federfarma
FEDERAZIONE NAZIONALE UNITARIA TITOLARI DI FARMACIE

Roma, 19 gennaio 2026
Uff.-Prot. n° PROMO/715/19/F7/PE
Oggetto: **DM 27 febbraio 2025.** Estensione dell'autenticazione a due o più fattori alle funzionalità della ricetta dematerializzata a carico del Servizio sanitario nazionale

ALLE ASSOCIAZIONI PROVINCIALI
ALLE UNIONI REGIONALI
ALLE SOFTWARE HOUSE

SOMMARIO:
Dal 31 gennaio 2026 sarà operativa, in via esclusiva, l'autenticazione a due o più fattori per accedere alle funzionalità della ricetta dematerializzata a carico del Servizio sanitario nazionale. Nella presente circolare vengono confermate le indicazioni operative per le farmacie delle regioni SAC. Le farmacie delle regioni SAR devono seguire le indicazioni dei propri Sistemi di Accoglienza Regionali e delle proprie Software House.

PRECEDENTI:

Circolari Federfarma prot. n. 15636/395 del 14/11/2025, *n.101 del 24/03/2025, n.47 del 26/1/2024, n. 26 del 12/01/2024, n. 582 del 29/12/2023, n. 572 del 22/12/2023, n. 440 del 29/09/2023, n. 302 del 6/07/2023, n. 64 del 01/02/2021*.

Federfarma ricorda che sulla Gazzetta Ufficiale Serie Generale n.57 del 10-03-2025 è stato pubblicato il Decreto ministeriale 27 febbraio 2025, adottato dal Ministero dell'Economia e delle finanze, di concerto con il Ministero della salute, recante "***Estensione dell'autenticazione a due o più fattori alle funzionalità della ricetta dematerializzata a carico del Servizio sanitario nazionale***".

Tale decreto stabilisce che **l'accesso alle funzionalità della ricetta elettronica a carico del Servizio sanitario nazionale** avviene mediante l'autenticazione a due o più fattori ***secondo le modalità già previste per la ricetta dematerializzata "bianca"***, di cui al decreto ministeriale 30 dicembre 2020 del Ministero dell'economia e delle finanze, di concerto con il Ministero della salute.

Ad oggi, anche a seguito della pubblicazione di nuove specifiche tecniche (in allegato), si conferma che ***dal 31 gennaio 2026*** tale accesso potrà avvenire esclusivamente tramite autenticazione a 2 o più fattori e che **per le farmacie delle Regioni SAC**, tale autenticazione "forte" avverrà nelle **stesse modalità utilizzate per la ricetta dematerializzata "bianca",** che prevedono, **come prima fase del processo, la certificazione di un indirizzo di posta elettronica ordinaria come di seguito specificato**.

FEDERFARMA
Via Emanuele Filiberto, 190
I – 00185 Roma (RM)
+06 70380.1
box@federfarma.it
c.f. 01976520583
www.federfarma.it

La documentazione tecnica, allegata per comodità di lettura, è reperibile al link https://sistemats1.sanita.finanze.it/portale/documents/d/guest/modalita_autenticazione_ws_2fattori_v1-1-20260112.

Più specificamente, in tale documento sono riportati i dettagli tecnici per l'accesso diretto al portale TS e attraverso i gestionali, unitamente ai **prerequisiti per poter operare con autenticazione a due o più fattori** come riportati, in dettaglio, di seguito.

L'Utente (Titolare di farmacia o Direttore) deve essere già dotato di Identità Digitale (SPID, CIE, TS-CNS, altri sistemi utilizzati localmente dai SAR).

Tale Utente **deve certificare un solo indirizzo e-mail per sede farmaceutica**, accedendo preventivamente alla propria area riservata del portale Sistema TS con SPID/CIE/TS-CNS (si raccomanda, per facilità di accesso e lettura, di **creare una casella di posta elettronica ordinaria, NON PEC, da dedicare esclusivamente a questa attività**).

Di seguito viene descritta, nel dettaglio, la procedura di certificazione della e-mail:

1. Autenticarsi su Sistema TS con SPID, CIE o TS-CNS (livello minimo di sicurezza LoA3): https://sistemats1.sanita.finanze.it/portale/area-riservata-operatore;
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 e-mail** 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 e-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 e-mail 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"

Si ricorda che questa procedura di validazione dell'indirizzo di posta elettronica **deve essere eseguita una sola volta per sede farmaceutica e serve unicamente per indicare l'indirizzo di posta elettronica dove ricevere automaticamente l'ID SESSIONE,** ossia il codice da inserire nell'apposito campo del gestionale, come da istruzioni della Software House. Da quel momento la farmacia potrà erogare entrambe le tipologie di ricette elettroniche fino alla scadenza dello stesso ID SESSIONE (circa 16 ore), al termine della quale, tramite gestionale, verrà richiesto un nuovo ID SESSIONE.

