SISTEMA TESSERA SANITARIA

MODALITA' DI ACCESSO TRAMITE AUTENTICAZIONE A 2 O PIU' FATTORI AI SERVIZI (WEB SERVICES) DELLA RICETTA BIANCA ELETTRONICA

(DECRETO 30 DICEMBRE 2020 /
DECRETO 1 DICEMBRE 2022
DECRETO 8 GIUGNO 2023)

VERSIONE 1.6 DEL 18 DICEMBRE 2023

INDICE

1. REVISIONI DEL DOCUMENTO

In base a ciò che viene modificato nel documento viene inserita la motivazione dell'aggiornamento, in modo che il lettore possa immediatamente sapere:

- se sono state variate le specifiche tecniche (AGGIORNAMENTO TECNICO) e, di conseguenza, deve variare il software affinchè sia funzionante (ad esempio cambiamenti nei tracciati record, nuovi valori di campi flag, etc.),
- se sono stati solamente meglio specificati alcuni argomenti già trattati nelle versioni precedenti (AGGIORNAMENTO CONCETTUALE), che non hanno però riflesso nella produzione del software (ad es. nuovo flusso del processo),
- se sono stati pubblicati nuovi servizi (AGGIORNAMENTO PER NUOVO SERVIZIO) non presenti nelle versioni precedenti e quindi da sviluppare.

DATA MODIFICA	DESCRIZIONE
28.06.2023	Prima versione del documento.
17.07.2023	Revisione documento sul flusso relativo all'autenticazione a 2 fattori tramite servizi WS.
04.08.2023	Aggiunti valori specifici per la modalità di autenticazione per il tag Assertion/AuthnStatement/AuthnContext/AuthnContextClassRef
25.08.2023	Aggiunti endpoints (TEST e PROD) per l'invocazione del WS
27.09.2023	Refusi e aggiornamenti su par. 2, 4.2, 4.3, 5.3. Aggiornamento dei periodi transitori su SAML Assertion (per le regioni/province) al par. 2. Aggiornamento sul rilassamento dei controlli sulla SAML Assertion (per le regioni/province).
29.09.2023	Aggiornamento delle modalità di fruizione dell'ID-SESSIONE al paragrafo 5.1 e 5.2.
27.11.2023	Rettifica o aggiunta dei paragrafi 5.4, 5.5 e 5.6 .
18.12.2023	Modifica paragrafo 5.2. e aggiunto paragrafo 5.2.1.

2. INTRODUZIONE

Il presente documento descrive la nuova modalità di accesso dei servizi della ricetta bianca elettronica, ovvero l'autenticazione a due o più fattori, stabilita dal Decreto MEF 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 piu' fattori.".

In particolare, tale modalità di accesso verrà applicata per:

- La trasmissione al Sistema TS da parte dei medici dei dati relativi alle prescrizioni su ricetta bianca elettronica.
- La trasmissione al Sistema TS da parte delle farmacie e parafarmacie dei dati relativi alle erogazioni di farmaci prescritti su ricetta bianca elettronica.

Le modalità sono diverse a seconda se l'inviante è un sistema regionale (SAR regionale), oppure il singolo utente che utilizza un software gestionale.

Nel caso dei SAR regionali:

Attivazione nuova modalità di autenticazione a 2 o più fattori: **05/07/2023**

Periodo transitorio, nel quale è ancora concesso l'utilizzo delle vecchie modalità di autenticazione: **dal 05/07/2023 al 05/10/2023**

Periodo transitorio, nel quale NON è concesso il mancato invio della SAML Assertion e su cui saranno effettuati controlli NON bloccanti: **dal 05/10/2023 al 30/12/2023**

Nel caso dei singoli utenti collegati al SAC che utilizzano un software gestionale:

Attivazione nuova modalità di autenticazione a 2 o più fattori: **30/09/2023**

Periodo transitorio, nel quale è ancora concesso l'utilizzo delle vecchie modalità di autenticazione: **dal 30/09/2023 al 30/12/2023**

Al termine dei rispettivi periodi transitori, le vecchie modalità di autenticazione saranno disattivate e sarà possibile utilizzare solo le nuove modalità a 2 o più fattori.

3. CANALI DI COMUNICAZIONE

L'invocazione dei servizi associati alla prescrizione ed erogazione delle ricette bianche elettroniche, può essere effettuata tramite:

- applicazione web del portale www.sistemats.it, trattata nel documento "Modalità di accesso all'area riservata operatore del portale Sistema TS", pubblicato sul portale del Sistema TS;

- servizi esposti da SistemaTS tramite modello Web Service e riportati in questo documento, fruibili attraverso il canale di comunicazione https.

