che permette di indicare i dati relativi a quanto effettivamente erogato al paziente a seguito di una prenotazione/accettazione di una ricetta dematerializzata.

2. Inquadramento e obiettivi del progetto

Il decreto [DEC 08GIU23] norma le modalità di accesso ai servizi esposti da SistemaTS per le ricette dematerializzate non a carico SSN mediante l'autenticazione a due o più fattori.

Il decreto [DEC 27FEB25] estende le stesse modalità anche ai servizi delle ricette dematerializzate a carico SSN.

I decreti prevedono, in sintesi:

- L'evoluzione dell'attuale modalità di autenticazione ai servizi di Sistema TS verso un'autenticazione forte.
- La garanzia da parte dei i sistemi regionali (SAR) dell'applicazione dei requisiti minimi di sicurezza adottati dal Sistema TS in termini di autenticazione forte
- La comunicazione a Sistema TS, da parte dei sistemi regionali (SAR) per ogni transazione, degli attributi qualificanti del soggetto che si è autenticato al sistema regionale
- L'adozione di un identificativo univoco di sessione (Id-Sessione), per gli utenti che, attraverso i loro gestionali, utilizzano direttamente i web service delle ricette dematerializzate esposti dal SAC, come token autorizzativo della transazione per le chiamate ai servizi interessati.

Il decreto 27 febbraio 2025 non prevede l'autenticazione a due o più fattori per i servizi delle ricette elettroniche (DPCM 26 marzo 2008).

Gli obiettivi del sistema regionale SIRPED sono:

- ottemperare a quanto richiesto dai succitati decreti introducendo l'autenticazione a due o più fattori per l'accesso ai servizi da questo esposti verso terzi,
- soddisfare la richiesta di Regione Piemonte relativa alla realizzazione, sul sistema SIRPED, di controlli di congruenza tra le abilitazioni assegnate agli utenti sul configuratore regionale, per la gestione delle ricette dematerializzate, e le operazioni (prescrizione, presa in carico ed erogazione) che questi effettuano sul sistema stesso.

2.1 Attori e sistemi coinvolti

L'adeguamento del sistema SIRPED prevede il coinvolgimento di tutti gli attori e dei sistemi che gestiscono il ciclo di vita delle ricette dematerializzate.

Gli attori coinvolti sono:

- i medici di famiglia: MMG e PLS
- i medici delle strutture pubbliche e private convenzionate o equiparate
- gli operatori amministrativi delle strutture pubbliche e private convenzionate o equiparate che gestiscono le prenotazioni
- i cittadini che utilizzano il servizio on-line del CUP Unico Regionale

I sistemi informativi coinvolti sono:

- i sistemi informativi delle Aziende Sanitarie pubbliche e private convenzionate o equiparate
- i gestionali dei medici di famiglia (MMG e PLS)
- il CUP Unico Regionale

- il sistema regionale delle ricette dematerializzare SIRPED (SAR comprensivo delle sue componenti locali CIL)
- il Sistema TS
- il configuratore regionale
- il notificatore regionale
- il Punto Unico di Accesso degli operatori regionali
- il sistema di profilazione degli operatori a supporto del configuratore regionale

3. L'autenticazione a due o più fattori nel sistema regionale piemontese

Per soddisfare quanto previsto dai decreti [DEC 08GIU23] e [DEC 27FEB25] viene introdotta la gestione dell'Id-Sessione anche nel sistema regionale SIRPED, in analogia a quanto definito da Sistema TS.

L'Id-Sessione viene assegnato univocamente dal sistema SIRPED ad ogni "utente-gestionale-azienda", che ne fa richiesta, ed ha una scadenza temporale predefinita, come previsto dai decreti.

La gestione della scadenza dell'ID-Sessione e l'eventuale richiesta di uno nuovo, quando necessario, è a carico del gestionale fruitore.

Il sistema SIRPED renderà disponibili due modalità per l'acquisizione e la gestione dell'Id-sessione:

1. Id-Sessione con mail certificata
2. Id-Sessione con protocollo OAuth2

La prima modalità prevede una gestione dell'Id-Sessione simile a quella adottata da Sistema, in particolare:

- l'utente certifica la propria mail mediante una web application (PUA) accessibile con SPID/CIE/TS-CNS/CNS di, almeno, livello 2
- il gestionale effettua una richiesta, per ricevere l'Id-Sessione, al sistema regionale SIRPED, mediante un nuovo servizio autenticato con credenziale RUPAR assegnata all'utente (basic authentication)
- il sistema SIRPED invia una mail contenente l'Id-Sessione, mediante il notificatore regionale, all'indirizzo di posta elettronica che l'utente ha certificato in precedenza sul PUA
- l'utente utilizza l'Id-Sessione ricevuto via mail come token autorizzativo della transazione per le chiamate ai servizi della ricetta dematerializzata; quindi, si autentica ai servizi con credenziali RUPAR (basic authentication + pincode), aggiungendo in più l'identificativo della transazione che è stato ottenuto tramite il secondo fattore.

Tale modalità prevede che tutti gli utenti devono disporre di:

- credenziale SPID/CIE/TS-CNS/CNS di, almeno, livello 2 per certificare la propria mail
- credenziale RUPAR nominativa per accedere ai servizi del sistema SIRPED.

La seconda modalità utilizza il protocollo di autorizzazione OAuth 2.0.

OAuth 2.0 è un protocollo standard di autorizzazione che permette a un sistema di chiedere il permesso per accedere a dati o servizi offerti da un altro sistema, in particolare:

- il gestionale, quando deve interagire con i servizi delle ricette dematerializzate, richiama una web application di autorizzazione
- la web application richiede all'utente di autenticarsi con SPID/CIE/TS-CNS/CNS di almeno livello 2, utilizzando GASP-RP-SALUTE, e di autorizzare il rilascio di un token al proprio gestionale per accedere ai servizi della ricetta dematerializzata
- se l'utente acconsente, l'applicazione richiedente ottiene un token, contenente l'Id-Sessione, che potrà usare per accedere ai servizi della ricetta dematerializzata.

Tale modalità prevede che tutti gli utenti devono disporre di credenziale SPID/CIE/TS-CNS/CNS di, almeno, livello 2

per autorizzare il rilascio del token contente l'Id-Sessione.

Per entrambe le modalità:

- è necessario che tutti gli utenti che utilizzano i servizi della ricetta dematerializzata, tranne i cittadini che utilizzano il CUP Unico Regionale, siano censiti nel configuratore regionale degli operatori con i relativi ruoli, le collocazioni ed i profili (prescrizione, presa in carico, erogazione)
- ad ogni richiesta di un nuovo Id-sessione viene inibita la validità di quello precedente, anche se non ancora scaduto
- sono previsti degli appositi servizi per verificare la validità dell'Id-Sessione o per revocarlo.

IMPORTANTE: Il CUP Unico Regionale dovrà realizzare la soluzione «Id-Sessione con protocollo OAuth2» per la prenotazione on-line da parte del cittadino, se questo rientrerà nei casi d'uso previsti dal MEF. Diversamente, dovranno essere adeguate le attuali specifiche tecniche al fine di soddisfare i requisiti che il MEF indicherà.

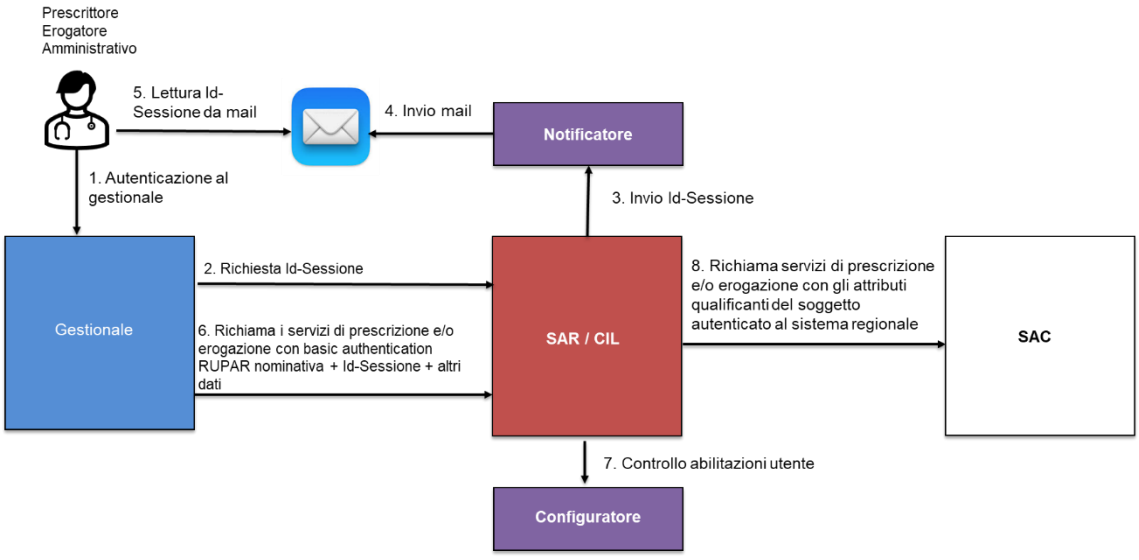
3.1 Modalità Id-Sessione con mail certificata

Questa modalità richiede l'interazione dell'utente ogni qualvolta l'Id-Sessione risulta non essere più valido: l'Id-Sessione viene ricevuto, via mail, dall'utente a seguito della richiesta effettuata dal gestionale al sistema regionale.