Per quanto riguarda le Regioni SAR, si invitano le farmacie a seguire le indicazioni dei propri Sistemi di Accoglienza Regionali e delle proprie Software House, le quali hanno prodotto e costantemente rilasciano i necessari adeguamenti tecnici dei propri gestionali, nonché la relativa documentazione di supporto, per consentire alle farmacie di eseguire agevolmente le procedure di accesso e di gestione dell'ID SESSIONE.

Si ribadisce, inoltre, che **NON occorre certificare un secondo indirizzo e-mail** e che **tale procedura riguarda entrambe le ricette elettroniche prescriventi farmaci, a carico e NON, del Servizio sanitario nazionale.**

Si consiglia fortemente di accedere **da subito al Sistema Tessera Sanitaria (TS) secondo la nuova modalità (autenticazione a 2 o più fattori tramite ID SESSIONE), senza attendere la**

scadenza del 31 gennaio 2026, in modo tale da verificare, senza urgenza, il corretto funzionamento della nuova procedura.

Per **l'assistenza sul Sistema TS**, Sogei mette a disposizione **il numero verde 800.030.070.**

Cordiali saluti.

IL SEGRETARIO
Dott. Michele PELLEGRINI CALACE

IL PRESIDENTE
Dott. Marco COSSOLO

All. n.1

SISTEMA TESSERA SANITARIA

MODALITA' DI ACCESSO TRAMITE AUTENTICAZIONE FORTE AI SERVIZI (WEB SERVICES) DEL SISTEMA TESSERA SANITARIA

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

VERSIONE 1.1 DEL 12 GENNAIO 2026

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 affinché 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.

VERSIONE	DATA MODIFICA	DESCRIZIONE
1.0	20.04.2025	Prima versione del documento.
1.1	12.01.2026	Introdotta la gestione del ciclo di vita dell'ID-SESSIONE (Capitolo 5).

2. INTRODUZIONE

Il presente documento descrive la nuova modalità di accesso ai servizi esposti dal Sistema TS, ovvero l'autenticazione a 2 o più fattori, stabilita dal Decreto MEF 8 giugno 2023 – "Modifica al decreto 30 dicembre 2020, concernente l'adozione delle modalità di accesso al Sistema TS mediante l'autenticazione a 2 o più fattori.".

L'applicazione di tale modalità di accesso viene attivata secondo i cronoprogrammi definiti dalle amministrazioni di riferimento.

La modalità di accesso tramite autenticazione forte può essere realizzata in due modi diversi:

1. Attraverso un apposito servizio di Sistema TS per la richiesta di un token che autorizza l'accesso ai servizi per i quali è stato richiesto.
2. Direttamente dai sistemi periferici. In questo caso, chi ha autenticato l'utente dovrà inviare, nell' header WS-Security delle chiamate SOAP, anche un'asserzione SAML firmata che garantisca lo svolgimento dell'autenticazione secondo criteri adeguati. In questo caso è necessario anche un certificato di firma da richiedersi al Sistema TS (regioni, asl, enti ecc...).

3. CANALI DI COMUNICAZIONE

L'invocazione dei diversi servizi esposti dal portale Sistema TS, 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 dal Sistema TS tramite modello Web Service fruibili attraverso il canale di comunicazione https.

L'autenticazione ai servizi web services di Sistema TS viene integrata con l'utilizzo di un secondo fattore di tipo OTP/Token di sessione, che si aggiunge alle modalità attuali (es.: basic authentication, pin cifrato ed eventualmente altre specifiche credenziali associate al servizio invocato). Tale OTP/Token deve essere inviato nell'header http in ogni transazione per la quale si richiede l'accesso (vedi par. 5).

Se l'autenticazione dell'utente finale non è fisicamente svolta da Sistema TS, nelle chiamate ai servizi web è necessario inserire un asserzione SAML che descriva i dettagli opportuni (es. modalità) del processo di identificazione (vedi par. 4) .

4. SPECIFICHE DELL'ASSERZIONE SAML

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 in diversi contesti, pertanto, alcuni valori hanno senso in alcuni contesti e in altri meno.
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.
- 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.