L'autenticazione ai servizi web services può essere effettuata attraverso l'utilizzo della basic authentication (in aggiunta del pincode *cifrato* specifico dell'utenza rilasciato alla creazione dell'utenza da parte del Sistema TS); per la sua corretta impostazione è necessario forzare la basic authentication nell'header dell'http, pena il rifiuto dei web services da parte del sistema.

L'utilizzo della basic authentication (in unione al *pincode cifrato*) NON è sostituita ma evoluta verso l'autenticazione a 2 o più fattori, con le tempistiche descritte nel par. 2.

Rimangono valide quindi le attuali modalità di autenticazione (salvo SAR regionali) alle quali si aggiunge un altro livello di sicurezza, descritte nel par. 5 .

Di seguito vengono specificate le azioni da compiere da parte dei medici, farmacie e parafarmacie e dei Sistemi di Accoglienza Regionale (SAR) per l'utilizzo del web services per la prescrizione ed erogazione della ricetta bianca elettronica secondo quanto previsto dal DM 8 giugno 2023, art. 1 "Modifiche al decreto 30 dicembre 2020 e successive modificazioni", e dal Decreto 8 giugno 2023 il quale regola le modalità per l'accesso al Sistema TS mediante l'autenticazione a due o più fattori riportate nel Disciplinare tecnico, Allegato 2.

I web services inerenti la ricetta bianca dematerializzata, posso essere invocati in due modalità :

- da parte dei Sistemi di Accoglienza Regionali (SAR) collegati con il SAC al quale inviano le ricette dei medici della propria regione, e l'erogato derivante da una farmacia o parafarmacia della regione di appartenza. Come descritto nel par. 4, l'unica modalità di autenticazione ammessa è attraverso il certificato client di autenticazione.

- da parte di singoli medici/farmacie/parafarmacie i quali utilizzano un gestionale di mercato e che vengono collegati direttamente al Sistema TS (Sistema di Accoglienza Centrale – SAC) a valle di una procedura di autenticazione a 2

fattori della persona fisica collegata all'utenza interessata. I dettagli dell'autenticazione a 2 fattori è descritta nel par. 5.

4. SISTEMI DI ACCOGLIENZA REGIONALI (SAR) COLLEGATI AL SAC

I Sistemi di Accoglienza Regionale al fine di invocare i servizi della ricetta bianca elettronica esposti dal SAC, devono utilizzare esclusivamente un certificato client di autenticazione e un certificato di firma, predisposto per la firma delle asserzioni SAML.

Le tempistiche di adozione di questa modalità sono riportate nel par. 2.

In rinforzo all' autenticazione tramite certificato è prevista, infatti, l'integrazione del protocollo SAML (Security Assertion Markup Language), tecnicamente questo comporta l'aggiunta dell'asserzione SAML nell' header WS-Security delle chiamate SOAP verso il SAC.

Le caratteristiche dell'asserzione SAML sono riportate di seguito.

4.1 STANDARD DELL'ASSERZIONE

L'asserzione segue regole e nomenclature dei seguenti standard OASIS:

- SAML 2.0
- Profili XACML e XSPA

L'asserzione da realizzare è di tipo ***asserzione di attributo***.

Le pagine di riferimento per gli standard sono:
https://docs.oasis-open.org/security/saml/v2.0 (SAML 2.0)
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml (XACML)
https://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0.pdf (XSPA)

Nel prossimo paragrafo verrà specificato come creare una asserzione con i valori di interesse.

4.2 VALORIZZAZIONE DELL'ASSERZIONE

La valorizzazione mira ad essere riutilizzata anche in altri contesti, pertanto alcuni valori hanno senso in contesti diversi dalla ricetta dematerializzata (es. Partita Iva), le informazioni richieste nell'asserzione sono:

- Soggetto identificato (Codice Fiscale / Partita IVA / UserID)
- Regione o Ente che ha prodotto l'asserzione (Issuer) o che veicola la chiamata (per la ricetta dematerializzata bianca coincidono).
- Ora in cui l'utente si è autenticato

- Modalità di autenticazione
- Organizzazione per la quale opera l'utente

In particolare:

- ***Soggetto identificato*** va inserito in due tag, entrambi con il namespace di riferimento: xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" :

  a) tag Assertion/Subject/NameID
  b) Attributo con Name urn:oasis:names:tc:xacml:1.0:subject:subject-id