Per l'utilizzo di questa modalità è necessario che l'utente abbia precedentemente effettuato, sul Punto Unico di Accesso, le seguenti operazioni:

- certificazione della propria mail
- fornito il consenso alla ricezione delle notifiche da parte del sistema regionale SIRPED.

Nel seguito viene presentato uno schema di interazione tra i sistemi:



In dettaglio le interazioni tra i sistemi:

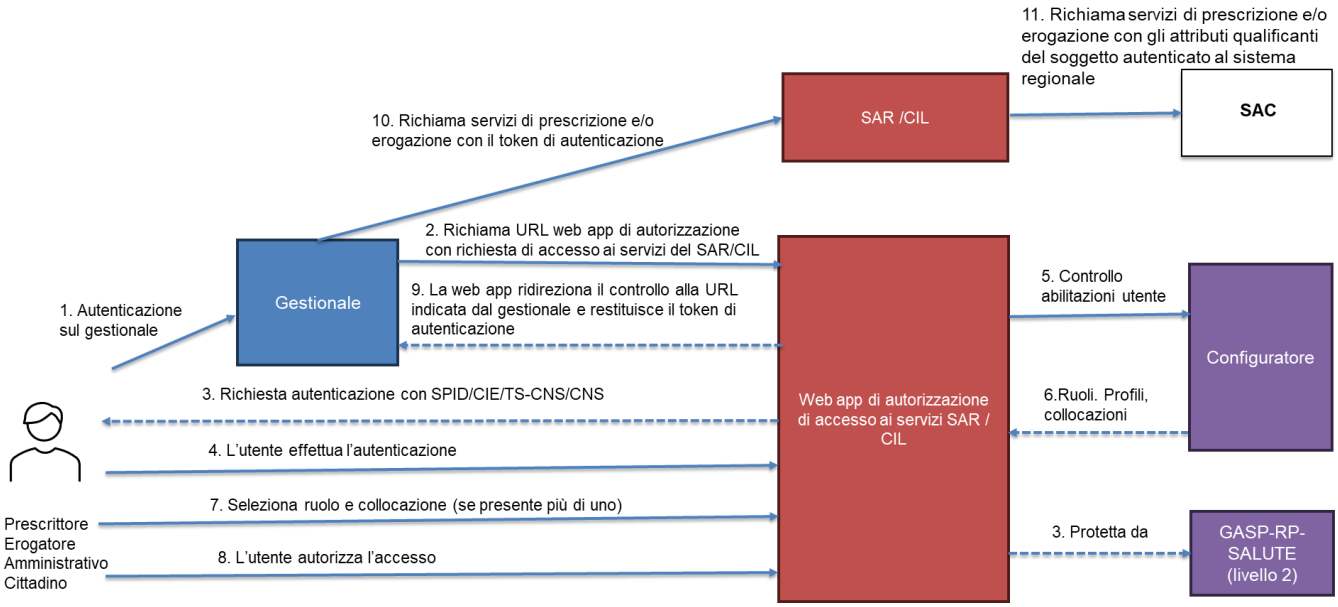
1. L'utente si autentica al proprio gestionale
2. Il gestionale richiede l'Id-Sessione tramite le credenziali RUPAR dell'utente collegato
3. Il SAR invia l'Id-Sessione al notificatore regionale
4. Il notificatore invia l'Id-Sessione alla mail certificata dall'utente sul PUA
5. L'utente recupera l'Id-Sessione dalla propria mail
6. Il gestionale richiama i servizi di prescrizione e di erogazione (presa in carico, erogato) autenticandosi con le credenziali RUPAR assegnate all'utente e comunicando anche l'Id-Sessione recuperato dalla mail, insieme ad altre informazioni
7. Il SAR/CIL verifica sul configuratore le abilitazioni dell'utente per l'accesso ai servizi della ricetta dematerializzata
8. Il SAR richiama i servizi del SAC con gli attributi qualificanti del soggetto autenticato al sistema regionale.

Qualora, il medico non ricevesse in tempo utile, per le sue attività, la mail contenente l'Id-Sessione, il gestionale dovrà rendere disponibile una modalità per richiedere l'invio di un nuovo Id-Sessione.

3.2 Modalità Id-Sessione con protocollo OAuth2

Questa modalità permette ai gestionali di gestire l'Id-Sessione in modo trasparente all'utente: a seguito dell'autorizzazione fornita dall'utente, l'Id-Sessione viene scambiato direttamente tra il sistema regionale e il gestionale richiedente.

Nel seguito viene presentato uno schema di interazione tra i sistemi:



In dettaglio, le interazioni tra i sistemi:

1. L'utente si autentica al proprio gestionale
2. Il gestionale, quando deve interagire con il sistema regionale SIRPED, richiama una web application di autorizzazione richiedendo l'accesso ai servizi della ricetta dematerializzata
3. La web application di autorizzazione richiede all'utente di autenticarsi con SPID/CIE/TS-CNS/CNS di, almeno, livello 2
4. L'utente si autentica
5. La web application di autorizzazione verifica sul configuratore che l'utente possa accedere al sistema regionale SIRPED.
6. La web application visualizza il ruolo, le collocazioni e i relativi profili (ad esempio: prescrittore, erogatore, presa in carico) dell'utente per il sistema regionale SIRPED
7. Se sono presenti più ruoli o collocazioni o profili, l'utente seleziona per quale, tra quelli presentati, vuole operare
8. L'utente dà l'autorizzazione a procedere per l'attività richiesta
9. La web application di autorizzazione restituisce il controllo alla url di ritorno indicata dal gestionale contestualmente al token di autenticazione contenente l'Id-Sessione, i dati dell'utente e i profili concessi
10. Il gestionale richiama i servizi di prescrizione e/o erogazione sul SAR/CIL utilizzando solo il token di autenticazione
11. Il SAR richiama i servizi del SAC con gli attributi qualificanti del soggetto autenticato al sistema regionale.

Le operazioni da 4 a 7 non sono effettuate se il richiedente è un cittadino che vuole effettuare la prenotazione di una ricetta mediante il CUP Unico Regionale.
Le operazioni da 2 a 9 devono essere effettuate dal gestionale ogni qual volta scade il token.

Qualora il gestionale sia federato con GASP-RP-Salute, garantendo il single sign on, al momento del richiamo della web application di autorizzazione, non saranno più richieste le credenziali SPID/CIE/TS-CNS/CNS in quanto l'utente risulterà già autenticato.

In questo caso, all'utente verrà richiesta comunque l'autorizzazione del rilascio del token di autenticazione al proprio gestionale, per accedere ai servizi regionali della ricetta dematerializzata.

4. Implementazione dell'autenticazione a due o più fattori nel sistema regionale piemontese

Di seguito vengono presentate le specifiche di dettaglio per l'implementazione dell'autenticazione a due o più fattori, per l'acceso ai servizi della ricetta dematerializzata, nelle due modalità rese disponibili dal sistema regionale.

Id-Sessione con mail certificata

Tale modalità prevede:

- Richiesta dell'ID sessione: il gestionale invia una richiesta a un apposito servizio SOAP (CreatAuth) per ottenere un identificativo di sessione (Id-Sessione)
- Notifica all'utente via e-mail certificata: il sistema SIRPED, mediante il notificatore regionale, invia l'Id-Sessione alla mail certificata dell'utente
- Utilizzo dell'ID sessione: l'utente, recuperato l'Id-Sessione dalla mail, lo comunica al proprio gestionale che lo utilizza insieme alle proprie credenziali RUPAR, per l'accesso ai servizi della ricetta dematerializzata.

Id-Sessione con protocollo OAuth2

Tale modalità prevede:

- Login dell'utente alla web application di autorizzazione: l'autenticazione viene effettuata tramite provider federati (GASP-RP Salute) utilizzando SPID o CIE o TS-CNS o CNS di, almeno, livello 2.
- Delegazione della sicurezza: il riconoscimento a due o più fattori è delegato al servizio di login federato; la piattaforma OAuth2 si limita a veicolare il token JWT emesso a valle di una sessione autenticata in modo forte.
- Sostituzione della Basic Authentication: tutte le chiamate ai servizi SOAP dovranno passare un Bearer Token nell'header HTTP, eliminando la basic authentication (user, password e PIN).

4.1 Sicurezza del sistema e protocollo di comunicazione

4.1.1 Sicurezza con la modalità "Id-Sessione con mail certificata"

Il sistema SIRPED implementa un meccanismo di sicurezza basato su HTTP Basic Authentication, utilizzando come credenziali di accesso quelle degli operatori RUPAR (username e password) assegnate a ciascun utente, alle quali si affianca l'indicazione del PIN inserito all'interno della request SOAP.