Esempio:

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

Esempio asl:

```
<saml2:Assertion>
    <saml2:Issuer>120201</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-DDThh: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>
```

- ***Livello di autenticazione*** va inserito nel tag

  `Assertion/AuthnStatement/AuthnContext/AuthnContextClassRef`

  Il valore da inserire, che descrive il livello di autenticazione effettuato coerentemente con il livello LoA (Level of Assurance) definito dalla specifica *ISO/IEC 29115*, dovrebbe essere scelto tra i seguenti:

  - urn:oasis:names:tc:SAML:2.0:ac:classes:**iso-iec-29115-LoA1**
  - urn:oasis:names:tc:SAML:2.0:ac:classes:**iso-iec-29115-LoA2**
  - urn:oasis:names:tc:SAML:2.0:ac:classes:**iso-iec-29115-LoA3**
  - urn:oasis:names:tc:SAML:2.0:ac:classes:**iso-iec-29115-LoA4**

  Per motivi di retrocompatibilità, in specifici contesti (es. ricetta bianca dematerializzata) è possibile utilizzare anche i seguenti valori che rappresentano la modalità di autenticazione piuttosto che il livello, ovvero:

  - ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**SpidL1** (spid livello 1)
  - ✓ 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)
  - ✓ 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)

  Sempre per motivi di retrocompatibilità in specifici contesti, di seguito si elencano i valori accettati in caso di autenticazioni di tipo custom da parte degli enti (ad uso quindi delle regioni o province).

  - ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA1**
  - ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA2**
  - ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA3**

  Se si utilizzano questi tre valori, è richiesta la corrispondenza del tipo di autorizzazione con il livello LoA superiore in termini di specifica ISO/IEC 29115 (es. genericLoA3 → Iso LoA4).

  Si osservi che i livelli di CIE e SPID non sono necessariamente congruenti con quelli ISO/IEC (es. SpidL3 → LoA4). Si osservi anche che non necessariamente un metodo di autenticazione individua senza ulteriori informazioni un LoA univoco (ad es. alcune CNS con chiavi deboli possono essere ricondotte al LoA3, mentre quelle con chiavi robuste al LoA4).

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:iso-iec-29115-LoA4
                 </saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  (…)
</saml2:AuthnStatement>
```

Modalità di autenticazione: da inserire nel tag

`Assertion/AuthnStatement/AuthnContext/AuthnContextDeclRef`

Rappresenta la modalità tramite la quale si è autenticato l'utente.
E' possibile utilizzare i seguenti valori:

- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**SpidL1** (spid livello 1)
- ✓ 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)
- ✓ 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:**FirmaQualificataL4** (Autenticazione Custom mediante processo con Firma Qualifica con LoA AAL4 secondo la ISO/IEC 29115)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA1** (Metodo di autenticazione custom con LoA1 secondo la ISO/IEC 29115)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA2**(Metodo di autenticazione custom con LoA1 secondo la ISO/IEC 29115)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA3**(Metodo di autenticazione custom con LoA1 secondo la ISO/IEC 29115)
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA4**(Metodo di autenticazione custom con LoA1 secondo la ISO/IEC 29115)

Si osservi che i livelli di CIE e SPID non sono necessariamente congruenti con quelli ISO/IEC (es. SpidL3 → LoA4).

Se esistono più valori compatibili va utilizzato il più preciso. In caso di Smartcard/CNS ad esempio, se l'accesso è con CNS, utilizzare

`urn:oasis:names:tc:SAML:2.0:ac:classes:CNS`

Esempi di valorizzazione:

Nel caso di CNS con LoA3, un esempio di valorizzazione è il seguente:

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:iso-iec-29115-LoA3
  </saml:AuthnContextClassRef>
  <saml:AuthnContextDeclRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:CNS
  </saml:AuthnContextDeclRef>
</saml:AuthnContext>
```

Nel caso di CNS con LoA4, un esempio di valorizzazione è il seguente:

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:iso-iec-29115-LoA4
  </saml:AuthnContextClassRef>
  <saml:AuthnContextDeclRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:CNS
  </saml:AuthnContextDeclRef>
</saml:AuthnContext>
```

Nel caso di Spid Livello 2 (2FA), corrispondente a LoA3, un esempio di valorizzazione è il seguente:

```
<saml:AuthnContext>
  <saml:AuthnContextClassRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:iso-iec-29115-LoA3
  </saml:AuthnContextClassRef>
  <saml:AuthnContextDeclRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2
  </saml:AuthnContextDeclRef>
</saml:AuthnContext>
```

- ***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.

Ad esempio, nel caso di SAR, 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

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
    IpYC+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>
            <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:iso-iec-29115-LoA3
            </saml:AuthnContextClassRef>
            <saml:AuthnContextDeclRef>urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2
            </saml:AuthnContextDeclRef>
        </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 questo, sotto la responsabilità del dichiarante, deve soddisfare tutti i requisiti del LoA associato in termini di ISO/IEC 29115 e dichiarato nel campo `AuthnContextClassRef`.

In altri termini, se il campo "`AuthnContextClassRef`" è popolato con uno dei seguenti valori:

- urn:oasis:names:tc:SAML:2.0:ac:classes:**iso-iec-29115-LoA1**
- urn:oasis:names:tc:SAML:2.0:ac:classes:**iso-iec-29115-LoA2**
- urn:oasis:names:tc:SAML:2.0:ac:classes:**iso-iec-29115-LoA3**
- urn:oasis:names:tc:SAML:2.0:ac:classes:**iso-iec-29115-LoA4**

e il campo "`AuthnContextDeclRef`" è popolato con uno dei seguenti valori:

- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA1**
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA2**
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA3**
- ✓ urn:oasis:names:tc:SAML:2.0:ac:classes:**genericLoA4**

Questi devono essere corrispondenti
(es.

`urn:oasis:names:tc:SAML:2.0:ac:classes:iso-iec-29115-LoA3`
e
`urn:oasis:names:tc:SAML:2.0:ac:classes:genericLoA3`

)

ed è responsabilità di chi effettua l'autenticazione garantire che siano rispettate le condizioni per garantire il LoA dichiarato.

5. AUTENTICAZIONE ATTRAVERSO SERVIZIO DI RICHIESTA TOKEN

Un utente del Sistema TS, in base ai servizi da invocare, utilizza le credenziali di accesso già in suo possesso composte da identificativo utente e password. A seconda della tipologia di utente e della natura del servizio da invocare, possono essere richieste altre informazioni che concorrono all'identificazione dell'utente come ad esempio pincode e/o nickname per i medici oppure un determinato identificativo come il codice inviante per alcuni servizi del 730. Oltre alle suddette informazioni l'utente 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 e valido dal momento della richiesta per un tempo dipenderà dal *contesto/applicazione* per cui il token viene generato. Queste peculiarità vengono specificate dalle applicazioni che espongono i servizi da richiamare sul Sistema TS le quali forniscono, per un determinato *contesto/applicazione,* i parametri necessari alla configurazione della chiamata al servizio per la restituzione del token. Le specifiche tecniche del servizio per la generazione e gestione del token sono contenute nel kit di sviluppo pubblicato sul Portale TS.

Gli utenti possono richiedere l'ID di sessione del Sistema TS in due modalità:

- tramite applicazione web del Sistema TS
- tramite web service attraverso apposita richiesta di un client

Il ciclo di vita dell'ID-SESSIONE è definito dalla sua durata e dallo stato in cui si trova.

Nel momento della richiesta di un ID-SESSIONE questo si trova in stato *Validato* che significa pronto ad essere utilizzato. Al primo utilizzo dell'ID-SESSIONE lo stato diventa *Attivo* e l'ID-SESSIONE potrà essere utilizzato fino alla sua naturale scadenza.

Quando si è in possesso di un ID-SESSIONE in stato *Attivo* è possibile richiedere anticipatamente un nuovo ID-SESSIONE (stato *Validato*) che non andrà a revocare in automatico il precedente in stato *Attivo*. Questa caratteristica consente di ottenere un ID-SESSIONE aggiuntivo rispetto a quello attualmente in uso che potrà essere utilizzato fino alla sua naturale scadenza garantendo la continuità lavorativa.

È bene non richiedere con troppo anticipo un secondo ID-SESSIONE, soprattutto se si tratta di un ID-SESSIONE che ha una lunga la durata. La durata di un ID-

SESSIONE parte dal momento in cui è stato richiesto e se questa richiesta è stata fatta con troppo anticipo, il secondo ID-SESSIONE potrebbe avere un tempo di utilizzo estremamente limitato rispetto alla sua normale durata.