  Esempio, se l'utente identificato è AAABBB00A01H501R:

```
<saml2:Assertion>
        (…)
        <saml2:Subject>
        <saml2:NameID>AAABBB00A01H501R</saml2:NameID>
        </saml2:Subject>       (…)
        <saml2:Attribute Name="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
      NameFormat=(…)">
                        <saml2:AttributeValue (…) xsi:type=" xsd:string"
      xmlns:xsi="(…)">AAABBB00A01H501R</saml2:AttributeValue>
        </saml2:Attribute>
        (…)
</saml2:Assertion>
```

- ***Ente che produce l'asserzione*** va inserito nel tag Assertion/Issuer. Se l'ente che produce l'asserzione è una regione/provincia autonoma, va indicato il codice ISTAT relativo, se è una ASL, va indicato il codice ASL.

  Esempio:

```
<saml2:Assertion>
      <saml2:Issuer>120</saml2:Issuer>
      (…)
</saml2:Assertion>
```

- ***Ora in cui l'utente si è autenticato*** va inserito nell'attributo *urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:start*

  Il formato richiesto è dateTime, ovvero : YYYY-MM-DD**T**hh:mm:ss

```
<saml2:Assertion>
      (…)
      <saml2:Attribute
Name="urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:start" (…)>
            <saml2:AttributeValue(…)>2023-06-16T15:30:00</saml2:AttributeValue>
    </saml2:Attribute>
      (…)
</saml2:Assertion>
```

- ***Modalità di autenticazione*** va inserita nel tag Assertion/AuthnStatement/AuthnContext/AuthnContextClassRef

I valori possibili sono :

- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**SpidL1** (spid livello 1 – accettato in Ricetta Bianca SOLO nel periodo transitorio definito nel par. 2)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**SpidL2** (spid livello 2)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**SpidL3** (spid livello 3)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**Smartcard** (Accesso con Smartcard, CNS o CIE)

Questi valori sono già stati formalizzati in passato in altri contesti,è raccomandato quando possibile utilizzare nuovi valori più specifici, ovvero:

- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**CNS** (Accesso con carta nazionale dei servizi)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**CIEL2** (Accesso con CIE L2)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**CIEL3** (Accesso con CIE L3)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**FirmaQualificataL3** (Autenticazione Custom mediante processo con Firma Qualifica con LoA AAL3)

Di seguito dei valori accettati, in caso di autenticazioni custom da parte degli enti (ad uso quindi delle regioni o province) che assicurano però i vincoli dell'autenticazione forte secondo i LoA AAL1/ **AAL2**/ **AAL3**.

- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericL1** (accettato in Ricetta Bianca SOLO nel periodo transitorio definito nel par. 2)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericL2**
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericL3**

Un esempio di valorizzazione è il seguente :

```
<saml2:Assertion (…) >
  (…)
  <saml2:AuthnStatement AuthnInstant="2023-05-02T11:30:03.454Z">
    <saml2:AuthnContext>
                <saml2:AuthnContextClassRef>
                      urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2
                 </saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
   (…)
 </saml2:AuthnStatement>
```

- ***Organizzazione di riferimento*** va inserita nell'attributo urn:oasis:names:tc:xspa:1.0:subject:organization-id

  In particolare, si intende organizzazione di riferimento l'organizzazione che rappresenta tutti gli utenti che veicolano le richieste attraverso di essa. Nel caso di SAR per la ricetta Dematerializzata bianca va a coincidere con l'Issuer.

  Un esempio di valorizzazione dell'attributo è il seguente :

```
<saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id"  (…)>
    <saml2:AttributeValue (…) >120</saml2:AttributeValue>
</saml2:Attribute>
```

- ***L'organizzazione locale per cui opera l'utente autenticato*** va inserita nell'attributo urn:oasis:names:tc:xspa:1.0:environment:locality.

  In particolare se l'utente sta effettuando una operazione all'interno/per conto di una ASL, il campo deve essere valorizzato con la stringa codice regione Istat+Codice ASL .

  Un esempio di valorizzazione per la ASL 201 all'interno della regione Lazio è il seguente :

```
<saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:environment:locality" (…)>
    <saml2:AttributeValue  xsi:type="xs:string">120201</saml2:AttributeValue>
</saml2:Attribute>
```

4.3 ESEMPIO

Sulla base di quanto detto nel paragrafo 3, un esempio di struttura dell'asserzione (senza pretesa di firma corretta) è il seguente:

```
<saml2:Assertion ID="_ec59d9e35fbe3bede43e72d4a2e7136e" IssueInstant="2023-05-02T11:30:03.454Z" Version="2.0"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <saml2:Issuer>120</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
            <ds:Reference URI="#_ec59d9e35fbe3bede43e72d4a2e7136e">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
    signature"/>
                    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces PrefixList="xsd"
    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                <ds:DigestValue>O8Xd6BYc1cNbtqxorEEqvF2mqaYHEs2RT6SUgN3K0fc=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>

        <ds:SignatureValue>JbyyNQyKdXhI9ccFQ75kKCJGxNe3TSJGckmQXtUBADdyRBuPhEMa4Ld/8x1IW1Wf7crjoaFg8S
    emppU8/69cEvEcImaKYth2hmYBFjEQXM/H9hON66IYb+cLAc+UNgs8zmm3IXXrPzflenD4mrbS2wtuEu3+7d2Syv38a9X67t03b
    hHPkVSdzwICCSGwxeWmzjATd6gqEOpaLXLkMakN+QysAf9Cxbf8H3rdaX6sZWijU6hNDjHBRnwKYAUIswMrt56gcSaUz52YA
    lpYC+EGFfdWGmoNe4AjwNwYea/yXF62nCaUi+b5opwaUXnUHd1ohV4GymddVnqXJVrlbo//5w==</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>MIIC4jCCAcq….==</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
    <saml2:Subject>
        <saml2:NameID>AAABBB00B01H501K</saml2:NameID>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2023-05-02T10:30:03.362Z" NotOnOrAfter="2023-05-12T11:30:03.362Z"/>
    <saml2:AuthnStatement AuthnInstant="2023-05-02T11:30:03.454Z">
        <saml2:AuthnContext>

        <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2</saml2:AuthnContextClassRef>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
        <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id" NameFormat="(…)">
            <saml2:AttributeValue xsi:type="xsd:string" xmlns:xsi="(…)">120</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="urn:oasis:names:tc:xacml:1.0:subject:subject-id" NameFormat="(…)">
            <saml2:AttributeValue xsi:type="xsd:string"
    xmlns:xsi="(…)">AAABBB00A01H501R</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:resource:org:hoursofoperation:start" (…)>
            <saml2:AttributeValue xsi:type="xsd:dateTime" xmlns:xsi=(…)>2023-06-
    16T15:30:00</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name=" urn:oasis:names:tc:xspa:1.0:resource:patient:hl7:confidentiality-code " (…)>
            <saml2:AttributeValue xsi:type="xsd:string" xmlns:xsi=(…)>AAL2</saml2:AttributeValue>
        </saml2:Attribute>
        <saml2:Attribute Name="urn:oasis:names:tc:xspa:1.0:environment:locality" (…)>
            <saml2:AttributeValue xsi:type="xs:string">120201</saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

N.B. :

Nel SignatureMethod si fa riferimento a Sha256, lo Sha1 è considerato deprecato.

Per leggibilità si è omesso di specificare negli attributi:

- Il NameFormat, da valorizzare con urn:oasis:names:tc:SAML:2.0:attrname-format:uri
- Il valore di xmlns:xsi all'interno di "AttributeValue", da valorizzare con http://www.w3.org/2001/XMLSchema-instance

4.4 AUTENTICAZIONE DI TIPO CUSTOM

