Modulo regionale di accesso semplificato dalle CCE
Specifiche di integrazione dei servizi di accesso

STATO DELLE VARIAZIONI

vers	**PARAGRAFO O PAGINA**	**DESCRIZIONE DELLA VARIAZIONE**
V01	Tutto il documento	Prima stesura del documento
V02	Tutto il documento	Revisione generale. In particolare, sono stati raggruppati i codici tipo_documento per il parametro aggiuntivo relativo all'applicazione FSE.
V03	Tutto il documento	Revisione generale per generalizzare l'integrazione fra CCE MMG/PLS e/o ospedaliere con FSE
V04	Paragrafo 2.2.1	Aggiunto paragrafo
	Cap. 3, Cap 4.	Aggiornati namespace delle request e delle response
	Cap. 5	Aggiornato wsdl
V05	Tutto il documento	Aggiunta descrizione servizio getAuthenticationConShibboleth Revisione codifiche Revisione accesso FSEr
V06	Cap.6 Cap 8,9,10	Revisione frase nel paragrafo 6.4 Il capitolo 2.2.1 è stato spostato e ulteriormente precisato nei capitoli 8,9,10

INDICE

1. Scopo e riferimenti del documento

1.1 Scopo del documento

Lo scopo del documento è fornire le specifiche dei requisiti di dettaglio che descrivano il funzionamento atteso, le caratteristiche e le modalità di utilizzo dei servizi esposti per consentire alle Cartelle Cliniche Elettroniche degli operatori sanitari (Medici di Medicina Generale, Pediatri di Libera Scelta, medici ospedalieri e altri operatori del settore) di accedere direttamente alle applicazioni Web dei Servizi della Sanità digitale della Regione Piemonte in maniera tale da agevolarne l'utilizzo.

Questo documento in particolare descrive le modalità con le quali è possibile:

- ottenere il token di accesso per le applicazioni di CCE non integrate con il sistema di autenticazione Shibbolet del CSI-Piemonte
- ottenere i token di accesso per le applicazioni di CCE integrate con il sistema di autenticazione Shibbolet del CSI-Piemonte
- utilizzare il token di accesso ottenuto per accedere al FSE di un assistito della Regione Piemonte

1.2 Glossario

CCE	Cartelle Cliniche elettroniche
URL di attivazione	Sinonimo di Pagina di accesso
Pagina di accesso	Si intende la nuova pagina o la nuova URL che viene resa disponibile dalle applicazioni web della Sanità digitale della Regione Piemonte per consentire agli operatori sanitari di accedere senza inserire le credenziali
Credenziali RUPAR	Sono le credenziali (username, password e pin) assegnate agli operatori della Pubblica Amministrazione (PA) per accedere alle procedure della PA Piemontese
SI FSE	Sistema Informativo del Fascicolo Sanitario Elettronico del Piemonte
FSE/ FSEr	Fascicolo Sanitario Elettronico del Piemonte
IP	Ip address: internet protocol address; indirizzo di rete della postazione da cui l'operatore sanitario accede
token	Stringa alfanumerica di tipo UID, utilizzata per definire un codice di autorizzazione di accesso alle web application, utilizzabile una solo volta.
Shibboleth	Sistema di autenticazione, adottato anche dal CSI-Piemonte, che consente di autenticarsi su sistemi differenti eseguendo un solo accesso

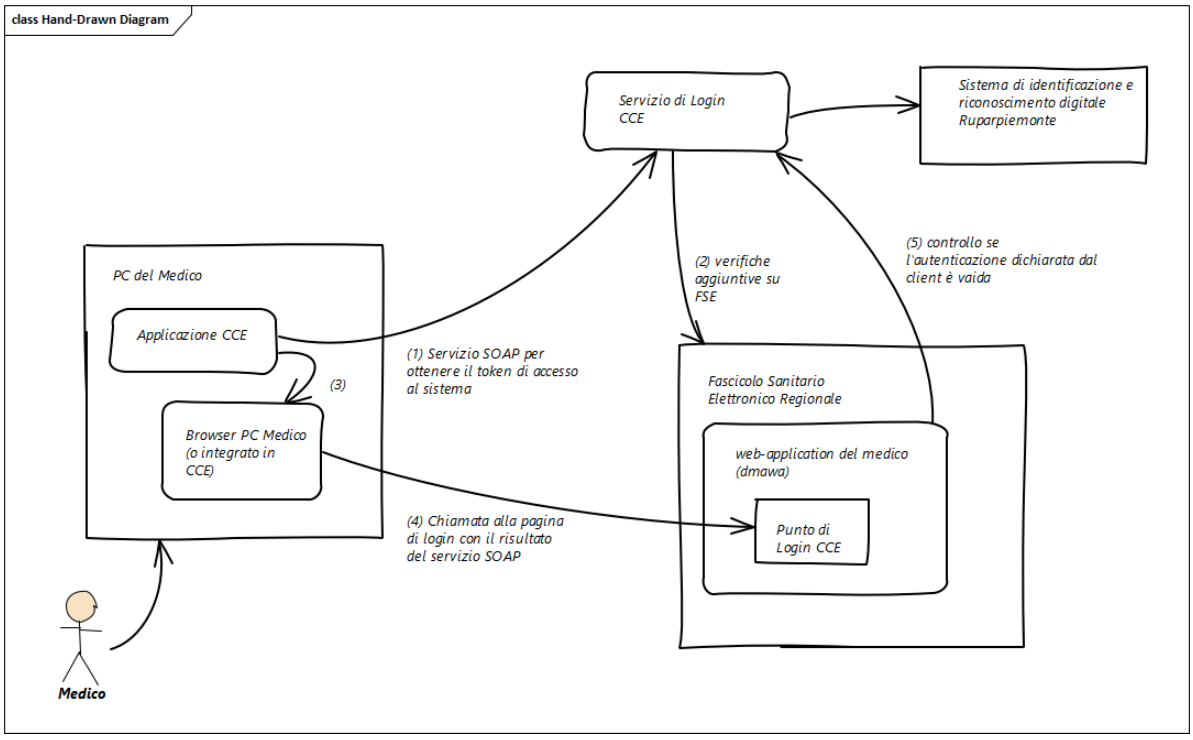
2. Specifiche tecniche

2.1 Specifiche funzionali

Al fine di consentire alle Cartelle Cliniche Elettroniche (CCE) di aprire il dettaglio di un assistito su una applicazione web dei Servizi della Sanità digitale Regionale, vengono resi disponibili:

- un servizio web SOAP per consentire alla cartella clinica non integrate con Shobboleth del CSI-Piemonte di autenticare l'utente e ottenere un token di accesso (in seguito "getAuthentication")
- un servizio web SOAP per consentire alla cartella clinica integrata con Shobboleth del CSI-Piemonte di ottenere un token di accesso (in seguito "getAuthenticationConShibboleth")
- una pagina di accesso (URL) nelle web-application per consentire alle CCE di eseguire l'accesso diretto, in questo documento viene descritto l'accesso di FSE

Il processo che si intende andare a realizzare è quanto descritto nel seguente diagramma, ipotizzando l'accesso alla web-application di FSE dedicata agli operatori sanitari.