A ulteriore rafforzamento della sicurezza, viene richiesto l'inserimento nell'intestazione HTTP del dato aggiuntivo relativo all'Id-Sessione.

Tale Id-Sessione viene generato e inviato all'operatore secondo la procedura descritta in precedenza.

Inoltre, l'integrazione con la piattaforma del Configuratore Regionale consente una profilazione centralizzata per gli operatori, contribuendo a una sicurezza ulteriormente rafforzata nella gestione degli accessi e delle abilitazioni.

4.1.2 Sicurezza con la modalità "Id-Sessione con protocollo OAuth2"

Il sistema regionale SIRPED implementa il sistema di sicurezza basata su OAuth 2.0, in particolare adottando lo standard Authorization Code Grant con PKCE (Proof Key for Code Exchange).

Questa modalità prevede un processo di autorizzazione alle risorse (webservice e applicazioni) garantendo la corretta gestione dei permessi e la tutela dei dati durante la comunicazione tra i diversi soggetti coinvolti.

Inoltre, l'autorizzazione all'accesso alle risorse da parte dell'utente avviene esclusivamente previa autenticazione tramite l'infrastruttura regionale GASP-RP Salute (che si integra con gli Identity Provider di SPID e CIE oltre che con TS-CNS e CNS) con livello di autenticazione a due o più fattori.

Inoltre, l'integrazione con la piattaforma del Configuratore Regionale consente una profilazione centralizzata per gli operatori, contribuendo a una sicurezza ulteriormente rafforzata nella gestione degli accessi e delle abilitazioni.

4.1.3 Protocollo di comunicazione

In entrambe le modalità, tutti i servizi sono esposti tramite protocollo HTTPS, garantendo così la cifratura dei dati scambiati e la protezione delle informazioni trasmesse tra client e server da possibili intercettazioni o manomissioni.

Per assicurare gli standard di sicurezza:

- È utilizzato il protocollo TLS 1.2.
- I protocolli precedenti e deprecati (come SSL, TLS 1.0 e TLS 1.1) non sono disponibili e risultano disabilitati sull'infrastruttura.

I sistemi fruitori dei servizi dovranno garantire la compatibilità con questi standard e impegnarsi ad adeguare i propri client, nel caso in cui l'adozione di nuove policy di sicurezza porti all'obbligo di utilizzare versioni più recenti di TLS, in maniera coordinata con il sistema regionale SIRPED (ad esempio, qualora il TLS 1.2 venga deprecato a favore di versioni successive).

4.2 Specifiche dei servizi per la gestione dell'Id-Sessione con mail certificata

I servizi in oggetto consentono, agli utenti del Sistema Regionale SIRPED, di poter gestire l'Id-Sessione che deve essere comunicato sui servizi delle ricette dematerializzate oltre a user, password e pincode. L'Id-Sessione è costituito da un identificativo alfanumerico (UUID) generato dal sistema regionale, valido dal momento della richiesta per un tempo predefinito ed assegnato ad ogni utente-gestionale-Azienda.

I servizi resi disponibili dal sistema SIRPED per la gestione dell'Id-Sessione consentono di:

- Richiedere l'Id-Sessione.
- Verificare la validità di un Id-Sessione precedentemente richiesto.
- Revocare un Id-Sessione precedentemente richiesto.

I WSDL e gli XSD dei servizi sono gli stessi previsti da Sistema TS [A2F_STWS], con la personalizzazione regionale del contenuto di alcuni campi.

4.2.1 Servizio di richiesta dell'Id-Sessione

Il servizio consente di richiedere un Id-Sessione come indicato nel documento [A2F_STWS].

Al fine di consentire un test completo della ricezione dell'ID-Sessione e del suo utilizzo nelle chiamate ai servizi di

ricetta dematerializzata del sistema regionale SIRPED, **solamente nell'ambiente di TEST,** l'Id-Sessione viene restituito direttamente nella risposta del servizio, oltre ad essere inviato via e-mail.

Il servizio richiede la basic authentication con credenziali RUPAR (user, password e pincode) nominative.

Descrizione degli elementi costitutivi del messaggio di richiesta dell'Id-Sessione (CreateAuth):

Nome campo	Descrizione	Caratteristiche
userId	username della credenziale RUPAR dell'utente	obbligatorio
identificativo	Sezione contenente il Pincode dell'utente	
tipo	Valorizzare con P	obbligatorio
valore	Pincode Nel caso di richiamo del servizio sul SAR deve essere cifrato e inviato in base64. Per la cifratura occorre utilizzare lo stesso certificato già in uso per gli altri servizi della ricetta dematerializzata Nel caso di richiamo del servizio sulla CIL non deve essere cifrato.	obbligatorio
cfUtente	codice fiscale dell'utente autenticato che richiede l'Id-Sessione	obbligatorio
codRegione	codice regione dell'utente autenticato valorizzare con 010	obbligatorio
codAslAo	codice ASR a cui appartiene l'utente autenticato codice a 3 caratteri per le aziende private convenzionate o equiparate indicare il relativo codice regionale presente su ARPE, ad esempio: per Gradenigo 992, per la CDC 705.	obbligatorio
codSsa	codice STS11 associato all'utente autenticato	opzionale
codiceStruttura	non valorizzare	opzionale
contesto	Valorizzare con RICETTA-DEM	obbligatorio
applicazione	Elenco dei permessi richiesti per l'Id-Sessione; se si vuole richiedere più di un permesso, questi devono essere separati da spazio. I valori ammessi sono: • prescrizione • erogazione • presa_in_carico I permessi corrispondono ai profili definiti sul configuratore	obbligatorio

	regionale per ogni utente.	
opzioni	Non valorizzare	opzionale
infoAggiuntive	Sezione delle informazioni aggiuntive composta da due campi: chiave e valore. chiave=APP valore=codice del gestionale richiedente seguito da "_XXX", dove XXX è il codice dell'Azienda. Per gli MMG/PLS il codice dell'azienda corrisponde all'ASL del medico presso cui operano, per esempio 301. Per le aziende sanitarie pubbliche il codice dell'azienda è quella della ASR, per esempio 301. Per le aziende private convenzionate o equiparate il codice dell'azienda corrisponde al codice regionale presente su ARPE, ad esempio: per Gradenigo 992, per la CDC 705. Il codice del gestionale richiedente viene rilasciato da Regione Piemonte al momento dell'avvio dell'attività di autocertificazione. Esempio di valorizzazione: chiave=APP valore=MIOAPPLICATIVO_301	Obbligatorio

Descrizione degli elementi costitutivi del messaggio di risposta relativo alla richiesta dell'Id-Sessione (CreateAuth):

Nome campo	**Descrizione**	**Caratteristiche**
codEsito	Codice esito della risposta (per le codifiche, vedere paragrafo "Codifica esito operazione")	
errore	Sezione con l'elenco degli errori o degli avvisi	
tipoErrore	Tipo di errore (per le codifiche, vedere paragrafo "Codifica esito operazione")	
codEsito	Codice dell'errore	
descrEsito	Descrizione dell'errore	
info	Sezione delle informazioni aggiuntive in riposta formato da due campi: chiave e valore. Il sistema restituisce due informazioni identificate dalle	

	chiavi di seguito elencate. chiave=emailStatus valore=Email con token inviata con successo al notificatore regionale	
comunicazioni	Sezione delle comunicazioni composta da più sezioni comunicazione. Per ogni comunicazione vi sono due campi: codice e messaggio. Valori previsti: 1) Permessi codice=permessi messaggio=elenco dei permessi concessi a seguito delle verifiche sul configuratore. Se è presente più di un permesso, questi sono separati da spazio. Le codifiche previste sono le stesse di quelle inviate sul campo "Applicazione". 2) Restituzione dell'Id-Sessione codice=token messaggio=valore Id-Sessione generato 3) Restituzione del momento di scadenza dell'Id-Sessione codice=dataFineValidita messaggio=<data e ora di scadenza> 4) Ambiente di richiesta dell'Id-Sessione codice=Working-mode messaggio=TEST L'Id-Sessione è un UUID. L'Id-Sessione viene restituito se non vi sono stati errori bloccanti	**ATTENZIONE:** Questa sezione viene valorizzata solo in ambiente di TEST.

4.2.2 Servizio di verifica dell'Id-Sessione

Il servizio permette di verificare la validità dell'Id-Sessione.

Il servizio richiede la basic authentication con credenziali RUPAR (user, password e pincode) nominative.