Non sarà mai possibile utilizzare contemporaneamente gli eventuali due ID-SESSIONE in possesso dell'utente. Infatti, al primo utilizzo del nuovo ID-SESSIONE in stato *Validato*, se il precedente ID-SESSIONE in stato *Attivo* non è ancora scaduto, questo sarà revocato implicitamente e di conseguenza non potrà essere più utilizzato.

È importante notare che è possibile avere un massimo di due ID-SESSIONI validi allo stesso momento: il primo in stato *Attivo* e il secondo in stato *Validato*. In questo caso, infatti, ulteriori richieste di un ID-SESSIONE invaliderebbero il precedente in stato *Validato* riportando la situazione a due ID-SESSIONE per utente (il primo *Attivo* e l'ultimo richiesto in stato *Validato*).

Tuttavia, l'unico utilizzabile in un dato momento è solo quello nello stato *Attivo*.

5.1 RICHIESTA ID-SESSIONE DEL SISTEMA TS TRAMITE APPLICAZIONE WEB

PREREQUISITO: l'utente è dotato di credenziali con livello minimo LoA3.

L'utente del Sistema TS si collega al portale www.sistemats.it autenticandosi con credenziali di livello minimo LoA3, quindi clicca sulla voce di menu "Sicurezza" e attraverso la funzionalità "Gestione ID-SESSIONE" chiede la generazione dell' ID-SESSIONE del Sistema TS per un determinato contesto e applicazione il quale viene restituito in un'apposita schermata.

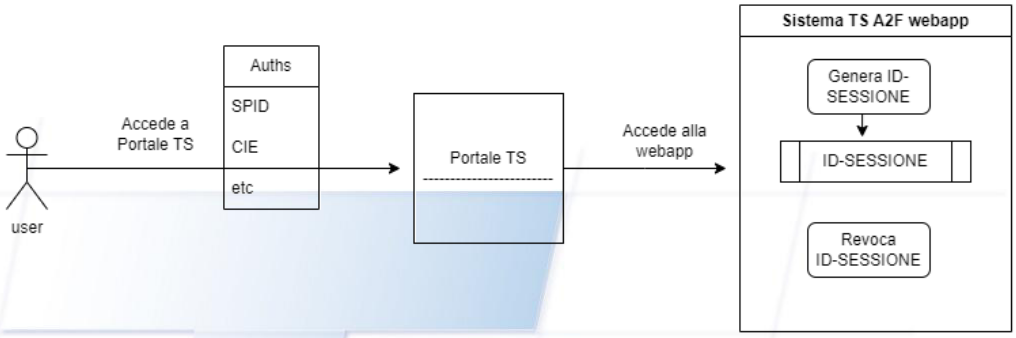
La funzionalità "Gestione ID-SESSIONE" permette, oltre alla generazione dell'ID di sessione, anche la sua visualizzazione e la revoca.

L' ID-SESSIONE dovrà dunque essere inserito nell' HEADER della richiesta HTTP del client per ciascuna chiamata ai servizi del Sistema TS secondo le modalità indicate nel par. 5.3.

Di seguito il diagramma descrittivo:

RICHIESTA ID-SESSIONE DEL SISTEMA TS TRAMITE APPLICAZIONE WEB

Di seguito la procedura per il recupero dell'ID-SESSIONE da parte di un utente tramite webapp del Sistema TS



5.2 RICHIESTA ID-SESSIONE DEL SISTEMA TS TRAMITE CLIENT

PREREQUISITO: l'utente è dotato di identità digitale e deve preventivamente accedere alla propria area autenticata del portale Sistema TS con un livello minimo di sicurezza LoA3 per certificare la propria email (vedi paragrafo 5.2.1).

L'utente del Sistema TS, esegue un richiesta client secondo le specifiche tecniche descritte nel par. 5.4 per l'invocazione web service per la generazione (ed invio) dell' ID-SESSIONE da parte del Sistema TS.

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

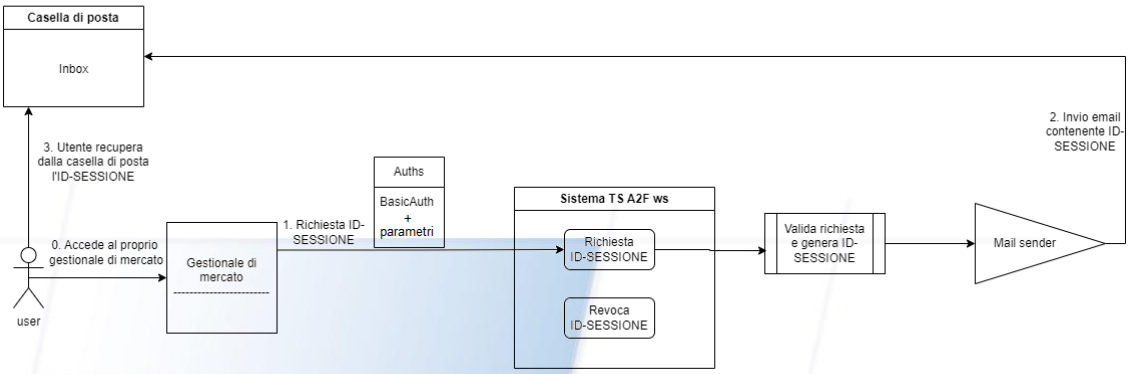
L' ID-SESSIONE avrà un periodo di validità descritto nel par. 5 e specificato anche nella mail ricevuta in cui è contenuto. Una volta scaduto risulterà inutilizzabile e sarà possibile effettuare una nuova richiesta.

L' ID-SESSIONE recuperato dalla mail ricevuta dall'utente utilizzatore, deve essere inviato all'interno della chiamata client ai web services per i quali è stato richiesto, secondo le modalità indicate nel par. 5.3.

Di seguito il diagramma descrittivo:

RICHIESTA ID-SESSIONE DEL SISTEMATS TRAMITE APPLICAZIONE CLIENT DI TERZE PARTI

Di seguito la procedura per il recupero dell'ID-SESSIONE da parte di un utente tramite procedura web-service del Sistema TS



5.2.1 CERTIFICAZIONE MAIL

L'utente deve certificare la casella di posta elettronica per ricevere l'ID-SESSIONE richiesto tramite chiamata client al servizio di Sistema TS.

Di seguito viene descritta nel dettaglio la procedura:

1. Autenticarsi su Sistema TS con un livello minimo di sicurezza LoA3 ;
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 e-mail** 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 un nuovo codice validazione** cliccando sull'apposito bottone;
7. L'indirizzo e-mail 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 SISTEMA TS

L' ID-SESSIONE del Sistema TS, va inviato dai client in ogni transazione verso i servizi interessati, 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 specifici servizi o di 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-CONTESTO-[APPLICAZIONE]

*** Campo [APPLICAZIONE] facoltativo*

Esempio 1: ID-SESSIONE= **AAABBB00B01H501K-2025-04-RICETTA-DEMA**

Esempio 2: ID-SESSIONE= **AAABBB00B01H501K-2025-04-RICETTA**

Al fine di consentire un test completo di ricezione ID-SESSIONE e suo utilizzo nella chiamata ai servizi, in ambiente di TEST la configurazione prevede che l'invio dell' ID-SESSIONE avvenga direttamente nella risposta della chiamata al servizio di creazione del token.