Descrizione:

Il medico, usando la propria cartella clinica (client web o desktop), apre la cartella di un paziente, e clicca sul tasto che serve ad aprire il fascicolo del paziente.

Caso 1: CCE o applicazioni non integrata con l'installazione Shibboleth del CSI-Piemonte

Nel caso in cui il chiamante sia una CCE o una applicazione non integrata con l'installazione Shibboleth del

CSI-Piemonte, verrà chiamato il web service di autenticazione "getAuthentication" fornendo le credenziali RUPAR del medico, il ruolo del medico e il codice fiscale del paziente per il quale si vuole consultare il fascicolo (1).

Il servizio "getAuthentication" verifica:

- le credenziali del medico
- contatta il SI FSE (2) per verificare che:
  - il medico sia censito nei sistemi di FSE
  - il paziente sia gestito dal FSEr
  - il paziente abbia espresso il consenso alla consultazione del proprio FSE

Se tutti i controlli hanno esito positivo, il servizio, restituisce alla CCE un token di autenticazione che la CCE dovrà utilizzare per aprire in un browser la pagina di accesso al FSEr, fornendo in GET anche il token di autenticazione (3).

Questa URL non viene protetta dal sistema di autenticazione del CSI-Piemonte Shibbolteh, in quanto si assumono come valide le credenziali fornite al servizio.

La web application dei medici del FSEr avvia una nuova sessione utente per il medico (4), verificando che il token fornito dalla cartella sia valido; dopodiché apre la pagina di dettaglio dell'assistito richiesto o l'elenco dei documenti di un assistito.

Caso 2: Applicazioni integrate con l'installazione Shibboleth del CSI-Piemonte (p.es. ECWMED)

Nel caso in cui il chiamante una applicazione integrata con l'installazione Shibboleth del CSI-Piemonte, verrà chiamato il web service di autenticazione "getAuthenticationConShibboleth", al quale verrà richiesto il codice fiscale del medico, il ruolo e il codice fiscale del paziente per il quale si vuole consultare il fascicolo (1).

Il servizio "getAuthenticationConShibboleth" verifica:

- contatta il SI FSE (2) per verificare che:
  - il medico sia censito nei sistemi di FSE
  - il paziente sia gestito dal FSEr
  - il paziente abbia espresso il consenso alla consultazione del proprio FSE

Se tutti i controlli hanno esito positivo, il servizio, restituisce all'applicazione chiamante un token di autenticazione che dovrà essere utilizzato per aprire in un browser la pagina di accesso al FSEr, fornendo in GET anche il token di autenticazione (3).

Questa URL viene protetta dal sistema di autenticazione del CSI-Piemonte Shibbolteh, attraverso i meccanismi di SSO la credenziale non verrà più richiesta.

La web application dei medici del FSEr avvia una nuova sessione utente per il medico (4), verificando che il token fornito dalla cartella sia valido; dopodiché apre la pagina di dettaglio dell'assistito richiesto o l'elenco dei documenti di un assistito.

2.2 Sicurezza del servizio e protocolli di comunicazione

Tutte le chiamate provenienti dalle cartelle cliniche o applicazioni non protette dal sistema di autenticazione Shibboleth del CSI-Piemonte, dovranno essere eseguite in https (TLS 1.2), la cartella clinica verrà autenticata con certificato X.509 (two-way SSL authentication).

Ogni fornitore di cartella clinica dovrà pertanto disporre di un certificato di autenticazione.

L'accesso da parte degli operatori sanitari con il meccanismo della chiamata di contesto proveniente dalle cartelle cliniche o applicazioni non protette dal sistema di autenticazione Shibboleth, sarà previa autorizzazione, attraverso richiesta scritta.

Tutte le chiamate provenienti da applicazioni protette dal sistema di autenticazione Shibboleth del CSI-Piemonte saranno eseguite in https (TLS 1.2), con riconoscimento del sistema chiamante attraverso la protezione del servizio tramite WS-Security UsernameToken-Profile.

I servizi "getAuthentication" e "getAuthenticationConShibboleth" verranno esposti con protocollo SOAP 1.2.

Quando il client di cartella clinica invoca il servizio "getAuthentication" e "getAuthenticationConShibboleth" dovranno fornire anche l'ip address del client che successivamente chiamerà la web-application del sistema regionale (ad esempio il FSE); tale IP sarà tracciato dai sistemi PUA e FSEr.

3. Servizio <SRV-01>: getAuthentication

3.1 Obiettivi

Consentire alla cartella clinica di avviare il processo di login diretto per un suo utente a una applicazione predisposta (p.es sul FSEr), così da poter accedere direttamente al dettaglio di un assistito.

3.2 Fruitori

Client di Cartella clinica di un operatore sanitario

3.3 Struttura del messaggio di "request"

GETAUTHENTICATIONREQUEST

1	richiedente	1..1	Identifica l'operatore sanitario che dalla CCE vuole eseguire il login automatico su una applicazione predisposta
2	credenziali	1..1	Oggetto credenziali dell'operatore sanitario
3	username	1..1	Username RUPAR Piemonte dell'operatore sanitario
3	password	1..1	Password delle credenziali RUPAR dell'operatore sanitario
3	PIN	0..1	PIN delle credenziali RUPAR dell'operatore sanitario
2	ruolo	1..1	Ruolo dell'operatore sanitario richiedente. I valori ammessi sono riportati in tabella 3 del presente documento
2	ipClient	0..1	IP Address della postazione dell'operatore sanitario che accederà alla web-application; se non specificato verrà assunto che l'ip della postazione dell'operatore sanitario sarà l'ip del client che ha chiamato il servizio.
2	applicazione	1..1	Identifica l'applicazione alla quale l'utente si vuole collegare. I valori ammessi sono riportati in tabella 4 del presente documento
1	codiceFiscaleAssistito	1..1	Codice fiscale del paziente del quale si vuole avere il dettaglio
1	parametriLogin	0..1	Elenco dei parametri aggiuntivi che si vuole passare alla web-application in fase di login.