Descrizione degli elementi costitutivi del messaggio di verifica dell'Id-Sessione (CheckToken):

Nome campo	Descrizione	Caratteristiche
userId	username della credenziale RUPAR dell'utente	obbligatorio

identificativo	Sezione contenente il Pincode dell'utente	
tipo	Valorizzare con P	obbligatorio
valore	Pincode Nel caso di richiamo del servizio sul SAR deve essere cifrato e inviato in base64. Per la cifratura occorre utilizzare lo stesso certificato già in uso per gli altri servizi della ricetta dematerializzata Nel caso di richiamo del servizio sulla CIL non deve essere cifrato.	obbligatorio
cfUtente	codice fiscale dell'utente autenticato	obbligatorio
token	Id-Sessione da verificare	obbligatorio
contesto	Valorizzare con RICETTA-DEM	obbligatorio
applicazione	Non valorizzare	N.A.
infoAggiuntive	Sezione delle informazioni aggiuntive composta da due campi: chiave e valore. chiave=APP valore=codice del gestionale richiedente seguito da "_XXX", dove XXX è il codice dell'Azienda. Per gli MMG/PLS il codice dell'azienda corrisponde all'ASL del medico presso cui operano, per esempio 301. Per le aziende sanitarie pubbliche il codice dell'azienda è quella della ASR, per esempio 301. Per le aziende private convenzionate o equiparate il codice dell'azienda corrisponde al codice regionale presente su ARPE, ad esempio: per Gradenigo 992, per la CDC 705. Il codice del gestionale richiedente viene rilasciato da Regione Piemonte al momento dell'avvio dell'attività di autocertificazione Esempio di valorizzazione: chiave=APP valore=MIOAPPLICATIVO_301	obbligatorio

Descrizione degli elementi costitutivi del messaggio di risposta relativo alla verifica dell'Id-Sessione (CheckToken):

Nome campo	Descrizione	Caratteristiche
codEsito	Codice esito della risposta (per le codifiche, vedere paragrafo "Codifica esito operazione")	
errore	Sezione con l'elenco degli errori o degli avvisi	
tipoErrore	Tipo di errore (per le codifiche, vedere paragrafo "Codifica esito operazione")	
codEsito	Codice dell'errore	
Errore.descrEsito	Descrizione dell'errore	
infoToken	Informazioni sul token	
stato	Stato del token 0->Valido 1-> Revocato 2-> Scaduto	
descrizione	Valido Revocato Scaduto	
dataInizioValidita	Data e ora di inizio validità del token	
dataFineValidita	Data e ora di fine validità del token	
comunicazioni	Sezione delle comunicazioni composta, per ogni comunicazione, da due campi: codice e messaggio. Disponibile solo in ambiente di test. Valori ammessi: 1) Ambiente di richiesta dell'Id-Sessione Codice=Working-mode messaggio= TEST	

4.2.3 Servizio di revoca dell'Id-Sessione

Il servizio permette di revocare un Id-Sessione.

Il servizio richiede la basic authentication con credenziali RUPAR (user, password e pincode) nominative.

Descrizione degli elementi costitutivi del messaggio di revoca dell'Id-Sessione (RevokeAuth):

Nome campo	Descrizione	Caratteristiche
userId	username della credenziale RUPAR dell'utente	Obbligatorio
identificativo	Sezione contenente il Pincode dell'utente.	
tipo	Valorizzare con P	obbligatorio
valore	Pincode Nel caso di richiamo del servizio sul SAR deve essere cifrato e inviato in base64. Per la cifratura occorre utilizzare lo stesso certificato già in uso per gli altri servizi della ricetta dematerializzata Nel caso di richiamo del servizio sulla CIL non deve essere cifrato.	obbligatorio
cfUtente	codice fiscale dell'utente autenticato.	obbligatorio
token	Id-Sessione da revocare	obbligatorio
contesto	Valorizzare con RICETTA-DEM	obbligatorio
applicazione	Non valorizzare	N.A.
opzioni	Elenco sezione opzioni	opzionale
infoAggiuntive	Sezione delle informazioni aggiuntive composta da due campi: chiave e valore. chiave=APP valore=codice del gestionale richiedente seguito da "_XXX", dove XXX è il codice dell'Azienda. Per gli MMG/PLS il codice dell'azienda corrisponde all'ASL del medico presso cui operano, per esempio 301. Per le aziende sanitarie pubbliche il codice dell'azienda è quella della ASR, per esempio 301. Per le aziende private convenzionate o equiparate il codice dell'azienda corrisponde al codice regionale presente su ARPE, ad esempio: per Gradenigo 992, per la CDC 705. Il codice del gestionale richiedente viene rilasciato da Regione Piemonte al momento dell'avvio dell'attività di autocertificazione	obbligatorio

	Esempio di valorizzazione: chiave=APP valore=MIOAPPLICATIVO_301	

Descrizione degli elementi costitutivi del messaggio di risposta relativo alla revoca dell'Id-Sessione (RevokeAuth):

Nome campo	**Descrizione**	**Caratteristiche**
codEsito	Codice esito della risposta (per le codifiche, vedere paragrafo "Codifica esito operazione")	
errore	Sezione con l'elenco degli errori o degli avvisi	
tipoErrore	Tipo di errore (per le codifiche, vedere paragrafo "Codifica esito operazione")	
codEsito	Codice dell'errore	
Errore.descrEsito	Descrizione dell'errore	
info	Sezione delle comunicazioni composta, per ogni comunicazione, da due campi: chiave e valore. I possibili valori restituiti sono: 1) Chiave=revokeStatus valore=Revoca del token eseguita correttamente valorizzato se la revoca ha avuto successo 2) Chiave=lastRevokePreviousDate valore=30/05/2025 20:51:07 valorizzato se si tenta di revocare un Id-Sessione già revocato in precedenza 3) Chiave=expiredDate Valore=30/05/2025 20:51:07 valorizzato se si tenta di revocare un Id-Sessione scaduto	
comunicazioni	Sezione delle comunicazioni composta, per ogni comunicazione, da due campi: codice e messaggio. Valori ammessi:	

	1) Ambiente di richiesta dell'Id-Sessione Codice=Working-mode messaggio= TEST	
infoAggiuntive	Sezione non valorizzata.	

4.2.4 Codifica esito operazione

L'esito delle chiamate ai servizi di gestione token ritornano sempre e solo due valori che avranno i seguenti significati:

- 0 → esito positivo
- 1 → esito negativo.

In caso di esito negativo, la risposta sarà accompagnata da una sezione che conterrà la definizione dell'errore: tipo, codice, descrizione dell'errore:

```
<a:errore>
  <a:tipoErrore>E</a:tipoErrore>
  <a:codEsito>9998</a:codEsito>
  <a:descrEsito> >Errore di configurazione nella chiamata al servizio</a:descrEsito>
</a:errore>
```

Il tipoErrore può assumere i seguenti valori:

- W : Warnig → Un avviso gestito che non causa un errore.
- E : Error → Errore nell'applicazione, spesso legato ad un'incongruenza tra i dati attesi e quelli inviati.
- F : Fatal → Un evento grave, imprevisto che impedirà il corretto funzionamento dell'applicazione.

4.2.5 Utilizzo dell'Id-Sessione con i servizi della ricetta dematerializzata

I servizi della ricetta dematerializzata, esposti dal SAR e dalle CIL, coinvolti sono:

- invio prescritto
- annulla prescritto
- interroga nre utilizzati
- visualizza erogato
- invio erogato
- sospendi erogato
- annulla erogato
- servizi ausiliari di erogazione
- richiesta nre (per le CIL)

Il sistema regionale SIRPED effettuerà delle verifiche sulla validità dell'Id-Sessione, trasmesso nella chiamata ai suddetti servizi, e sulla coerenza del servizio chiamato con le abilitazioni dell'utente presenti sul configuratore regionale.

Utilizzando questa modalità i gestionali devono autenticarsi ai servizi tramite credenziali RUPAR con PINCODE assegnate al singolo utente; pertanto, non è più consentito l'uso di credenziali applicative.

I gestionali dovranno valorizzare nell'Header http dei servizi sopra elencati le seguenti informazioni:

Tag HTTP	Descrizione	Obbligatorietà	Note
X-idSessione	Identificativo della sessione ottenuto tramite il servizio createAuth	Sì	secondo l'Auth Schema "Bearer authentication". Ad esempio: X-idSessione: Bearer <Id-Sessione>
X-Gestionale	Codice del gestionale richiedente seguito da "_XXX", dove XXX è il codice dell'Azienda. Per gli MMG/PLS il codice dell'azienda corrisponde all'ASL del medico presso cui operano, per esempio 301. Per le aziende sanitarie pubbliche il codice dell'azienda è quella della ASR, per esempio 301. Per le aziende private convenzionate o equiparate il codice dell'azienda corrisponde al codice regionale presente su ARPE, ad esempio: per Gradenigo 992, per la CDC 705.	Sì	Il codice del gestionale richiedente viene rilasciato da Regione Piemonte al momento dell'avvio dell'attività di autocertificazione Esempio di valorizzazione: valore=MIOAPPLICATIVO_301