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 client, richiama il servizio di richiesta dell' ID SESSIONE che può essere invocato all'inizio della sessione lavorativa o comunque ogni volta che si ha la necessità d'invocare un servizio che richiede l'autenticazione forte (per ID-SESSIONE di media o lunga durata, tipicamente una volta al giorno o comunque in base alla durata descritta al par. 5). Le specifiche del tracciato sono descritte nel prossimo paragrafo.

5.4.1 *AUTENTICAZIONE, GENERAZIONE ED INVIO DELL' ID-SESSIONE*

Di seguito, si riporta la descrizione dei parametri che è possibile inoltrare al servizio per la generazione ed invio dell' ID-SESSIONE. Alla base della chiamata c'è la basic authentication alla quale si aggiungono i parametri che saranno definiti dai diversi servizi del Sistema TS che adotteranno l'autenticazione forte.

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

Nome campo	Descrizione	Caratteristiche
identificativo	Codice identificativo in possesso del soggetto abilitato all'invio. Il valore può differire a seconda della tipologia di utente. Può essere, ad esempio, il PIN-CODE per un medico o l'id inviante per soggetti invianti 730. Nel caso in cui non sia previsto l'identificativo nella chiamata al servizio questo attributo deve essere omesso.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
tipo	Stringa che definisce la tipologia di *identificativo*. La lunghezza massima del campo è di due caratteri.	Obbligatorio se presente il campo *identificativo*. Il valore da inserire è specifico per ogni tipologia di identificativo ed è descritto nel kit di sviluppo.
valore	Stringa che rappresenta il valore dell'*identificativo* (Es.: PIN-CODE). Tale campo deve essere inserito criptato tramite l'utilizzo del certificato SanitelCF.cer.	Obbligatorio se presente il campo *identificativo*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.
userId	È la userId che identifica l'utente del Portale TS. Solitamente coincide con la userid utilizzata nell'autenticazione basic; può differire se per l'autenticazione basic viene utilizzato ad esempio il nickname.	Elemento obbligatorio
cfUtente	Codice fiscale associato all'utenza utilizzata nella basic authentication.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
codRegione	Codice Regione / Provincia Autonoma di appartenenza del	Obbligatorietà definita dal CONTESTO/APPLICAZIONE

	soggetto indicato in *userId*.	per cui il token viene richiesto
codAslAo	Codice ASL di appartenenza del soggetto indicato in *userId*.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
codSsa	Codice SSA di appartenenza del soggetto indicato in *userId*.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
codiceStruttura	Codice della struttura di appartenenza del soggetto indicato in *userId*.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
contesto	Insieme al campo applicazione, definisce il perimetro di validità del token relativo ai servizi che devono essere invocati.	Elemento obbligatorio. Il valore è definito dagli ambiti applicativi che utilizzano l'autenticazione forte.
applicazione	Insieme al campo contesto, definisce il perimetro di validità del token relativo ai servizi che devono essere invocati.	Obbligatorietà e valore definiti dal CONTESTO per cui il token viene richiesto.
opzioni	Lista di elementi di tipo *opzione*. Può contenere al massimo 10 elementi *opzione*. Nel caso in cui non siano previste opzioni nella chiamata al servizio questo attributo deve essere omesso.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
opzione	È un attributo del campo *opzioni* e consente l'inserimento di valori definiti attraverso gli attributi *chiave* e *valore*.	Obbligatorio se presente il campo *opzioni*.
chiave	Stringa che definisce il nome della chiave dell'attributo *opzione*.	Obbligatorio se presente il campo *opzione*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.
valore	Stringa che rappresenta il valore associato alla *chiave* dell'attributo *opzione*.	Obbligatorio se presente il campo *opzione*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.
infoAggiuntive	Lista di elementi di tipo *opzione*. Può contenere al massimo 10 elementi *opzione*. Nel caso in cui non siano	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto

		previste opzioni nella chiamata al servizio questo attributo deve essere omesso.	
	opzione	È un attributo del campo *infoAggiuntive* e consente l'inserimento di valori definiti attraverso gli attributi *chiave* e *valore*.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
		chiave	Stringa che definisce il nome della chiave dell'attributo *opzione*.	Obbligatorio se presente il campo *opzione*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.
		valore	Stringa che rappresenta il valore associato alla *chiave* dell'attributo *opzione*.	Obbligatorio se presente il campo *opzione*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.

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

In caso di errore viene fornito un messaggio diagnostico.

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

Endpoint di produzione:
https://servizits.sanita.finanze.it/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 SistemaTS attraverso l'invocazione dell'operation "revoke" del web service descritto di seguito.

Il client 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, si riporta la descrizione dei parametri che è possibile inoltrare al servizio per la revoca dell' ID-SESSIONE. Alla base della chiamata c'è la basic authentication alla quale si aggiungono i parametri che saranno definiti dai diversi servizi del SistemaTS che adotteranno l'autenticazione forte.

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

Nome campo	Descrizione	Caratteristiche
identificativo	Codice identificativo in possesso del soggetto abilitato all'invio. Il valore può differire a seconda della tipologia di utente. Può essere, ad esempio, il PIN-CODE per un medico o l'id inviante per soggetti invianti 730. Nel caso in cui non sia previsto l'identificativo nella chiamata al servizio questo attributo deve essere omesso.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
tipo	Stringa che definisce la tipologia di *identificativo*. La lunghezza massima del campo è di due caratteri.	Obbligatorio se presente il campo *identificativo*. Il valore da inserire è specifico per ogni tipologia di identificativo ed è descritto nel kit di sviluppo.

valore	Stringa che rappresenta il valore dell'*identificativo* (Es.: PIN-CODE). Tale campo deve essere inserito criptato tramite l'utilizzo del certificato SanitelCF.cer.	Obbligatorio se presente il campo *identificativo*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.
userId	È la userId che identifica l'utente del Portale TS. Solitamente coincide con la userid utilizzata nell'autenticazione basic; può differire se per l'autenticazione basic viene utilizzato ad esempio il nickname.	Elemento obbligatorio
cfUtente	Codice fiscale associato all'utenza utilizzata nella basic authentication.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
token	ID-SESSIONE da revocare	Elemento obbligatorio
contesto	Insieme al campo applicazione, definisce il perimetro di validità del token relativo ai servizi che devono essere invocati.	Elemento obbligatorio. Il valore è definito dagli ambiti applicativi che utilizzano l'autenticazione forte.
applicazione	Insieme al campo contesto, definisce il perimetro di validità del token relativo ai servizi che devono essere invocati.	Obbligatorietà e valore definiti dal CONTESTO per cui il token viene richiesto.
opzioni	Lista di elementi di tipo *opzione*. Può contenere al massimo 10 elementi *opzione*. Nel caso in cui non siano previste opzioni nella chiamata al servizio questo attributo deve essere omesso.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
opzione	È un attributo del campo *opzioni* e consente l'inserimento di valori definiti attraverso gli attributi *chiave* e *valore*.	Obbligatorio se presente il campo *opzioni*.
chiave	Stringa che definisce il nome della chiave dell'attributo *opzione*.	Obbligatorio se presente il campo *opzione*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.

		valore	Stringa che rappresenta il valore associato alla *chiave* dell'attributo *opzione*.	Obbligatorio se presente il campo *opzione*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.
infoAggiuntive			Lista di elementi di tipo *opzione*. Può contenere al massimo 10 elementi *opzione*. Nel caso in cui non siano previste opzioni nella chiamata al servizio questo attributo deve essere omesso.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
	opzione		È un attributo del campo *infoAggiuntive* e consente l'inserimento di valori definiti attraverso gli attributi *chiave* e *valore*.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
		chiave	Stringa che definisce il nome della chiave dell'attributo *opzione*.	Obbligatorio se presente il campo opzione. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.
		valore	Stringa che rappresenta il valore associato alla *chiave* dell'attributo *opzione*.	Obbligatorio se presente il campo opzione. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.

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://servizitstest.sanita.finanze.it/a2f-auth-ws/soap/v1/authentication-service

Endpoint di produzione:
https://servizits.sanita.finanze.it/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 SistemaTS attraverso l'invocazione dell'operation "checkToken" del web service descritto di seguito.

Il client 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, si riporta la descrizione dei parametri che è possibile inoltrare al servizio per la verifica dell' ID-SESSIONE. Alla base della chiamata c'è la basic authentication alla quale si aggiungono i parametri che saranno definiti dai diversi servizi del SistemaTS che adotteranno l'autenticazione forte.

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

Nome campo	Descrizione	Caratteristiche
identificativo	Codice identificativo in possesso del soggetto abilitato all'invio. Il valore può differire a seconda della tipologia di utente. Può essere, ad esempio, il PIN-CODE per un medico o l'id inviante per soggetti invianti 730. Nel caso in cui non sia previsto l'identificativo nella chiamata al servizio questo attributo deve essere omesso.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
tipo	Stringa che definisce la tipologia di *identificativo*. La lunghezza massima del campo è di due caratteri.	Obbligatorio se presente il campo *identificativo*. Il valore da inserire è specifico per ogni tipologia di identificativo ed è descritto nel kit di sviluppo.

valore	Stringa che rappresenta il valore dell'*identificativo* (Es.: PIN-CODE). Tale campo deve essere inserito criptato tramite l'utilizzo del certificato SanitelCF.cer.	Obbligatorio se presente il campo *identificativo*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.
userId	È la userId che identifica l'utente del Portale TS. Solitamente coincide con la userid utilizzata nell'autenticazione basic; può differire se per l'autenticazione basic viene utilizzato ad esempio il nickname.	Elemento obbligatorio
cfUtente	Codice fiscale associato all'utenza utilizzata nella basic authentication.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
token	ID-SESSIONE da verificare	Elemento obbligatorio
contesto	Insieme al campo applicazione, definisce il perimetro di validità del token relativo ai servizi che devono essere invocati.	Elemento obbligatorio. Il valore è definito dagli ambiti applicativi che utilizzano l'autenticazione forte.
applicazione	Insieme al campo contesto, definisce il perimetro di validità del token relativo ai servizi che devono essere invocati.	Obbligatorietà e valore definiti dal CONTESTO per cui il token viene richiesto.
opzioni	Lista di elementi di tipo *opzione*. Può contenere al massimo 10 elementi *opzione*. Nel caso in cui non siano previste opzioni nella chiamata al servizio questo attributo deve essere omesso.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
opzione	È un attributo del campo *opzioni* e consente l'inserimento di valori definiti attraverso gli attributi *chiave* e *valore*.	Obbligatorio se presente il campo *opzioni*.
chiave	Stringa che definisce il nome della chiave dell'attributo *opzione*.	Obbligatorio se presente il campo *opzione*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.

		valore	Stringa che rappresenta il valore associato alla *chiave* dell'attributo *opzione*.	Obbligatorio se presente il campo *opzione*. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.
infoAggiuntive			Lista di elementi di tipo *opzione*. Può contenere al massimo 10 elementi *opzione*. Nel caso in cui non siano previste opzioni nella chiamata al servizio questo attributo deve essere omesso.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
	opzione		È un attributo del campo *infoAggiuntive* e consente l'inserimento di valori definiti attraverso gli attributi *chiave* e *valore*.	Obbligatorietà definita dal CONTESTO/APPLICAZIONE per cui il token viene richiesto
		chiave	Stringa che definisce il nome della chiave dell'attributo *opzione*.	Obbligatorio se presente il campo opzione. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.
		valore	Stringa che rappresenta il valore associato alla *chiave* dell'attributo *opzione*.	Obbligatorio se presente il campo opzione. Il valore è definito dal CONTESTO/APPLICAZIONE per cui il token viene richiesto.

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://servizitstest.sanita.finanze.it/a2f-auth-ws/soap/v1/authentication-service

Endpoint di produzione:
https://servizits.sanita.finanze.it/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 - Accesso – Autenticazione a 2 Fattori (web services) - Documenti e specifiche tecniche