			L'elenco dei parametri aggiuntivi ammessi è riportato al paragrafo 3.5.2 Se "parametriLogin" non viene valorizzato, al momento del login, la web-application eseguirà l'operazione di default.
2	parametro	1..*	Parametro aggiuntivo
3	Codice	1..1	Codice del parametro aggiuntivo I valori ammessi sono nel paragrafo 3.5.2 del presente documento
3	valore	1..1	Valore per il parametro I valori ammessi sono nel paragrafo 3.5.2 del presente documento

Request di esempio:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
               xmlns:log="http://dma.csi.it/LoginCCE">
   <soap:Header/>
   <soap:Body>
      <log:getAuthenticationRequest>
         <richiedente>
            <credenziali>
               <username>allione@test</username>
               <password>?</password>
            </credenziali>
            <ruolo>MMG</ruolo>
            <applicazione>DMAWA</applicazione>
         </richiedente>
         <codiceFiscaleAssistito>XXXYYY59R45G163O</codiceFiscaleAssistito>
      </log:getAuthenticationRequest>
   </soap:Body>
</soap:Envelope>
```

3.4 Struttura del messaggio di "response"

GETAUTHENTICATION

RESPONSE

1	errori	0..1	In caso di errori viene valorizzato con l'elenco degli errori riscontrati
2	errore	1..*	Errore rif. Tabella 1 - Elenco degli errori
3	codice	1..1	Codice dell'errore
3	descrizione	0..1	Descrizione dell'errore
1	esito	1..1	Esito della chiamata del servizio • SUCCESSO • FALLIMENTO

1	authenticationToken	0..1	Se non si verificano errori bloccanti viene restituito il token di autenticazione, da utilizzare per collegarsi all'applicazione web del sistema regionale

Esempio di response con esito positivo:

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <env:Header/>
   <env:Body>
      <ns3:getAuthenticationResponse xmlns:ns3="http://dma.csi.it/LoginCCE">
         <esito>SUCCESSO</esito>
         <authenticationToken>d660807d-0545-4b11-9820-78a1e4024fa0</authenticationToken>
      </ns3:getAuthenticationResponse>
   </env:Body>
</env:Envelope>
```

Esempio di response con esito negativo:

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <env:Header/>
   <env:Body>
      <ns3:getAuthenticationResponse xmlns:ns3="http://dma.csi.it/LoginCCE">
         <errori>
            <errore>
               <codice>FSE_ER_507</codice>
               <descrizione>L'applicazione remota non è disponibile a esegiore il login</descrizione>
            </errore>
         </errori>
         <esito>FALLIMENTO</esito>
      </ns3:getAuthenticationResponse>
   </env:Body>
</env:Envelope>
```

Esempio di eccezione

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <env:Header/>
   <env:Body>
      <env:Fault>
         <env:Code>
            <env:Value>env:Receiver</env:Value>
         </env:Code>
         <env:Reason>
            <env:Text xml:lang="en">javax.management.RuntimeErrorException</env:Text>
         </env:Reason>
      </env:Fault>
   </env:Body>
</env:Envelope>
```

4. Servizio <SRV-02>: getAuthenticationConShibboleth

4.1 Obiettivi

Consentire alla cartella clinica di far accedere a un suo utente direttamente al dettaglio di un assistito di applicazione predisposta (p.es sul FSEr).

4.2 Fruitori

Client di Cartella clinica di un operatore sanitario

4.3 Struttura del messaggio di "request"

GETAUTHENTICATIONCONSHIBBOLETHREQUEST

1	richiedente	1..1	Identifica l'operatore sanitario che dalla CCE vuole eseguire il login automatico su una applicazione predisposta
2	applicazione	1..1	Identifica l'applicazione alla quale l'utente si vuole collegare. I valori ammessi sono riportati in tabella 4 del presente documento
2	codiceFiscaleMedico	1..1	Codice fiscale dell'operatore che vuole accedere alla applicazione e che ha eseguito il login nella applicazione chimante
2	ipClient	0..1	IP Address della postazione dell'operatore sanitario che accederà alla web-application; se non specificato verrà assunto che l'ip della postazione dell'operatore sanitario sarà l'ip del client che ha chiamato il servizio.
2	ruolo	1..1	Ruolo dell'operatore sanitario richiedente. I valori ammessi sono riportati in tabella 3 del presente documento
1	codiceFiscaleAssistito	1..1	Codice fiscale del paziente del quale si vuole avere il dettaglio
1	parametriLogin	0..1	Elenco dei parametri aggiuntivi che si vuole passare alla web-application in fase di login. L'elenco dei parametri aggiuntivi ammessi è riportato al paragrafo 3.5.2 Se "parametriLogin" non viene valorizzato, al momento del login, la web-application eseguirà l'operazione di default.
2	parametro	1..*	Parametro aggiuntivo
3	Codice	1..1	Codice del parametro aggiuntivo I valori ammessi sono nel paragrafo 3.5.2 del presente documento
3	valore	1..1	Valore per il parametro I valori ammessi sono nel paragrafo 3.5.2 del presente documento

Request di esempio:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:dmac="http://dmaccbl.csi.it/"
                    xmlns:dmac1="http://dmac.csi.it/" xmlns:dma="http://dma.csi.it/">
   <soap:Header/>
   <soap:Body>
      <dmac:getAuthenticationConShibbolethRequest>
         <dmac1:richiedente>
            <applicazione>DMAWA</applicazione>
            <codiceFiscaleMedico>XXXYYY84R55L219M</codiceFiscaleMedico>
            <ipClient>555.36.33.555</ipClient>
            <ruolo>MMG</ruolo>
         </dmac1:richiedente>
         <dma:codiceFiscaleAssistito>XXXYYY59R45G163O</dma:codiceFiscaleAssistito>
      </dmac:getAuthenticationConShibbolethRequest>
   </soap:Body>
</soap:Envelope>
```

4.4 Struttura del messaggio di "response"

GETAUTHENTICATIONCONSHIBBOLETHRESPONSE

1	errori	0..1	In caso di errori viene valorizzato con l'elenco degli errori riscontrati
2	errore	1..*	Errore rif. Tabella 1 - Elenco degli errori
3	codice	1..1	Codice dell'errore
3	descrizione	0..1	Descrizione dell'errore
1	esito	1..1	Esito della chiamata del servizio • SUCCESSO • FALLIMENTO
1	authenticationToken	0..1	Se non si verificano errori bloccanti viene restituito il token di autenticazione, da utilizzare per collegarsi all'applicazione web del sistema regionale

Esempio di response con esito positivo:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
   <soap:Body>
      <ns4:getAuthenticationConShibbolethResponse xmlns:ns2="http://dmac.csi.it/"
                        xmlns:ns3="http://dma.csi.it/" xmlns:ns4="http://dmacc.csi.it/">
         <ns3:errori/>
         <esito>SUCCESSO</esito>
         <ns3:authenticationToken>a4016c79-ac0f-4d9d-b777-a6780488f363</ns3:authenticationToken>
      </ns4:getAuthenticationConShibbolethResponse>
   </soap:Body>
</soap:Envelope>
```