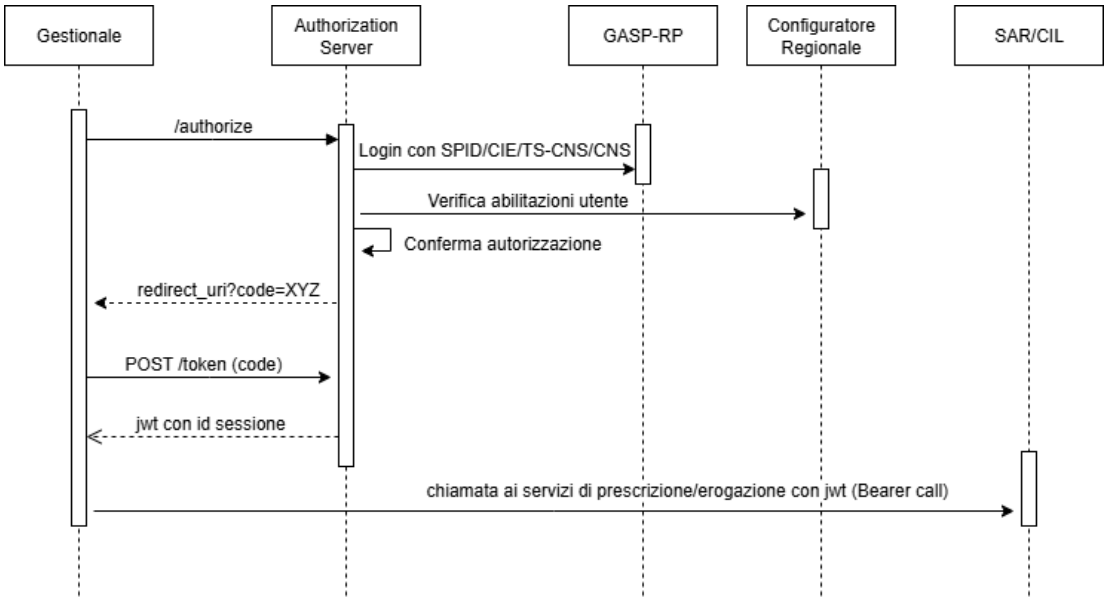
4.3 Specifiche dei servizi per la gestione dell'Id-Sessione con protocollo OAuth2

I servizi in oggetto consentono, agli utenti del Sistema Regionale SIRPED, di poter gestire l'Id-Sessione che deve essere comunicato sui servizi delle ricette dematerializzate. L'Id-Sessione è costituito da un identificativo alfanumerico (UUID) generato dal sistema regionale, valido dal momento della richiesta per un tempo predefinito ed assegnato ad ogni utente-gestionale-Azienda.

Il sistema SIRPED mette a disposizione, oltre ai servizi standard del protocollo OAuth2 per l'acquisizione dell'Id-Sessione, due servizi regionali per:

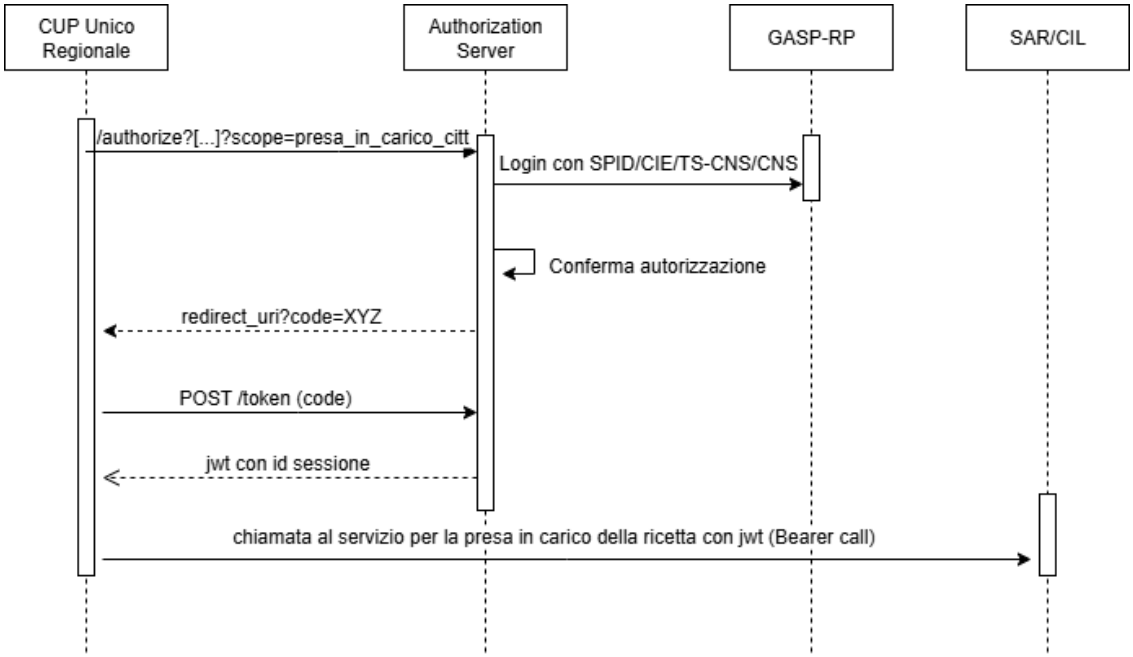
- Verificare la validità di un Id-Sessione precedentemente richiesto.
- Revocare un Id-Sessione precedentemente richiesto.

Di seguito viene riportato lo schema delle interazioni tra i sistemi coinvolti per l'acquisizione dell'ID-Sessione nel caso in cui l'utente sia un operatore delle strutture pubbliche o private convenzionate/equiparate o un medico di famiglia:



- Il gestionale redirige l'utente verso l'endpoint /oauth2/authorize dell'Authorization Server, specificando parametri quali client_id, redirect_uri, scope, oltre alla challenge PKCE.
- L'utente effettua l'autenticazione con SPID/CIE/TS-CNS/CNS di, almeno, livello 2
- L'authorization server controlla se i profili richiesti per l'utente (*scope*) sono presenti sul configuratore regionale degli operatori
- L'authorization server visualizza all'utente i suoi ruoli e le collocazioni relativi all'azienda del gestionale chiamante (in base al valore del parametro *client_id*)
- Se, sul configuratore regionale, risulta che l'utente ha più ruoli e/o opera in più collocazioni, deve selezionare prima un ruolo e poi una collocazione
- L'authorization server visualizza all'utente i permessi per cui sta autorizzando il gestionale; i permessi corrispondono all'intersezione tra i valori indicati nel parametro scope e quelli presenti sul configuratore regionale per il ruolo e la collocazione selezionati
- L'utente autorizza e viene reindirizzato verso l'endpoint di callback (redirect_uri) fornito dal gestionale, con un *authorization code* e lo stato (*state*) di correlazione
- Il gestionale utilizza il codice ottenuto per effettuare una chiamata POST sull'endpoint /oauth2/token al fine di ottenere l'access_token/jwt
- L'access_token/jwt deve essere utilizzato per invocare i servizi della ricetta dematerializzata esposti dal sistema regionale SIRPED.

Nel caso in cui l'utente sia un cittadino, che effettua le prenotazioni delle ricette dematerializzate in autonomia accedendo al servizio on-line del CUP Unico Regionale, lo schema di interazione tra i sistemi per l'acquisizione dell'Id-Sessione è il seguente:



- Il gestionale redirige il cittadino verso l'endpoint /oauth2/authorize dell'Authorization Server, specificando parametri quali client_id, redirect_uri, *scope=presa_in_carico_citt*, oltre alla challenge PKCE
- Il cittadino effettua l'autenticazione con SPID/CIE/TS-CNS/CNS di, almeno, livello 2
- L'authorization server visualizza al cittadino i permessi per cui sta autorizzando il gestionale
- Il cittadino autorizza e viene reindirizzato verso l'endpoint di callback (redirect_uri) fornito dal gestionale, con un *authorization code* e lo stato (*state*) di correlazione
- Il gestionale utilizza il codice ottenuto per effettuare una chiamata POST sull'endpoint /oauth2/token al fine di ottenere l'access_token/jwt
- L'access_token/jwt deve essere utilizzato per invocare il servizio per la presa in carico della ricetta dematerializzata esposto dal sistema regionale SIRPED.

Lo scope deve essere valorizzato con il codice "presa_in_carico_citt".

Il CUP Unico Regionale dovrà gestire per ogni cittadino un differente JWT e la sua relativa scadenza.

Al CUP Unico Regionale verranno assegnati due distinti client_id: uno per il servizio online delle prenotazioni per i cittadini ed uno per il gestionale ad uso degli operatori.

4.3.1 Servizio di Autorizzazione dell'Utente (Authorization Endpoint)

L'accesso alle risorse (servizi e applicazioni) protette mediante protocollo OAuth2 avviene tramite l'endpoint di autorizzazione, il quale avvia il flusso di autenticazione da parte dell'utente.

Diversamente dai tradizionali servizi web, questo endpoint non è progettato per l'invocazione diretta da parte dei gestionali.

La modalità operativa prevede il reindirizzamento dell'utente all'URL di autorizzazione tramite redirect HTTP.

Le applicazioni non web-based dovranno implementare l'apertura di un browser esterno per consentire il reindirizzamento verso l'endpoint di autorizzazione.