In caso di utilizzo di un sistema di autenticazione custom (es. FirmaQualificataL3, genericL1, genericL2, genericL3 etc), questo deve essere prima dichiarato e censito. Deve essere inoltre comunicato – sotto la assoluta responsabilità del dichiarante- il LoA che tale sistema garantisce.

Sono state introdotte le autorizzazioni custom "genericL**n**" come implementazioni specifiche LoA da parte delle regioni. Si ricorda che il LoA 1 non è attualmente accettato in Ricetta Bianca (accettato solo nel periodo transitoria definito al par. 2).

Lo schema che identifica i LoA è il seguente :

LoA 1 (AAL1): Autenticazione di tipo single-factor.
Accettato dalla ricetta bianca dematerializzata solo nel periodo transitoria definito al par. 2.
Esempio : username/password.

LoA 2 (**AAL2**): L'utente deve dimostrare di possedere il controllo di due diversi fattori di autenticazione.
Sono richieste tecniche crittografiche approvate e well-known.

LoA 3 (**AAL3**) : L'autenticazione deve basarsi sulla prova di possesso di una chiave utilizzata attraverso un protocollo crittografico. AAL3 è simile a AAL2 ma richiede un autenticatore crittografico che deve fornire adeguate garanzie per evitare che qualcuno possa impersonare il possessore della chiave. Tipicamente, una autenticazione tramite SmartCard soddisfa il livello AAL3.

5. UTENTI COLLEGATI AL SAC

Un utente del Sistema TS, sia esso medico o farmacia/parafarmacia in base ai servizi da invocare, utilizza le credenziali di accesso al Sistema TS già in uso, composte da identificativo utente, password e pincode, alle quali deve aggiungere un secondo fattore di autenticazione.

Il secondo fattore di autenticazione viene definito come **ID di sessione del Sistema TS**, da qui in avanti denominato anche come "ID-SESSIONE", ed è costituito da un identificativo alfanumerico generato dal Sistema TS valido dal momento della richiesta per almeno 8 ore. Il valore esatto di validità del token sarà eventualmente modificato in futuri aggiornamenti della specifica o nel kit di sviluppo pubblicato sul Portale TS.

L'utente prescrittore (medico) o utente erogatore (farmacia/parafarmacia) può richiedere l'ID di sessione del SistemaTS in due modalità:

- tramite applicazione web del Sistema TS
- tramite web service integrato nel proprio gestionale di mercato

Le tempistiche di adozione di questa modalità sono riportate nel par. 2.

5.1 RICHIESTA ID-SESSIONE DEL SISTEMA TS TRAMITE APPLICAZIONE WEB

PREREQUISITO: l'utente è dotato di identità digitale SPID/CIE/TS-CNS.

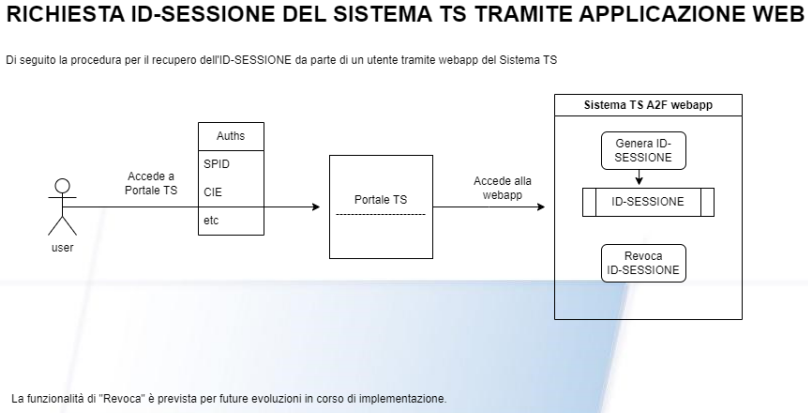
L'utente del Sistema TS si collega al portale www.sistemats.it, si autentica con SPID, CIE oppure TS-CNS, quindi clicca sulla voce di menu "Sicurezza" e attraverso la funzionalità "Gestione ID-SESSIONE" chiede la generazione dell'ID-SESSIONE del Sistema TS che viene restituito in un'apposita schermata.

La funzionalità "Gestione ID-SESSIONE" permette oltre alla generazione dell'ID di sessione, anche la visualizzazione e la revoca.

Tale ID di sessione del Sistema TS deve essere inserito, a cura del medico per i servizi lato prescrittore, o dalla farmacia/parafarmacia per i servizi lato erogatore, in un apposito campo predisposto da ciascun gestionale di mercato, secondo le istruzioni fornite all'utilizzatore.

Tutto ciò si traduce tecnicamente, nell'invio da parte del gestionale di mercato dell' ID di sessione, per ciascuna chiamata al Sistema TS, secondo le modalità indicate nel par. 5.3.

Di seguito il diagramma descrittivo:



5.2 RICHIESTA ID-SESSIONE DEL SISTEMATS TRAMITE GESTIONALE DI MERCATO

PREREQUISITO: l'utente è dotato di identità digitale e deve preventivamente accedere alla propria area autenticata del portale Sistema TS con SPID/CIE/TS-CNS per certificare la propria email (vedi paragrafo 5.2.1).

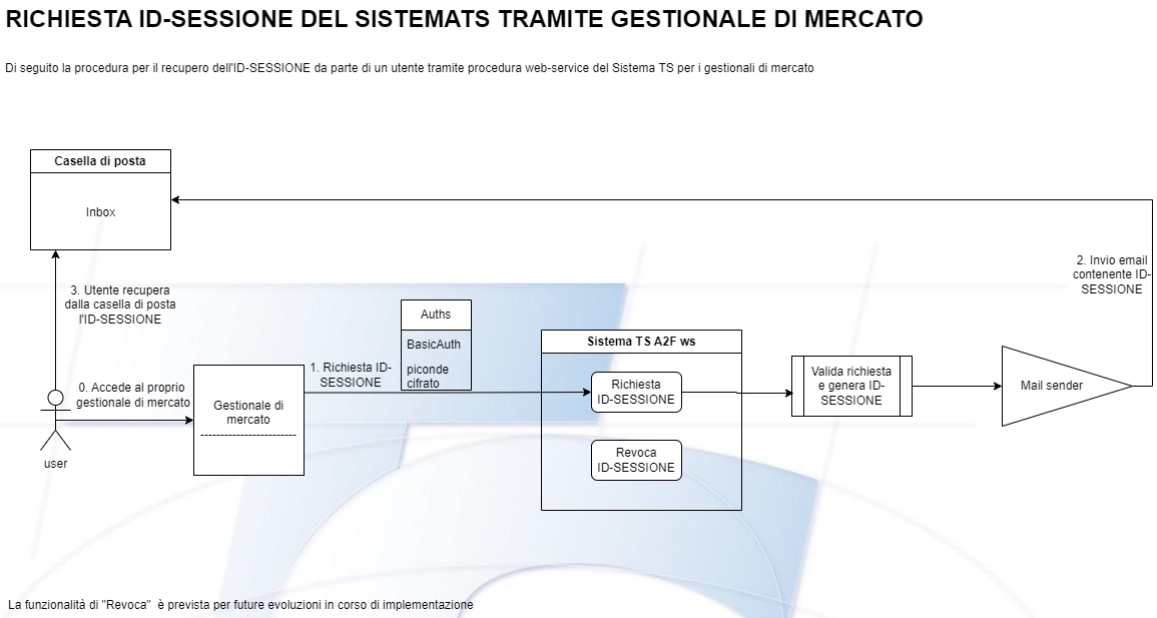
L'utente del Sistema TS, attraverso un'apposita funzionalità web service messa a disposizione dal proprio gestionale di mercato, esegue la richiesta secondo le specifiche tecniche descritte nel par. 5.4 per l'invocazione del servizio web service per la generazione (ed invio) dell' "ID-SESSIONE" da parte del SistemaTS.

La richiesta dell'utente genera una mail con l'identificativo alfanumerico "**ID-SESSIONE**", che il Sistema TS invia all'indirizzo di posta elettronica che il medico/farmacista/parafarmacista ha certificato precedentemente (vedi paragrafo 5.2.1).

L' "ID-SESSIONE" ha un periodo di validità descritto nel par. 5 e specificato anche nella mail ricevuta in cui è contenuto. Una volta scaduto risulterà inutilizzabile e sarà possibile effettuare una nuova richiesta.

L' "ID-SESSIONE" recuperato dalla mail ricevuta dall'utente utilizzatore deve essere inserito in un apposito campo, predisposto da ciascun gestionale di mercato e inviato dallo stesso gestionale di mercato del medico/farmacista/parafarmacista ai web services della Ricetta Bianca, secondo le modalità indicate nel par. 5.3.

Di seguito il diagramma descrittivo:



5.2.1 CERTIFICAZIONE MAIL

L'utente prescrittore (medico) o utente erogatore (farmacia/parafarmacia) deve certificare la casella di posta elettronica per ricevere l'ID-SESSIONE richiesto tramite il gestionale di mercato.

Di seguito viene descritta nel dettaglio la procedura:

1. Autenticarsi su Sistema TS con SPID, CIE o TS-CNS;
2. Dalla pagina "Servizi on line" scegliere la voce "**Sicurezza**" nel menù a sinistra;
3. Cliccare il link "**Certifica mail**";
4. Seguire le indicazioni riportate nella pagina inserendo **l'indirizzo email** che si vuole certificare e confermare;
5. Sulla nuova schermata inserire il "**codice validazione**" ricevuto sulla casella di posta indicata al punto precedente e confermare. Nel caso la mail non risulti ricevuta, controllare anche la cartella spam o la posta indesiderata;

6. Nel caso non si sia ricevuta nessuna mail è possibile da questa stessa pagina **richiedere nuovo codice validazione** cliccando sull'apposito bottone;

7. L'indirizzo email sarà **certificato** quando viene visualizzato il messaggio "La mail è stata validata e registrata con successo".

8. A questo punto dalla stessa applicazione si può modificare o revocare la casella di posta tramite i bottoni "**modifica**" e "**revoca**" seguendo le indicazioni riportate nella pagina "Gestione mail certificata".

5.3 UTILIZZO DELL' ID-SESSIONE DEL SISTEMATS

L' ID-SESSIONE del Sistema TS va inviato dai software gestionali in ogni transazione verso i servizi della ricetta bianca, inserendolo nello specifico campo dell'header Http "Authorization2F" secondo l' Auth Schema "**Bearer authentication**".

Di seguito un esempio:

Authorization2F: Bearer <ID-SESSIONE>

In ambiente di TEST, al fine di testare la funzionalità o eseguire le classiche operazioni di integrazione senza aver a disposizione la possibilità di ricevere l' ID-SESSIONE, sarà possibile invocare i servizi inviando come ID-SESSIONE una stringa wildcard avente la seguente nomenclatura (che quindi varierà ogni mese):

UTENZA-YYYY-MM

Esempio: ID-SESSIONE= **AAABBB00B01H501K-2023-09**

5.4 SERVIZIO (WEB SERVICE) PER LA RICHIESTA DELL' ID-SESSIONE DEL SISTEMATS

La richiesta dell'invio dell' ID-SESSIONE attraverso canale web services è assicurato dal Sistema TS attraverso l'invocazione dell'operation "create" del web service descritto di seguito.

Il gestionale di mercato richiama il servizio di richiesta dell' ID-SESSIONE che deve essere eseguito solamente all'inizio della sessione lavorativa (tipicamente una volta al giorno ed in base alla durata descritta al par. 5), secondo le specifiche del tracciato descritto nel prossimo paragrafo.

5.4.1 AUTENTICAZIONE, GENERAZIONE ED INVIO DELL' ID-SESSIONE

Di seguito i parametri da inoltrare al servizio per la generazione ed invio dell'ID-SESSIONE, al quale è possibile accedere secondo le stesse modalità di autenticazione dei servizi della Ricetta Bianca (Basic authentication + pincode cifrato).

Il tracciato WSDL è pubblicato sul Portale TS dove è possibile scaricare l'ulitma versione aggiornata (cap. 6).

Nome campo	Descrizione	Caratteristiche
pinCode	Codice PIN in possesso del soggetto abilitato all'invio. Tale campo deve essere inserito criptato tramite l'utilizzo del certificato SanitelCF.cer.	Elemento obbligatorio
cfUtente	In base alla richiesta specifica può essere valorizzato con codice fiscale del medico o del titolare dell'erogatore.	Elemento obbligatorio
codRegione	Codice Regione / Provincia Autonoma di appartenenza del soggetto indicato in userId.	Elemento obbligatorio
codAslAo	Codice ASL di appartenenza del soggetto indicato in userId.	Elemento obbligatorio
codiceStruttura	Codice della struttura di appartenenza del soggetto indicato in userId. Nel caso in cui il codice struttura non sia presente è necessario valorizzare con un a stringa di lunghezza 0.	Elemento obbligatorio

Il servizio che risponde con esito positivo, genera l'ID-SESSIONE e viene inviato all'indirizzo email certificata dell'utente.

In caso di errore viene fornito un messaggio diagnostico.

Endpoint di test:
https://ricettabiancaservicetest.sanita.finanze.it/sts-a2f-auth-ws/soap/v1/authentication-service

Endpoint di produzione:

https://ricettabiancaservice.sanita.finanze.it/sts-a2f-auth-ws/soap/v1/authentication-service

5.5 SERVIZIO (WEB SERVICE) PER LA RICHIESTA DI REVOCA DELL' ID-SESSIONE DEL SISTEMATS

La richiesta di revoca dell' ID-SESSIONE attraverso canale web services è assicurato dal Sistema TS attraverso l'invocazione dell'operation "revoke" del web service descritto di seguito.

Il gestionale di mercato richiama il servizio di richiesta di revoca dell' ID-SESSIONE precedentemente generato (par. 5.4), secondo le specifiche del tracciato descritto nel prossimo paragrafo.

5.5.1 AUTENTICAZIONE E REVOCA DELL' ID-SESSIONE

Di seguito i parametri da inoltrare al servizio per la revoca dell'ID-SESSIONE, al quale è possibile accedere secondo le stesse modalità di autenticazione dei servizi della Ricetta Bianca (Basic authentication + pincode cifrato).

Il tracciato WSDL è pubblicato sul Portale TS dove è possibile scaricare l'ulitma versione aggiornata (cap. 6).

Nome campo	Descrizione	Caratteristiche
pinCode	Codice PIN in possesso del soggetto abilitato all'invio. Tale campo deve essere inserito criptato tramite l'utilizzo del certificato SanitelCF.cer.	Elemento obbligatorio
cfUtente	In base alla richiesta specifica può essere valorizzato con codice fiscale del medico o del titolare dell'erogatore.	Elemento obbligatorio
codRegione	Codice Regione / Provincia Autonoma di appartenenza del soggetto indicato in userId.	Elemento obbligatorio
codAslAo	Codice ASL di appartenenza del soggetto indicato in userId.	Elemento obbligatorio
codiceStruttura	Codice della struttura di appartenenza del soggetto indicato in userId. Nel caso in cui il codice struttura non sia presente è necessario valorizzare con un a stringa di lunghezza 0.	Elemento obbligatorio

Nome campo	Descrizione	Caratteristiche
token	ID-SESSIONE da revocare	Elemento obbligatorio

Il servizio che risponde con esito positivo, revoca l'ID-SESSIONE indicato in request.

In caso di errore viene fornito un messaggio diagnostico.

Endpoint di test:
https://ricettabiancaservicetest.sanita.finanze.it/sts-a2f-auth-ws/soap/v1/authentication-service

Endpoint di produzione:
https://ricettabiancaservice.sanita.finanze.it/sts-a2f-auth-ws/soap/v1/authentication-service

5.6 SERVIZIO (WEB SERVICE) PER LA RICHIESTA DI VERIFICA/INFO DELL' ID-SESSIONE DEL SISTEMATS

La richiesta di verifica dell' ID-SESSIONE attraverso canale web services è assicurato dal Sistema TS attraverso l'invocazione dell'operation "checkToken" del web service descritto di seguito.

Il gestionale di mercato richiama il servizio di richiesta di verifica dell' ID-SESSIONE precedentemente generato (par. 5.4), secondo le specifiche del tracciato descritto nel prossimo paragrafo.

5.6.1 AUTENTICAZIONE E VERIFICA DELL' ID-SESSIONE

Di seguito i parametri da inoltrare al servizio per la verifica dell'ID-SESSIONE, al quale è possibile accedere secondo le stesse modalità di autenticazione dei servizi della Ricetta Bianca (Basic authentication + pincode cifrato).

Il tracciato WSDL è pubblicato sul Portale TS dove è possibile scaricare l'ulitma versione aggiornata (cap. 6).

Nome campo	Descrizione	Caratteristiche
pinCode	Codice PIN in possesso del soggetto abilitato all'invio. Tale campo deve essere inserito criptato tramite l'utilizzo del certificato SanitelCF.cer.	Elemento obbligatorio
cfUtente	In base alla richiesta specifica può essere valorizzato con codice fiscale del medico o del titolare dell'erogatore.	Elemento obbligatorio
codRegione	Codice Regione / Provincia Autonoma di appartenenza del soggetto indicato in userId.	Elemento obbligatorio
codAslAo	Codice ASL di appartenenza del soggetto indicato in userId.	Elemento obbligatorio
codiceStruttura	Codice della struttura di appartenenza del soggetto indicato in userId. Nel caso in cui il codice struttura non sia presente è necessario valorizzare con un a stringa di lunghezza 0.	Elemento obbligatorio

Nome campo	Descrizione	Caratteristiche
token	ID-SESSIONE da verificare	Elemento obbligatorio

Il servizio che risponde con esito positivo, riporta le informazioni dell'ID-SESSIONE indicato in request.

In caso di errore viene fornito un messaggio diagnostico.

Endpoint di test:
https://ricettabiancaservicetest.sanita.finanze.it/sts-a2f-auth-ws/soap/v1/authentication-service

Endpoint di produzione:
https://ricettabiancaservice.sanita.finanze.it/sts-a2f-auth-ws/soap/v1/authentication-service

6. SPECIFICHE TECNICHE

Gli schemi xsd e i wsdl relativi ai servizi descritti in precedenza sono pubblicati nel portale https://sistemats1.sanita.finanze.it/portale/ nel relativo Kit di sviluppo recuperabile sul seguente percorso:

Home - Il Sistema TS - Ricette elettroniche - Ricetta NON a carico SSN - Documenti e specifiche tecniche