Esempio di response con esito negativo:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
   <soap:Body>
      <ns4:getAuthenticationConShibbolethResponse xmlns:ns2="http://dmac.csi.it/"
                              xmlns:ns3="http://dma.csi.it/" xmlns:ns4="http://dmacc.csi.it/">
         <ns3:errori>
            <ns3:errore>
               <codice>AUTH_ER_518</codice>
               <descrizione>Utente richiedente non censito per il servizio di Login CCE</descrizione>
            </ns3:errore>
         </ns3:errori>
         <esito>FALLIMENTO</esito>
      </ns4:getAuthenticationConShibbolethResponse>
   </soap:Body>
</soap:Envelope>
```

Esempio di eccezione

```
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
   <env:Header/>
   <env:Body>
      <env:Fault>
         <env:Code>
            <env:Value>env:Receiver</env:Value>
         </env:Code>
         <env:Reason>
            <env:Text xml:lang="en">javax.management.RuntimeErrorException</env:Text>
         </env:Reason>
      </env:Fault>
   </env:Body>
</env:Envelope>
```

5. Codifiche dei servizi

5.1.1 Elenco errori

Tabella 1 - Elenco degli errori

Codice	Descrizione	
AUTH_ER_000	Errore di sistema	Errore interno del servizio; quando si verifica è necessario informare l'utente di riprovare e, se l'errore persiste, di contattare l'assistenza.
AUTH_ER_501	Errore di autenticazione	Le credenziali dell'operatore sanitario fornite al sistema sono errate o non più validi; per motivi si sicurezza questo errore non viene dettagliato.
AUTH_ER_502	Ruolo non valido	Il ruolo fornito non esiste per l'applicazione richiedente
AUTH_ER_506	La CCE per questo operatore sanitario non è autorizzata all'accesso	Il sistema non è stato configurato per consentire all'operatore sanitario di accedere dalla CCE all'applicazione richiesta
AUTH_ER_507	L'applicazione remota non è disponibile a eseguire il login	Si verifica quando l'applicazione remota alla quale si vuole accedere è temporaneamente off-line o ha restituito un errore in fase di verifica iniziale.
AUTH_ER_510	Il parametro Pin del richiedente deve essere valorizzato	Nella chiamata getAuthentication non è stato impostato il parametro Pin del richiedente
AUTH_ER_511	Il parametro Ruolo Richiedente deve essere valorizzato	Come da descrizione
AUTH_ER_512	Il parametro Ip Client del Richiedente deve essere valorizzato	Come da descrizione
AUTH_ER_513	Il parametro Applicazione deve essere valorizzato	Come da descrizione
AUTH_ER_514	Il parametro cf Assistito deve essere valorizzato	Come da descrizione
AUTH_ER_517	I parametri "XXX" non sono previsti per l'applicazione "XXX"	Si verifica quando viene indicato un parametro non conforme all'applicazione richiesta
AUTH_ER_515	Il Richiedente deve essere valorizzato	Come da descrizione
AUTH_ER_516	Le credenziali devono essere valorizzate	Come da descrizione
AUTH_ER_628	Il campo "XXX" deve essere valorizzato	Si verifica quando un parametro obbligatorio non è stato indicato (p.es. si valorizza il campo parametro.codice ma non parametro.valore)

A questi errori si aggiungono gli errori specifici che può restituire il sistema al quale ci si vuole collegare.

Per l'applicazione FSE:

Codice	Descrizione	
FSE_ER_000	Errore di sistema	Errore interno del servizio; quando si verifica è necessario informare l'utente di riprovare e, se l'errore persiste, di contattare l'assistenza FSE.
FSE_ER_503	Paziente non trovato	Il codice fiscale fornito non è stato trovato nel FSE
FSE_ER_505	Il paziente non ha fornito il consenso alla consultazione	L'assistito non ha fornito il consenso alla consultazione del proprio FSE
FSE_ER_504	Tipo documento non valido	Il tipo di documento indicato non è tra quelle accettati dal sistema.

5.1.2 Tipi PARAMETRO AGGIUNTIVO

Tabella 2 Elenco tipi parametro per Applicazione

Applicazione	Codice	Descrizione
FSE	**TIPO_DOCUMENTO**	Tipologia di documento che deve essere impostata come filtro nella visualizzazione dell'elenco dei documenti del FSE

Tabella - Elenco valori parametro per TIPO_DOCUMENTO del FSE

Codice	Descrizione
57833-6	PRESCRIZIONE FARMACEUTICA
57832-8	PRESCRIZIONE DIAGNOSTICA O SPECIALISTICA
60591-5	PROFILO SANITARIO SINTETICO / PATIENT SUMMARY
ATTO_OPERATORIO	ATTO OPERATORIO
29304-3	PRESTAZIONE FARMACEUTICA
81223-0	PRESTAZIONE SPECIALISTICA
28653-4	CERTIFICATO DI MALATTIA
59258-4	VERBALE DI PRONTO SOCCORSO che vale anche per la vecchia codifica DEA_VERBALE utilizzata nel connettore di alimentazione del FSE prima del 2018
34105-7	LETTERA DI DIMISSIONE OSPEDALIERA che vale anche per la vecchia codifica LET_DIMISSIONE utilizzata nel connettore di alimentazione del FSE prima del 2018
68604-8	REFERTO DI RADIOLOGIA che vale anche per la vecchia codifica REFERTO_RIS utilizzata nel connettore di alimentazione del FSE prima del 2018
11488-4	REFERTO SPECIALISTICO che vale anche per la vecchia codifica REFERTO utilizzata nel connettore di alimentazione del FSE prima del 2018
11526-1	REFERTO DI ANATOMIA PATOLOGICA che vale anche per la vecchia codifica REFERTO_AP utilizzata nel connettore di alimentazione del FSE prima del 2018
11502-2	REFERTO DI LABORATORIO che vale anche per la vecchia codifica REFERTO_LIS utilizzata nel connettore di alimentazione del FSE prima del 2018
57829-4	PRESCRIZIONE PER PRODOTTO O APPARECCHIATURE MEDICHE
57827-8	ATTESTATO DI ESENZIONE
REG-87273-9	SCHEDA VACCINALE
87273-9	SCHEDA VACCINALE
PCP	PIANO DI CURA PERSONALIZZATO
BDS	BILANCIO DI SALUTE
PCP	PIANO DI CURA PERSONALIZZATO

REG-ESE-11488-4	CERTIFICATO DI CONDIZIONE O MALATTIA

5.1.3 Ruoli per applicazione

Tabella 3 - Elenco ruoli

Per l'applicazione FSE

Codice	Descrizione
INF	Personale infermieristico
MEDOSP	Dirigente Sanitario
MEDRP	Medico Rete di Patologia
MEDRSA	Medico RSA
FAR	Farmacista
OPSOCSA	Professionista del sociale
AAS	Personale di assistenza ad alta specializzazione (Medico)
DSA	Direttore Sanitario
DAM	Direttore Amministrativo
MMG	Medico di Medicina Generale
PLS	Medico di Medicina Generale /pediatra di Libera scelta (PLS)
GUARD	Guardia medica

5.1.4 Elenco Applicazioni

Tabella 4 - Elenco Applicazioni

Codice	Descrizione
DMAWA	FSE per operatori sanitari

6. Pagina <SRV-02>: Accesso al fascicolo da parte dell'operatore sanitario

6.1 Obiettivi

Consentire di eseguire l'accesso diretto al dettaglio di un assistito per un utente della CCE sul FSEr.

6.2 Fruitori

Client di Cartella clinica dell'operatore sanitario

6.3 Struttura del messaggio di "request"

Request URL per le applicazioni con shibbolet integrato:

https://med.fsepiemonte.it/dmawa/xxxx?token=**{authenticationToken}**

Request URL per le applicazioni senza shibbolet integrato:

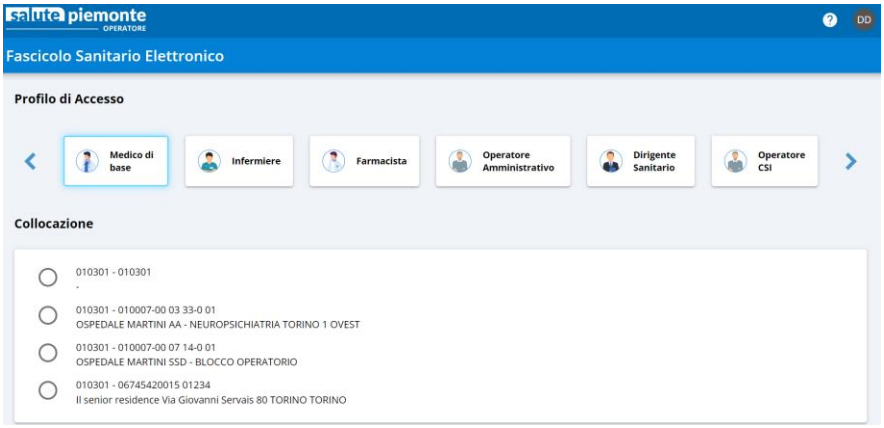
https://medtok.fsepiemonte.it/dmawa/xxxx?token=**{authenticationToken}**

Request Method: `GET`

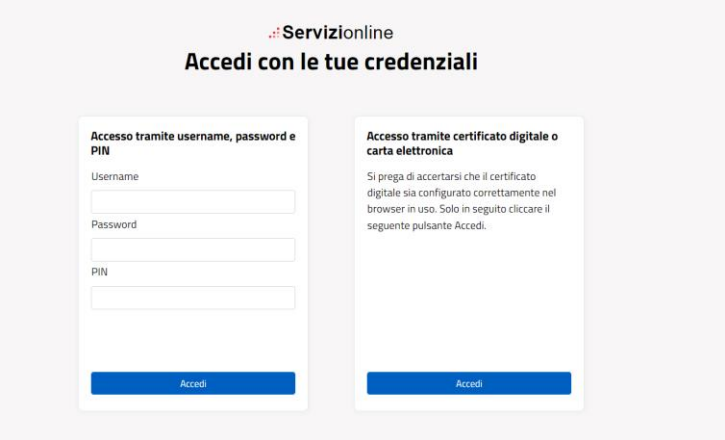
authenticationToken: si tratta del codice (token) di autenticazione restituito dal servizio "getAuthentication" o "getAuthenticationConShibboleth"

6.4 Pagina di risposta

Esempio di videata di accesso al FSE chiamando il servizio senza autenticazione Shibboleth (https://cert-medtok.fsepiemonte.it/dmawa/lcce?tokenLCCE=XXX)



Viene presentata la stessa videata soprariporata se è già stato effettuato il login su IDP Rupar. In caso contrario viene riportata la pagina di login pur richiamando la url: https://cert-med.fsepiemonte.it/dmawa/ecwdmed?tokenLCCE=<token> .



L'applicazione web del fascicolo oltre alla pagina richiesta (dettaglio fascicolo o elenco documenti), potrà restituire una pagina di errore (rif. Tabella 3 - Elenco errori web-application).

6.4.1 Elenco errori

Tabella 3 - Elenco errori web-application

Codice	Descrizione	
WEB_000	Errore interno al sistema. Non è stato possibile completare l'operazione	Errore interno del servizio.
WEB_001	Token di autenticazione non valido	Questo errore viene restituito quando si tenta di accedere alla web application del sistema regionale usando un token: • non generato dal servizio "getAuthentication" • già utilizzato in precedenza • scaduto

7. Definizione dei servizi (wsdl)

7.1 Servizio getAuthentication