URL ESPOSTA DALL'AUTHORIZATION SERVER:

```
GET /oauth2/authorize
```

PARAMETRI RICHIESTI

Parametro	Descrizione
client_id	Codice del gestionale richiedente seguito da "_XXX", dove XXX è il codice dell'Azienda. Per gli MMG/PLS il codice dell'azienda corrisponde all'ASL del medico presso cui operano, per esempio 301. Per le aziende sanitarie pubbliche il codice dell'azienda è quella della ASR, per esempio 301. Per le aziende private convenzionate o equiparate il codice dell'azienda corrisponde al codice regionale presente su ARPE, ad esempio: per Gradenigo 992, per la CDC 705. Per il CUP Unico Regionale ad uso degli operatori delle aziende pubbliche e private convenzionate o equiparate, il codice dell'Azienda deve essere quello a cui appartiene l'operatore. Per il CUP Unico Regionale ad uso degli operatori del call center e del cittadino, il codice dell'Azienda deve essere quello che Regione Piemonte indicherà come "capofila" (es. Azienda Zero codice 900) Il codice del gestionale richiedente viene rilasciato da Regione Piemonte al momento dell'avvio dell'attività di autocertificazione Esempio di valorizzazione: valore=MIOAPPLICATIVO_301
response_type	Valorizzare con code
redirect_uri	URL di callback verso cui l'utente sarà reindirizzato al termine del processo di autorizzazione (dettagliato nei successivi paragrafi).
scope	elenco degli scope/permessi richiesti. E' possibile fornire un elenco di scope separandoli con uno spazio
state	Stringa casuale generata dal gestionale per ricordare informazioni relative alla sessione utente o all'operazione in corso e prevenire attacchi CSRF. Questa stringa viene restituita inalterata in callback. La stringa può avere una lunghezza massima di 500 caratteri.
code_challenge	Challenge conforme a [RFC 7636 - PKCE] (viene riportato un esempio nei successivi paragrafi)

code_challenge_method	Metodo di calcolo del challenge, valorizzare con S256.

SCOPE

All'interno del parametro *scope* devono essere specificati uno o più permessi, separati da spazio.

Di seguito l'elenco dei valori disponibili per il parametro scope:

Scope	Descrizione
prescrizione	Consente la prescrizione delle ricette dematerializzate
erogazione	Consente la sola erogazione delle ricette dematerializzate
presa_in_carico	Consente la sola presa in carico delle ricette dematerializzate
presa_in_carico_citt	Consente la presa in carico delle ricette dematerializzate da parte del cittadino. Riservato esclusivamente al servizio di prenotazione on-line per il cittadino del CUP Unico Regionale

I valori degli scope corrispondono ai profili disponibili sul Configuratore Regionale per il sistema regionale SIRPED.

REDIRECT URI

L'endpoint di callback (redirect URI) è l'URL esposta dal gestionale per ricevere la risposta al termine del processo di autorizzazione e costituisce il punto di ritorno in cui verrà reindirizzato l'utente (sia in caso di successo che di errore).

La redirect_uri può essere anche un indirizzo locale alla postazione dell'utente (ad esempio *http://localhost:8081/callback*) in particolare durante le fasi di sviluppo, testing, nel caso di applicazioni desktop o native mobile (non web-oriented).

La specifica OAuth2 e il protocollo PKCE prevedono che il ritorno avvenga tramite redirect del browser dell'utente anche verso una risorsa HTTP locale alla postazione dell'utente, in quanto non trattasi di una "chiamata server to server", ma di una semplice redirezione HTTP eseguita dal client (il browser).

Importante: La redirect_uri dovrà essere nota al sistema regionale prima dell'avvio della nuova modalità di autenticazione. La redirect_uri presente nel servizio `authorize` dovrà corrispondere esattamente (path e protocollo) a quanto noto al sistema regionale. E' possibile fornire al sistema regionale un elenco di url che potranno essere utilizzate ove previsto dal protocollo OAuth2. Il servizio *Authorize* richiede una sola redirect_uri per ogni chiamata.

Quando l'utente completa la fase di autorizzazione, l'Authorization Server effettua un redirect verso la redirect_uri (o endpoint di callback) specificata dal gestionale fruitore, aggiungendo i parametri *code* e *state*.

Il gestionale quando riceve la chiamata sul redirect_uri deve effettuare almeno le seguenti attività:

- Validazione del parametro "state":
  La specifica **[JWT-STD]** prevede che venga verificato che il parametro *state* ricevuto nella richiesta di callback corrisponda a quello generato e memorizzato al momento dell'avvio della richiesta di autorizzazione.

Questa operazione serve a garantire la sicurezza della transazione ed evitare attacchi di tipo CSRF (Cross-Site Request Forgery).

- Estrazione e utilizzo del parametro "code":
  Il codice di autorizzazione (code) deve essere estratto dalla query string e utilizzato entro la sua scadenza, che sarà fissata nell'ordine di qualche minuto, per invocare l'endpoint /oauth2/token: sarà così possibile ottenere un access token valido per accedere ai servizi protetti.
- Gestione della user experience all'interno della pagina di callback: una volta elaborata la richiesta, il gestionale dovrà:
  - fornire un messaggio di feedback comprensibile all'utente sull'esito dell'operazione (ad esempio "Accesso autorizzato", "Operazione annullata", ecc.)
  - gestire eventuali errori (ad esempio: mancanza di parametri, errore di validazione del parametro *state*, timeout del codice, ecc.), mostrando all'utente messaggi chiari e appropriati.

REQUEST DI ESEMPIO:

```
GET
/oauth2/authorize?client_id=myapp&response_type=code&redirect_uri=http://localhost:8081
/callback&scope=prescrizione&state=abcxyz&code_challenge=...&code_challenge_method=S256
```

L'utente effettuerà l'autenticazione, fornirà l'autorizzazione e sarà reindirizzato verso:

```
http://localhost:8081/callback?code=<authorization-code>&state=abcxyz
```

REDIRECT URI IN CASO DI ERRORE

Nella fase di autorizzazione, l'Authentication Server può comunicare al sistema chiamante un esito di errore.

In questo caso non si otterrà il token di autorizzazione, non sarà possibile procedere con lo scambio del token di autenticazione (servizio token) e il processo non potrà proseguire.

Il gestionale chiamante dovrà prevedere che la url di callback sia in grado di gestire anche il caso sopra descritto.

Esempio di url di callback in errore:

```
https://localhost:9443/oauth/callback?error=access_denied&error_description=L'utente non possiede le
abilitazioni sul configuratore regionale
```

In generale in caso di errore, i parametri restituiti sulla url di callback saranno:

- *error*: può assumere uno dei seguenti valori:

Codice errore	Quando viene restituito il codice di errore
access_denied	Accesso negato
invalid_request	Parametri mancanti/errati
invalid_grant	I dati dell'utente o del client non sono validi per la generazione dell'authorization code

unauthorized_client	Il client_id non è abilitato per questo flusso
invalid_client	Parametro client_id non riconosciuto o code_challenge e code_verifier non corrispondenti/non verificabili
unsupported_grant_type	Grant type non supportato
invalid_scope	Scope richiesto non valido
invalid_request	Request non valida
server_error	Il server ha incontrato un errore non gestito
Invalid_redirect_uri	Redirect URI non valida

- *error_description*: Opzionale, l'authorization server potrebbe non fornirlo in tutti i casi, indica una descrizione di dettaglio che specifica meglio la situazione di errore.

PKCE

L'authorization server di SIRPED utilizza PKCE (Proof Key for Code Exchange) per impedire l'intercettazione del codice di autorizzazione senza distribuire password ai client. PKCE prevede la generazione di:

- *code_verifier*: stringa casuale generata dal client, utilizzata nel servizio di scambio token, la stringa deve avere una lunghezza compresa tra 43 e 128 caratteri;
- *code_challenge*: versione hash del code_verifier, utilizzata nella richiesta di autorizzazione iniziale (servizio authorize);

Nota: il code_verifier viene generato per primo ma trasmesso successivamente sul servizio token; il servizio authorize richiede il code_challenge.

Esempio generazione di PKCE (code_challenge e code_verifier)

Viene riportato un esempio di generazione di entrambi i codici tramite bash shell Linux:

```
#### Generazione PKCE

# Genera code_verifier (stringa random base64url di 43-128 caratteri)
CODE_VERIFIER=$(openssl rand -base64 32 | tr -d "=+/" | cut -c1-43)
echo "Code Verifier: $CODE_VERIFIER"

# Genera code_challenge (SHA256 hash del code_verifier, base64url encoded)
CODE_CHALLENGE=$(echo -n $CODE_VERIFIER | openssl dgst -sha256 -binary | openssl base64 | tr -d "=+/" | tr -d
'\n')
echo "Code Challenge: $CODE_CHALLENGE"
```

4.3.2 Servizio Token

Il Servizio Token permette lo scambio del codice di autorizzazione (authorization_code) ricevuto sulla URI di callback, con l'access token per accedere ai servizi delle ricette dematerializzate.

L'access token rilasciato dal sistema è un JWT (JSON Web Token).

A differenza del servizio di autorizzazione, questo è un servizio REST classico.

Il Servizio Token implementa la specifica OAuth2 e richiede grant di tipo Authorization Code, (grant_type= authorization_code) con PKCE (come descritto nel paragrafo precedente).