```
<?xml version='1.0' encoding='UTF-8'?>
<wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:tns="http://dmacc.csi.it/"
            xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
            xmlns:ns2="http://schemas.xmlsoap.org/soap/http" xmlns:ns1="http://dmaccbl.csi.it/"
            name="AuthenticationService" targetNamespace="http://dmacc.csi.it/">
  <wsdl:types>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://dmacc.csi.it/"
          xmlns:ns2="http://dma.csi.it/" xmlns:ns1="http://dmac.csi.it/"
          attributeFormDefault="unqualified" elementFormDefault="unqualified"
          targetNamespace="http://dmacc.csi.it/">
  <xs:import namespace="http://dmac.csi.it/"/>
  <xs:import namespace="http://dma.csi.it/"/>
  <xs:element name="getAuthenticationRequest" type="tns:getAuthenticationRequest"/>
  <xs:element name="getAuthenticationResponse" type="tns:getAuthenticationResponse"/>
  <xs:element name="parametriLogin" type="ns2:parametriLogin"/>
  <xs:complexType name="getAuthenticationRequest">
    <xs:sequence>
      <xs:element minOccurs="0" ref="ns1:richiedente"/>
      <xs:element minOccurs="0" ref="ns2:codiceFiscaleAssistito"/>
      <xs:element maxOccurs="unbounded" minOccurs="0" ref="ns2:parametriLogin"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="getAuthenticationResponse">
    <xs:complexContent>
      <xs:extension base="tns:serviceResponse">
        <xs:sequence>
          <xs:element minOccurs="0" ref="ns2:authenticationToken"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="serviceResponse">
    <xs:complexContent>
      <xs:extension base="tns:Ens_Response">
        <xs:sequence>
          <xs:element minOccurs="0" ref="ns2:errori"/>
          <xs:element minOccurs="0" name="esito" type="tns:risultatoCodice"/>
          <xs:element maxOccurs="unbounded" minOccurs="0" ref="ns2:codifiche"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="Ens_Response">
    <xs:complexContent>
      <xs:extension base="tns:Ens_Messagebody">
        <xs:sequence/>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="Ens_Messagebody">
    <xs:sequence/>
  </xs:complexType>
  <xs:complexType name="errori">
    <xs:sequence>
      <xs:element maxOccurs="unbounded" minOccurs="0" ref="ns2:errore"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="Ens_Request">
    <xs:complexContent>
      <xs:extension base="tns:Ens_Messagebody">
        <xs:sequence/>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:simpleType name="risultatoCodice">
```

```
    <xs:restriction base="xs:string">
      <xs:enumeration value="SUCCESSO"/>
      <xs:enumeration value="FALLIMENTO"/>
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://dmac.csi.it/"
xmlns:ns1="http://dma.csi.it/" attributeFormDefault="unqualified" elementFormDefault="unqualified"
targetNamespace="http://dmac.csi.it/">
  <xs:import namespace="http://dma.csi.it/"/>
  <xs:element name="richiedente" type="tns:richiedente"/>
  <xs:complexType name="richiedente">
    <xs:sequence>
      <xs:element minOccurs="0" name="applicazione" type="xs:string"/>
      <xs:element minOccurs="0" name="credenziali" type="ns1:credenziali"/>
      <xs:element minOccurs="0" name="ipClient" type="xs:string"/>
      <xs:element minOccurs="0" name="ruolo" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://dma.csi.it/"
xmlns:ns1="http://dmacc.csi.it/" attributeFormDefault="unqualified" elementFormDefault="unqualified"
targetNamespace="http://dma.csi.it/">
  <xs:import namespace="http://dmacc.csi.it/"/>
  <xs:element name="authenticationToken" type="xs:string"/>
  <xs:element name="codiceFiscaleAssistito" type="xs:string"/>
  <xs:element name="codifiche" type="tns:codifica"/>
  <xs:element name="errore" type="tns:errore"/>
  <xs:element name="errori" type="ns1:errori"/>
  <xs:element name="parametriLogin" type="tns:parametriLogin"/>
  <xs:complexType name="credenziali">
    <xs:sequence>
      <xs:element minOccurs="0" name="PIN" type="xs:string"/>
      <xs:element minOccurs="0" name="password" type="xs:string"/>
      <xs:element minOccurs="0" name="username" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="parametriLogin">
    <xs:sequence>
      <xs:element minOccurs="0" name="codice" type="xs:string"/>
      <xs:element minOccurs="0" name="valore" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="errore">
    <xs:complexContent>
      <xs:extension base="tns:codifica">
        <xs:sequence/>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="codifica">
    <xs:sequence>
      <xs:element minOccurs="0" name="codice" type="xs:string"/>
      <xs:element minOccurs="0" name="descrizione" type="xs:string"/>
      <xs:element minOccurs="0" name="riferimento" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://dmacc.csi.it/"
xmlns="http://dmaccbl.csi.it/" attributeFormDefault="unqualified" elementFormDefault="qualified"
targetNamespace="http://dmaccbl.csi.it/">
  <xsd:import namespace="http://dmacc.csi.it/"/>
  <xsd:element name="getAuthenticationRequest" nillable="true" type="tns:getAuthenticationRequest"/>
</xsd:schema>
  </wsdl:types>
  <wsdl:message name="getAuthentication">
    <wsdl:part element="ns1:getAuthenticationRequest" name="getAuthenticationRequest">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="getAuthenticationResponse">
    <wsdl:part element="tns:getAuthenticationResponse" name="getAuthenticationResponse">
```

```
    </wsdl:part>
  </wsdl:message>
  <wsdl:portType name="AuthenticationService">
    <wsdl:operation name="getAuthentication">
      <wsdl:input message="tns:getAuthentication" name="getAuthentication">
    </wsdl:input>
      <wsdl:output message="tns:getAuthenticationResponse" name="getAuthenticationResponse">
    </wsdl:output>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="AuthenticationServiceSoapBinding" type="tns:AuthenticationService">
    <soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="getAuthentication">
      <soap12:operation soapAction="http://dmaccbl.csi.it/getAuthentication" style="document"/>
      <wsdl:input name="getAuthentication">
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output name="getAuthenticationResponse">
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="AuthenticationService">
    <wsdl:port binding="tns:AuthenticationServiceSoapBinding" name="AuthenticationService">
      <soap12:address location="https://sg-srv-lcce.isan.csi.it/lccews/AuthenticationService"/>
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