Si precisa che, nonostante la specifica OAuth2 preveda anche il grant di tipo refresh_token per il rinnovo automatico dei token, l'authentication server del sistema regionale SIRPED non supporterà questo grant.

Questa scelta è motivata dai requisiti normativi del decreto, che impone una scadenza fissa per i token di accesso. Di conseguenza, alla scadenza del token sarà sempre necessario richiedere una nuova autorizzazione esplicita all'utente.

URL ESPOSTA DALL'AUTHORIZATION SERVER:

```
POST /oauth2/token
Content-Type: application/x-www-form-urlencoded
grant_type=authorization_code
&code=...
&redirect_uri=...
&client_id=...
&code_verifier=...
```

PARAMETRI RICHIESTI

Descrizione degli elementi del messaggio di richiesta:

Nome	Obbligatorio	Descrizione
grant_type	Sì	valorizzare con authorization_code
code	Sì	Il codice di autorizzazione ricevuto sulla callback
redirect_uri	Sì	Deve coincidere esattamente con quanto inviato sul servizio authorize
client_id	Sì	Codice del gestionale richiedente seguito da "_XXX", dove XXX è il codice dell'Azienda. Per gli MMG/PLS il codice dell'azienda corrisponde all'ASL del medico presso cui operano, per esempio 301. Per le aziende sanitarie pubbliche il codice dell'azienda è quella della ASR, per esempio 301. Per le aziende private convenzionate o equiparate il codice dell'azienda corrisponde al codice regionale presente su ARPE, ad esempio: per Gradenigo 992, per la CDC 705. Per il CUP Unico Regionale ad uso degli operatori delle aziende pubbliche e private convenzionate o equiparate, il codice dell'Azienda deve essere quello a cui appartiene l'operatore. Per il CUP Unico Regionale ad uso degli operatori del call center e del cittadino, il

		codice dell'Azienda deve essere quello che Regione Piemonte indicherà come "capofila" (es. Azienda Zero codice 900) Il codice del gestionale richiedente viene rilasciato da Regione Piemonte al momento dell'avvio dell'attività di autocertificazione Esempio di valorizzazione: valore=MIOAPPLICATIVO_301
code_verifier	Sì	Il code_verifier generato dal client, necessario per validare la challenge PKCE (vedi paragrafo precedente)

Descrizione degli elementi del messaggio di risposta:

Nome	Descrizione
access_token	Stringa JWT che rappresenta il token di accesso rilasciato dall'Authorization Server. Deve essere utilizzato nelle richieste ai servizi della ricetta dematerializzata.
scope	Elenco dei permessi effettivamente concessi con il token, separati da spazio. Corrisponde agli *scope* autorizzati dall'utente e quindi determina i servizi della ricetta dematerializzata per i quali il token può essere utilizzato.
token_type	Specifica la tipologia del token; valorizzato con *Bearer*
client_id	Identificativo del gestionale a cui è stato rilasciato il token.
expires_in	Durata di validità residua del token di accesso, in formato Unix time (secondi dal 1970-01-01T00:00:00Z). Indica per quanto tempo il token può essere utilizzato prima di essere considerato scaduto.

I campi indicati sono quelli standard del protocollo OAuth2, per maggiori dettagli fare riferimento a [JWT-STD].

FORMATO DELL'ACCESS_TOKEN (JWT)

Il token JWT è composto da <Header>.<Payload>.<Signature>

Le sezioni Header, Payload e Signature sono codificate in base64.

La parte di payload è costituita dai seguenti campi:

Campo	**Descrizione**
sub **(*)**	(Subject) Codice fiscale dell'utente a cui il token è stato assegnato (utente autenticato).
aud **(*)**	(Audience) Identificativo del client (gestionale) per cui il token è stato rilasciato (negli esempi: MIOAPPLICATIVO_301).
nbf **(*)**	(Not Before) Istante in cui il token diventa valido, in formato Unix

		time (secondi dal 1970-01-01T00:00:00Z).
userData		Oggetto che contiene dati personalizzati relativi all'utente e alla sessione di autenticazione.
	cfutente	Codice fiscale dell'utente (valorizzato come il campo *sub*).
	idSessione	Identificativo univoco della sessione di autenticazione.
	autenticazioneTs	Timestamp della data/ora dell'autenticazione dell'utente, formattato come dd/MM/yyyy HH:mm.ss.SSSS, rilevata dal sistema regionale SIRPED (secondo la configurazione dell'ora dei server del sistema)
	livelloAautenticazione	Livello di autenticazione ottenuto. Valori possibili: • iso-iec-29115-LoA3 • iso-iec-29115-LoA4
	modAautenticazione	Modalità di autenticazione ottenuto. Valori possibili: • SpidL2 • SpidL3 • CNS (Accesso con carta nazionale dei servizi) • CIEL2 • CIEL3
	organizzazione	Identificativo dell'organizzazione associata all'utente: • Per le strutture pubbliche è il codice dell'ASR (codice a 3 caratteri, p.es 301 ASR Città di Torino) • Per le aziende private convenzionate o equiparate il codice dell'azienda corrisponde al codice regionale presente su ARPE, ad esempio: per Gradenigo 992, per la CDC 705. • Vuoto per il cittadino.
	scope	Elenco dei permessi concessi dall'utente: può essere diverso da quanto richiesto dal gestionale in fase di autorizzazione sia per le abilitazioni presenti sul Configuratore Regionale, sia perché l'utente può non autorizzare tutti gli *scope*. Codici degli *scope* previsti: prescrizione, erogazione, presa_in_carico, presa_in_carico_citt
	clientid	Identificativo del gestionale a cui il token si riferisce (valorizzato come il campo *aud*).
scope **(*)**		Contiene le stesse informazioni del campo scope della sezione userData
iss **(*)**		(Issuer) URL dell'Authorization Server che ha emesso il token.

exp **(*)**	(Expiration) Scadenza del token, in formato Unix time (secondi dal 1970-01-01T00:00:00Z). Indica quando il token non sarà più valido.
iat **(*)**	(Issued At) Istante di emissione del token in formato Unix time (secondi dal 1970-01-01T00:00:00Z).
jti **(*)**	JWT ID. Identificativo univoco del token

(*) In merito ai campi standard previsti dal protocollo fare riferimento a [JWT-STD].

Il token JWT viene firmato mediante un certificato e la firma viene riportata nella sezione signature.

REQUEST/RESPONSE DI ESEMPIO

Esempio di request:

```
POST /oauth2/token HTTP/1.1
Host: <url-dei-servizi-oauth2>
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=12234-aaa-bbb-456

grant_type=authorization_code
&client_id=MIOAPPLICATIVO_301
&code_verifier=AOODWpBSX8mEomeyQD9PP3u4AAZGnwOiqiuYFJOwvY
&code=jMmB1EQ-0SyAS7xgOMwN2EAx2dA…
&redirect_uri=http://localhost:8082/callback
```

Esempio di response:

```
{
    "access_token": "eyJraWQiOiJkOWQzMzI2MS04YjIwLTQwMDItYmVkNC05YzEz …",
    "scope": "prescrizione",
    "token_type": "Bearer",
    "expires_in": 7199
}
```

4.3.3 Servizio JWKS (JSON Web Key Set)

Il Servizio JWKS espone la chiave pubblica da utilizzare per la verifica della firma digitale dei JWT rilasciati dal sistema SIRPED.

Questo servizio è implementato secondo lo standard RFC 7517 (JSON Web Key).

Lo standard offre la possibilità di utilizzare più chiavi, nel caso del sistema SIRPED viene utilizzata una unica chiave.

URL ESPOSTA DALL'AUTHORIZATION SERVER:

```
/.well-known/jwks.json
```

FORMATO DELLA CHIAVE

La risposta del servizio è un JSON così composto:

Campo		Descrizione
keys		Elenco delle chiavi; SIRPED ne usa solo una.
	Kty	Tipo di chiave. Fisso a "RSA"
	e	Esponente RSA in Base64URL senza padding. Fisso a "AQAB" (65537).
	kid	Identificatore univoco della chiave, usato dai client per selezionare la chiave corretta per verificare il JWT. Fisso a "rel-oauth2-key"
	v	Rappresenta la parte principale della chiave pubblica. Modulo RSA in Base64URL senza padding.

REQUEST/RESPONSE DI ESEMPIO

Esempio di request:

```
GET /reloauthserver/.well-known/jwks.json HTTP/1.1
Host: <url-dei-servizi-oauth2>
```

Esempio di response:

```
{
   "keys":[
      {
         "kty":"RSA",
         "e":"AQAB",
         "kid":"rel-oauth2-key",
         "n":"qM_8..."
      }
   ]
}
```

4.3.4 Servizio di verifica dell'Id-Sessione contenuto nel JWT

Il servizio permette di verificare la validità dell'Id-Sessione contenuto nel JWT.

Descrizione degli elementi costitutivi del messaggio di verifica dell'Id-Sessione

URL ESPOSTA DALL'AUTHORIZATION SERVER:

```
GET /sessionid/verify?client_id=...&cfutente=...
Authorization: Bearer <jwt_token>
Content-Type: application/json
```

PARAMETRI RICHIESTI

Nome	Obbligatorio	Descrizione
client_id	Sì	Identificativo assegnato al gestionale; deve corrispondere al client_id che ha eseguito l'operazione di richiesta del *token*
cfutente	Sì	Codice fiscale dell'utente a cui è associato il token jwt

Il servizio richiede che l'intestazione di sicurezza (header http) sia valorizzato come segue:

Authorization: Bearer <access_token>

Dove access_token è la stringa jwt in base64 restituito nell'*access_token* dal servizio *token*.

Il servizio restituisce l'esito dell'operazione nello status code:

Codice	Quando viene restituito il codice
200	Operazione eseguita correttamente, viene restituito lo stato dell'Id-Sessione
401	Token non valido Verrà restituito quando il jwt non è riconosciuto dal sistema.
500	Errore di elaborazione del sistema

Il servizio restituisce un json come segue:

Nome campo	Descrizione	Caratteristiche
errore	Sezione con l'elenco degli errori o degli avvisi	Valorizzato se status code=500 Il dettaglio dell'errore viene restituito solo se il token JWT fornito in fase di autenticazione viene riconosciuto come valido.
tipoErrore	Tipo di errore può assumere i seguenti valori: • W : Warnig → Un avviso gestito che non causa un errore. • E : Error → Errore nell'applicazione	

	• F : Fatal → Un evento grave, imprevisto che impedirà il corretto funzionamento dell'applicazione.	
codEsito	Codice dell'errore	
Errore.descrEsito	Descrizione dell'errore	
infoToken	Informazioni sul token	Valorizzato se status code=200
stato	Stato del token 0->Valido 1-> Revocato 2-> Scaduto	
descrizione	Valido Revocato Scaduto	
dataInizioValidita	Data e ora di inizio validità del token	
dataFineValidita	Data e ora di fine validità del token	

REQUEST/RESPONSE DI ESEMPIO

Esempio di request:

```
GET /reloauthserver/sessionid/verify?client_id=xxx&cfutente=xxx HTTP/1.1
Host: <url-dei-servizi-oauth2>
Authorization: Bearer <access_token>
```

Esempio di response:

```
HTTP/1.1 200
{
    "infoToken": {
        "stato": 0,
        "descrizione": "Valido",
        "dataInizioValidita": "2025-10-17T08:00:00.000Z",
        "dataFineValidita": "2025-10-17T18:00:00.000Z"
    }
}
```

Esempio di response in caso di errore:

```
HTTP/1.1 401
```

Esempio di response in caso di errore 500:

```
HTTP/1.1 500
{
    "errore": {
        "codEsito": "xxxx",
        "tipoErrore": "E",
        "descrEsito": "Identificativo del gestionale non riconosciuto"
    }
}
```

4.3.5 Servizio di revoca del token

Il Servizio di Revoca Token permette al gestionale di invalidare un token di accesso jwt precedentemente rilasciato, rendendolo inutilizzabile per accedere ai servizi della ricetta dematerializzata.

Si evidenzia che il jwt mantiene la sua validità formale dal punto di vista crittografico e di scadenza; tuttavia, i servizi delle ricette dematerializzate verificheranno la validità dell'Id-Sessione. L'utilizzo di un token con Id-Sessione revocata genererà un errore, impedendo l'accesso alle funzionalità del sistema.

URL ESPOSTA DALL'AUTHORIZATION SERVER:

```
DELETE /sessionid/revoke?client_id=...&cfutente=...
Authorization: Bearer <jwt_token>
Content-Type: application/json
```

PARAMETRI RICHIESTI

Nome	Obbligatorio	Descrizione
client_id	Sì	Identificativo assegnato al gestionale; deve corrispondere al client_id che ha eseguito l'operazione di richiesta del *token*
cfutente	Sì	Codice fiscale dell'utente a cui è associato il token jwt

Il servizio richiede che l'intestazione di sicurezza (header http) sia valorizzato come segue:

Authorization: Bearer <access_token>

Dove access_token è la stringa jwt in base64 restituito nell'*access_token* dal servizio *token*.

Il servizio restituisce l'esito dell'operazione nello status code:

Codice	Quando viene restituito il codice
200	Operazione eseguita correttamente: il token JWT è stato revocato
401	Verrà restituito quando il token jwt fornito è scaduto oppure l'Id-Sessione è già stato revocato oppure il jwt non è riconosciuto dal sistema.

500	Errore di elaborazione del sistema. Non è stato possibile revocare l'Id-Sessione associato al jwt per un errore di elaborazione del sistema.

Il servizio restituisce un json come segue:

Nome campo	Descrizione	Caratteristiche
errore	Sezione con l'elenco degli errori o degli avvisi, se previsti	Valorizzato se status code=500 Il dettaglio dell'errore viene restituito solo se il token JWT fornito in fase di autenticazione viene riconosciuto come valido.
tipoErrore	Tipo di errore può assumere i seguenti valori: • W : Warnig → Un avviso gestito che non causa un errore. • E : Error → Errore nell'applicazione • F : Fatal → Un evento grave, imprevisto che impedirà il corretto funzionamento dell'applicazione.	
codEsito	Codice dell'errore	Tra gli errori restituiti viene indicato anche se l'Id-Sessione risultava già revocato oppure scaduto
Errore.descrEsito	Descrizione dell'errore	

Esempio di request:

```
DELETE /reloauthserver/sessionid/revoke?client_id=xxx&cfutente=xxx HTTP/1.1
Host: <url-dei-servizi-oauth2>
Authorization: Bearer <access_token>
```

Esempio di response:

```
HTTP/1.1 200
```

Esempio di response in caso di errore 401:

```
HTTP/1.1 401
```

Esempio di response in caso di errore 500:

```
HTTP/1.1 500
```

```
{
    "errore": {
        "codEsito": "xxxx",
        "tipoErrore": "E",
        "descrEsito": "Identificativo del gestionale non riconosciuto"
    }
}
```

4.3.6 Utilizzo del token di autorizzazione con i servizi della ricetta dematerializzata

I servizi della ricetta dematerializzata esposti dal SAR e dalle CIL coinvolti sono:

- Invio prescritto
- annulla prescritto
- interroga nre utilizzati
- visualizza erogato
- invio erogato
- sospendi erogato
- annulla erogato
- servizi ausiliari di erogazione
- richiesta nre (per le CIL)

Il sistema regionale SIRPED effettuerà delle verifiche sulla validità del token JWT, trasmesso sulla chiamata ai suddetti servizi, e sulla coerenza del servizio chiamato con le abilitazioni dell'utente presenti sul configuratore regionale.

Per adeguare le chiamate ai web service SOAP del sistema regionale SIRPED alle nuove specifiche di sicurezza e autenticazione basate su OAuth2, è necessario sostituire l'autenticazione di tipo basic authentication con l'utilizzo di un JWT.

Di seguito vengono riportate le indicazioni operative da seguire:

- Utilizzare il JWT nell'header HTTP con schema *Bearer*.
- Rimuovere l'header *Authorization* di tipo Basic e ogni autenticazione HTTP basata su username e password.
- Lasciare sempre vuoto il campo *pinCode* nelle richieste SOAP ai suddetti servizi della ricetta dematerializzata.
- Non valorizzare altri parametri negli header di autenticazione nei messaggi SOAP.

Inserimento del JWT nell'header HTTP

Il token JWT in base64 così come fornito dal servizio *token* del protocollo OAuth2, deve essere riportato nell'intestazione HTTP di ogni chiamata ai servizi della ricetta dematerializzata, usando lo schema Bearer:

```
X-OAuth2-Authorization: Bearer <jwt>
```

Eliminazione della Basic HTTP authentication

Nel caso di utilizzo del jwt oauth2 non é consentito includere l'intestazione HTTP Authorization con schema Basic (username:password codificati in Base64).

Ogni sistema deve rimuovere tale autenticazione dalle chiamate.

Gestione del campo pinCode nel payload SOAP

Il campo pinCode, precedentemente utilizzato nelle request SOAP insieme alla Basic Authentication, deve essere impostato a vuoto (<pinCode></pinCode>) quando si usa il JWT.

Nessun altro dato di autenticazione deve essere valorizzato nel body o nell'header SOAP del messaggio.

Esempio di richiesta SOAP aggiornata

```
POST /servizio REL HTTP/1.1
Host: tst-rel-xxxx.csi.it
X-OAuth2-Authorization: Bearer <jwt>
Content-Type: text/xml; charset=utf-8

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:inv="http://invioprescrittorichiesta.xsd.dem.sanita.finanze.it"
xmlns:tip="http://tipodati.xsd.dem.sanita.finanze.it">
   <soapenv:Header/>
   <soapenv:Body>
      <inv:InvioPrescrittoRichiesta>
         <inv:pinCode></inv:pinCode>
         <inv:cfMedico1>xxxx</inv:cfMedico1>
   [...]
      </inv:InvioPrescrittoRichiesta>
   </soapenv:Body>
</soapenv:Envelope>
```