7.2 Servizio getAuthenticationConShibboleth

```
<?xml version='1.0' encoding='UTF-8'?>
<wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:tns="http://dmacc.csi.it/"
        xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
        xmlns:ns2="http://schemas.xmlsoap.org/soap/http" xmlns:ns1="http://dmaccbl.csi.it/"
        name="AuthenticationConShibbolethService" targetNamespace="http://dmacc.csi.it/">
  <wsdl:types>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://dmacc.csi.it/"
           xmlns:ns2="http://dma.csi.it/" xmlns:ns1="http://dmac.csi.it/"
           attributeFormDefault="unqualified" elementFormDefault="unqualified"
           targetNamespace="http://dmacc.csi.it/">
  <xs:import namespace="http://dmac.csi.it/"/>
  <xs:import namespace="http://dma.csi.it/"/>
  <xs:element name="getAuthenticationConShibbolethRequest"
type="tns:getAuthenticationConShibbolethRequest"/>
  <xs:element name="getAuthenticationConShibbolethResponse"
type="tns:getAuthenticationConShibbolethResponse"/>
  <xs:element name="parametriLogin" type="ns2:parametriLogin"/>
  <xs:complexType name="getAuthenticationConShibbolethRequest">
    <xs:sequence>
      <xs:element minOccurs="0" ref="ns1:richiedente"/>
      <xs:element minOccurs="0" ref="ns2:codiceFiscaleAssistito"/>
      <xs:element maxOccurs="unbounded" minOccurs="0" ref="ns2:parametriLogin"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="getAuthenticationConShibbolethResponse">
    <xs:complexContent>
      <xs:extension base="tns:serviceResponse">
        <xs:sequence>
          <xs:element minOccurs="0" ref="ns2:authenticationToken"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="serviceResponse">
    <xs:complexContent>
      <xs:extension base="tns:Ens_Response">
        <xs:sequence>
          <xs:element minOccurs="0" ref="ns2:errori"/>
          <xs:element minOccurs="0" name="esito" type="tns:risultatoCodice"/>
          <xs:element maxOccurs="unbounded" minOccurs="0" ref="ns2:codifiche"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="Ens_Response">
    <xs:complexContent>
      <xs:extension base="tns:Ens_Messagebody">
        <xs:sequence/>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="Ens_Messagebody">
    <xs:sequence/>
  </xs:complexType>
  <xs:complexType name="errori">
    <xs:sequence>
      <xs:element maxOccurs="unbounded" minOccurs="0" ref="ns2:errore"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="Ens_Request">
    <xs:complexContent>
      <xs:extension base="tns:Ens_Messagebody">
        <xs:sequence/>
      </xs:extension>
    </xs:complexContent>
```

```
  </xs:complexType>
  <xs:simpleType name="risultatoCodice">
    <xs:restriction base="xs:string">
      <xs:enumeration value="SUCCESSO"/>
      <xs:enumeration value="FALLIMENTO"/>
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://dmac.csi.it/"
targetNamespace="http://dmac.csi.it/" version="1.0">

  <xs:element name="richiedente" type="tns:richiedente"/>

  <xs:complexType name="richiedente">
    <xs:sequence>
      <xs:element minOccurs="0" name="applicazione" type="xs:string"/>
      <xs:element minOccurs="0" name="codiceFiscaleMedico" type="xs:string"/>
      <xs:element minOccurs="0" name="ipClient" type="xs:string"/>
      <xs:element minOccurs="0" name="ruolo" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>

</xs:schema>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://dma.csi.it/"
xmlns:ns1="http://dmacc.csi.it/" attributeFormDefault="unqualified" elementFormDefault="unqualified"
targetNamespace="http://dma.csi.it/">
  <xs:import namespace="http://dmacc.csi.it/"/>
  <xs:element name="authenticationToken" type="xs:string"/>
  <xs:element name="codiceFiscaleAssistito" type="xs:string"/>
  <xs:element name="codifiche" type="tns:codifica"/>
  <xs:element name="errore" type="tns:errore"/>
  <xs:element name="errori" type="ns1:errori"/>
  <xs:element name="parametriLogin" type="tns:parametriLogin"/>
  <xs:complexType name="parametriLogin">
    <xs:sequence>
      <xs:element minOccurs="0" name="codice" type="xs:string"/>
      <xs:element minOccurs="0" name="valore" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="errore">
    <xs:complexContent>
      <xs:extension base="tns:codifica">
        <xs:sequence/>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
  <xs:complexType name="codifica">
    <xs:sequence>
      <xs:element minOccurs="0" name="codice" type="xs:string"/>
      <xs:element minOccurs="0" name="descrizione" type="xs:string"/>
      <xs:element minOccurs="0" name="riferimento" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://dmacc.csi.it/"
xmlns="http://dmaccbl.csi.it/" attributeFormDefault="unqualified" elementFormDefault="qualified"
targetNamespace="http://dmaccbl.csi.it/">
  <xsd:import namespace="http://dmacc.csi.it/"/>
  <xsd:element name="getAuthenticationConShibbolethRequest" nillable="true"
type="tns:getAuthenticationConShibbolethRequest"/>
</xsd:schema>
  </wsdl:types>
  <wsdl:message name="getAuthenticationConShibbolethResponse">
    <wsdl:part element="tns:getAuthenticationConShibbolethResponse"
name="getAuthenticationConShibbolethResponse">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="getAuthenticationConShibboleth">
    <wsdl:part element="ns1:getAuthenticationConShibbolethRequest"
name="getAuthenticationConShibbolethRequest">
    </wsdl:part>
```

```
  </wsdl:message>
  <wsdl:portType name="AuthenticationConShibbolethService">
    <wsdl:operation name="getAuthenticationConShibboleth">
      <wsdl:input message="tns:getAuthenticationConShibboleth" name="getAuthenticationConShibboleth">
    </wsdl:input>
      <wsdl:output message="tns:getAuthenticationConShibbolethResponse"
name="getAuthenticationConShibbolethResponse">
    </wsdl:output>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="AuthenticationConShibbolethServiceSoapBinding"
type="tns:AuthenticationConShibbolethService">
    <soap12:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="getAuthenticationConShibboleth">
      <soap12:operation soapAction="http://dmaccbl.csi.it/getAuthenticationConShibboleth"
style="document"/>
      <wsdl:input name="getAuthenticationConShibboleth">
        <soap12:body use="literal"/>
      </wsdl:input>
      <wsdl:output name="getAuthenticationConShibbolethResponse">
        <soap12:body use="literal"/>
      </wsdl:output>
    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="AuthenticationConShibbolethService">
    <wsdl:port binding="tns:AuthenticationConShibbolethServiceSoapBinding"
name="AuthenticationConShibbolethService">
      <soap12:address location="https://sg-srv-
lcce.isan.csi.it/lccews/AuthenticationConShibbolethService"/>
    </wsdl:port>
  </wsdl:service>

</wsdl:definitions>
```

8. Processo di autocertificazione

Il fornitore che intende autocertificarsi deve inviare una mail alla casella di posta supporto.fse@csi.it indicando il prodotto per cui desidera effettuare la certificazione e la modalità di integrazione (chiamata di contesto con o senza Shibboleth).

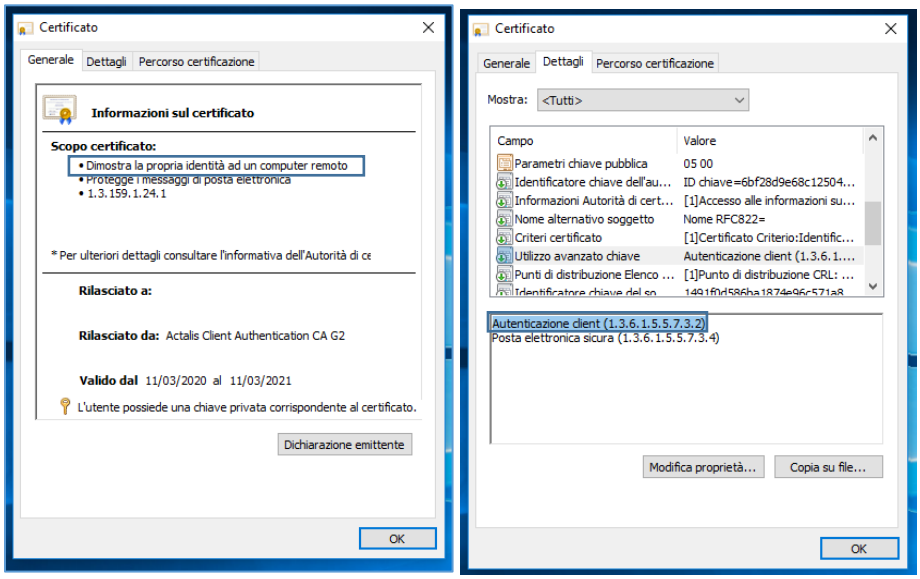
Il CSI fornisce le url di certificazione, il certificato client *demo* che dovrà utilizzare per la fase dei test e di autocertificazione, assieme alle credenziali *di test* da utilizzare per invocare il servizio di getAuthentication e le informazioni anagrafiche dell'assistito e del medico da utilizzare.Tale certificato varrà solo per la fase di test.

Per dimostrare l'avvenuto test di integrazione, il fornitore dovrà quindi produrre un documento in cui indicherà i dati relativi all'autocertificazione come da Facsimile riportati nei capitoli 9 e 10.

Il fornitore dovrà inviare il documento di autocertificazione alle caselle di posta gestione.informatica@regione.piemonte.it e supporto.fse@csi.it per concludere il processo di autocertificazione.

Per l'avvio in produzione il fornitore dovrà dotarsi di un proprio certificato e dovrà fornire al CSI-Piemonte la chiave pubblica al fine di consentire l'abilitazione della CCE.

Il certificato richiesto per l'integrazione dovrà essere stato rilasciato ai fini della "Autenticazione client" o "Client authentication" (1.3.6.1.5.5.7.3.2) emesso da una **Certification Authority accreditata da Agid**; di questa tipologia di certificati fanno parte la CNS, i certificati S/MIME (utilizzati per firmare e/o cifrare i messaggi di posta elettronica), e altri; i certificati idonei si riconoscono in quanto posseggono le seguenti caratteristiche:

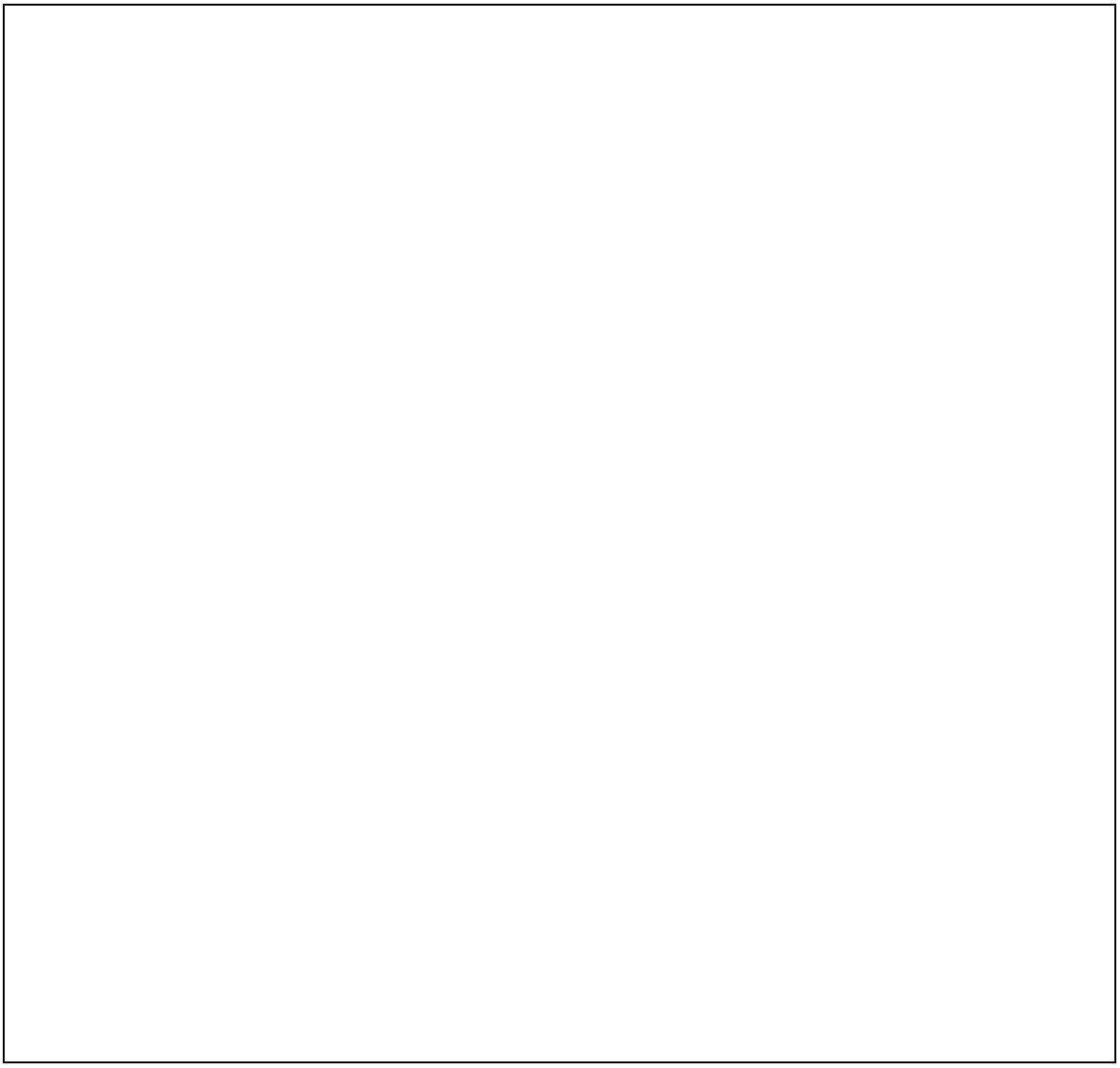


Il CSI-Piemonte fornirà le URL degli ambienti di esercizio per poi procedere con l'avvio del servizio.

Facsimile della dichiarazione di autocertificazione-CHIAMATA DI CONTESTO CON SHIBBOLETH

FORNITORE	**<Inserire nome del fornitore che si sta certificando>**
DATA DI CERTIFICAZIONE:	**<Inserire data di certificazione>**
URL SERVIZIO	https://cert-be-lcce-rupar.isan.csi.it/lccews/AuthenticationConShibbolethService
URL WEB APP	https://cert-med.fsepiemonte.it/dmawa/ecwdmed?tokenLCCE=<token>
CERTIFICATO	**<Inserire codice fiscale del certificato fornito dal CSI in fase di richiesta di certificazione>**
CERTIFICAZIONE	Chiamata di contesto CON Shibboleth

Immagine:



9. Facsimile della dichiarazione di autocertificazione-CHIAMATA DI CONTESTO SENZA SHIBBOLETH

FORNITORE	**<Inserire nome del fornitore che si sta certificando>**
DATA DI CERTIFICAZIONE:	**<Inserire data di certificazione>**
URL SERVIZIO	https://cert-srv-lcce.isan.csi.it/lccews/AuthenticationService
URL WEB APP	https://cert-medtok.fsepiemonte.it/dmawa/lcce?tokenLCCE=<Inserire Token ricevuto>
CERTIFICATO	**<Inserire codice fiscale del certificato fornito dal CSI in fase di richiesta di certificazione>**
CERTIFICAZIONE	Chiamata di contesto SENZA Shibboleth

Immagine: