Termini e condizioni di utilizzo “Specifica Asserzione Applicativa con Certificati” per l’alimentazione del FSE

Sommario

Revisioni

Versione	Stato	Data	Descrizione Modifica
1.0	BOZZA	01/10/2019	Prima versione
2.0	BOZZA	08/11/2019	Seconda versione, dopo discussione collegiale con responsabili S.I. delle Aziende
3.0	FINALE	09/1/2020	Stesura definitiva

Lista acronimi

Acronimo	Descrizione
FSE	Fascicolo Sanitario Elettronico
CNS	Carta Nazionale dei Servizi
TS-CNS	Tessera Sanitaria elettronica - Carta Nazionale dei Servizi
SPID	Sistema Pubblico di Identità Digitale
ITI	IHE IT Infrastructure
PIN	Personal Identification Number
OTP	One Time Password
LDAP	Lightweight Directory Access Protocol
IdP	Identification Provider
CA	Certification Authority
AgId	Agenzia per l'Italia digitale

Quadro generale

Il presente documento definisce le modalità operative e i requisiti minimi che gli applicativi sanitari e l'infrastruttura ICT nell'ambito della quale questi operano, devono possedere al fine di potersi integrare con infrastrutture ospitate presso i datacenter regionali, ed in particolare consentire l'attivazione della modalità di alimentazione del FSE con transazione IHE ITI-41 e IHE ITI-42 basata sull'utilizzo di asserzioni applicative come descritta nel documento "Specifica Asserzione Applicativa con Certificati" (allegato 1) anche pubblicata al link:

https://fse.sanita.marche.it/web/portal/interfacce-al-fse

Tale specifica definisce una modalità di interazione con l'infrastruttura FSE dove, limitatamente alle transazioni IHE ITI-41, IHE ITI-42 e verifica del consenso (al fine dell'eventuale oscuramento) i client installati presso organizzazioni autorizzate e appositamente abilitati e configurati vengono riconosciuti come fonte fidata dei documenti inviati.

Attualmente, tali transazioni vengono in diverse situazioni gestite attraverso l'autenticazione sincrona tramite Cohesion dell'utente che sta richiedendo la transazione e questo crea ritardi nell'operatività, maggiore complessità delle transazioni e possibili rischi di interruzione del servizio in caso di malfunzionamento dell'infrastruttura di autenticazione.

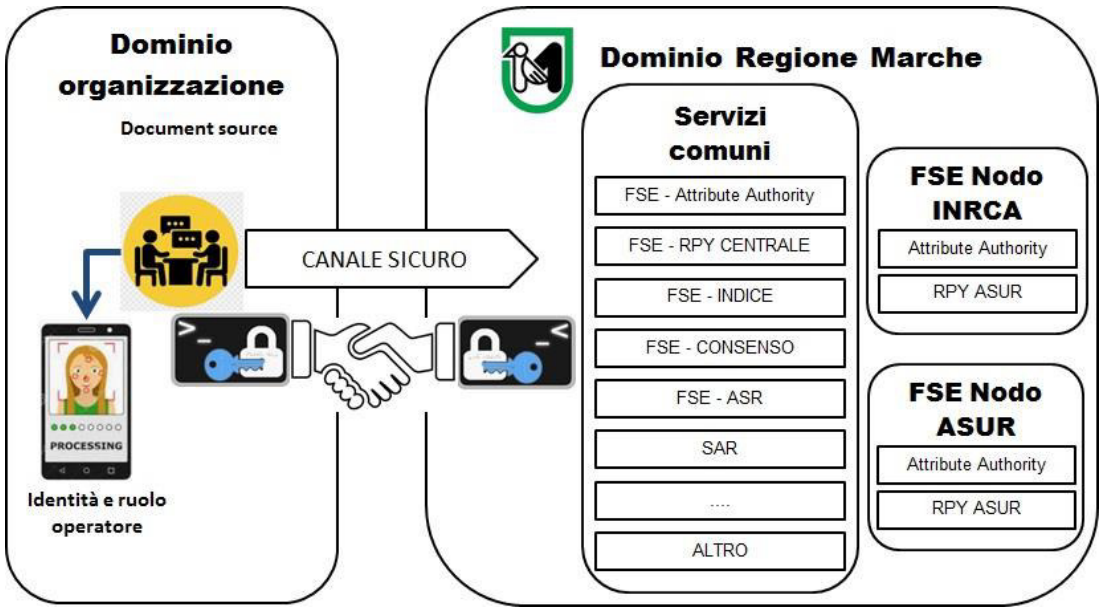
Nello scenario oggetto del presente documento, che potrebbe comunque essere replicabile anche in ambiti diversi dal FSE, vengono invece delegate ai client stessi le seguenti attività:

a) identificazione dell'operatore sanitario che esegue l'invio di uno o più documenti all'infrastruttura FSE;

b) verifica del ruolo dell'operatore sanitario identificato al punto a) e della sua compatibilità con l'esecuzione di una richiesta di transazione IHE ITI-41 o ITI-42, o di eventuali altre.

Tali operazioni ricadono quindi interamente sotto l'ambito di controllo e responsabilità dell'organizzazione che richiede l'integrazione dei propri applicativi con ruolo "document-source". Dove per organizzazione si intende: Azienda sanitaria, struttura convenzionata o qualsiasi altro ente con personalità giuridica autonoma rispetto alla Regione Marche.

L'infrastruttura regionale si limita ad offrire un canale di comunicazione sicuro con gli applicativi client, non potendo in alcun modo entrare nel merito delle operazioni di cui ai punti a) e b), in quanto queste restano tecnicamente al di fuori del suo ambito di controllo come schematizzato nella seguente figura.



Le modalità di integrazione descritte nel presente documento NON devono essere adottate in tutti gli scenari in cui gli applicativi delle aziende sanitarie operano in qualità di document consumer, come ad esempio nel caso di accesso ad un FSE per il recupero di un referto. In tali casi rimangono ferme le modalità di integrazione basate sullo scambio di token SAML 2.0 SSO.

Requisiti minimi client

Al fine di mantenere un elevato livello di sicurezza potranno essere integrati con la modalità di cui al documento "Specifica Asserzione Applicativa con Certificati" i soli applicativi per i quali l'organizzazione richiedente è in grado di assicurare il rispetto delle seguenti condizioni.

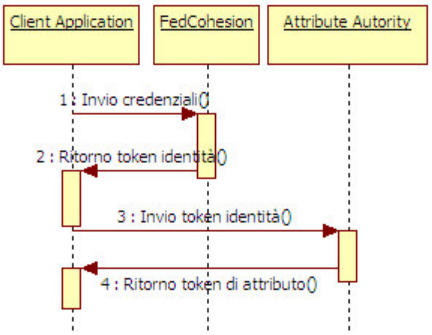
1. Ogni credenziale di identificazione degli operatori sanitari è concessa ad uso personale ed esclusivo di un'unica persona fisica e non è ammessa la condivisione di credenziali da parte di più soggetti.
2. L'autenticazione dell'operatore sanitario deve essere eseguita dal client utilizzando meccanismi che garantiscano la sua identificazione certa. Sono pertanto ammissibili:
   2.1. le modalità di autenticazione di all'art. 64 del Dlgs 82/2005 ovvero: SPID, TS-CNS, CNS, CIE;
   2.2. il sistema regionale di autenticazione FedCohesion, limitatamente alle sole modalità che prevedono l'autenticazione "de visu" del soggetto ovvero: PIN, OTP, CNS, CIE;
   2.3. altri IdP posti in federazione con FedCohesion;
   2.4. sistemi di directory aziendali (Active Directory, LDAP, ecc.) purché la procedura di rilascio delle credenziali preveda il riconoscimento del soggetto "de visu", eventualmente non estesa a tutti i dipendenti aziendali, ma anche limitata ai i soli soggetti abilitati all'utilizzo degli applicativi effettivamente oggetto di integrazione con l'infrastruttura regionale. A titolo di esempio nel caso di integrazione di un applicativo della radiologia, il censimento de visu potrebbe essere limitato a tutti e soli i soggetti abilitati all'utilizzo del software di radiologia e nello specifico alle funzionalità effettivamente integrate tramite asserzione applicativa con l'infrastruttura regionale.
   2.5. sistemi di autenticazione locali all'Azienda purché il processo di rilascio di credenziali preveda il riconoscimento "de visu" almeno per i soli soggetti abilitati all'utilizzo degli applicativi

effettivamente oggetto di integrazione con l'infrastruttura regionale e purché tecnologicamente la soluzione garantisca una sicurezza almeno pari a quella del punto precedente rispettando almeno le regole prescritte negli art. 1-15 dell'allegato B del D.Lgs. 196/03 "Disciplinare tecnico in materia di misure minime di sicurezza", anche se abrogato.

2.6. altri sistemi di autenticazione che prevedano il rilascio di credenziali previo riconoscimento "de visu" del soggetto almeno per i soli soggetti abilitati all'utilizzo degli applicativi effettivamente oggetto di integrazione con l'infrastruttura regionale e che tecnologicamente assicurino almeno:
   - l'impossibilità di eseguire un furto delle credenziali anche accedendo al database di protezione con diritti amministrativi (es. criptazione dei dati memorizzati nel DB ecc.)
   - l'adozione di algoritmi per lo scambio delle credenziali con gli applicativi client tali da impedirne l'intercettazione da parte di eventuali terzi in grado di spiare il traffico di rete (es. utilizzo di canali di trasmissione protetti, adozione di algoritmi challenge/response, utilizzo sistemi di autenticazione a più fattori ecc.)
   - la possibilità di imporre policy di complessità tese a garantire un elevato grado di sicurezza delle credenziali (lunghezze minima password, tipo di caratteri utilizzati ecc.)
   - la possibilità di imporre la modifica delle credenziali con frequenza almeno trimestrale e di impedirne il riutilizzo nei 12 mesi successivi.

3. La verifica del ruolo dell'utente può essere eseguita:
   3.1. utilizzando l'interfaccia esposta dall'infrastruttura FSE per l'interrogazione dell'Attribute Authority di riferimento per il servizio richiesto;
   3.2. verificando il ruolo dell'utente su sistemi aziendali (Active Directory, LDAP ecc.), purché sia garantita la disattivazione tempestiva dei soggetti cessati e/o decaduti dal ruolo.
4. Devono essere in ogni caso rispettati i requisiti minimi di sicurezza previsti nella circolare AgID n. 2 18/4/2017 pubblicata sulla Gazzetta Ufficiale della Repubblica Italina serie generale n. 103 del 15/5/2017

In assenza di tali requisiti la modalità di integrazione tra gli applicativi e l'infrastruttura FSE, specificatamente per il ruolo document-source, dovrà necessariamente essere realizzata nella modalità SAML 2.0 SSO come da specifiche previste dal documento "Progetto esecutivo di dettaglio" al paragrafo 2.3.1. pubblicato al link: https://fse.sanita.marche.it/web/portal/interfacce-al-fse di cui si riporta qui lo schema logico del sistema di autenticazione e determinazione del ruolo.



Modalità abilitazione client

La sicurezza del canale offerto si basa sulla distribuzione ai client autorizzati di certificati digitali emessi dalla CA della Regione Marche e della relativa chiave segreta privata.

Qualora un'azienda sanitaria intenda integrare con l'infrastruttura FSE uno o più dei propri sistemi secondo la modalità di cui al documento "Specifica Asserzione Applicativa con Certificati" (Allegato 1) dovrà:

a) inoltrare al Servizio sanità della Regione Marche formale richiesta per il rilascio di uno o più certificati X.509 per la messa in sicurezza di Web-Service (Allegato 2);
b) inoltrare al Servizio sanità della Regione Marche formale richiesta di abilitazione del o degli applicativi di cui si richiede l'integrazione.

La richiesta di cui al punto a) dovrà essere inviata per ogni certificato richiesto, e successivamente dovrà essere reiterata nel momento in cui si renderà necessaria la sostituzione del certificato X.509, quando questo sia giunto in prossimità della sua scadenza. Si lascia libertà all'Azienda di scegliere se adottare un

certificato unico “aziendale” per tutti i servizi in cui l’Azienda è coinvolta o un certificato per ogni servizio (o gruppo di servizi).

La richiesta di cui al punto b) dovrà essere formalizzata per tutti gli applicativi che l’azienda sanitaria ha necessità di integrare con l’infrastruttura FSE secondo la modalità di cui al documento “Specifica Asserzione Applicativa con Certificati”, e potrà pertanto essere reiterata più volte nel corso del tempo quando si presenti la necessità di abilitare nuovi applicativi.

Tale richiesta ha tra l’altro lo scopo di consentire l’attivazione del necessario supporto tecnico per eseguire i test di integrazione e la validazione della stessa. Potranno essere integrati i soli applicativi espressamente autorizzati dal Servizio sanità della Regione Marche che abbiano superato positivamente i test di validazione.

L’azienda sanitaria che detiene il certificato X.509 dovrà:

- provvedere alla richiesta di emissione di un nuovo certificato almeno 60 giorni prima della sua scadenza al fine di evitare il rischio di interruzioni del servizio;
- custodire la chiave privata del certificato ricevuto in luogo sicuro ed evitarne la diffusione a terzi non autorizzati;
- limitare la distribuzione del certificato e della sua chiave privata ai soli soggetti incaricati della gestione degli applicativi autorizzati dal Servizio sanità della Regione Marche secondo le modalità di cui al punto b).

Allegato 1 – Specifica Asserzione Applicativa con Certificati

Specifiche Asserzione Applicativa con Certificati

Sommario

Obiettivo del documento.

Il presente documento intende definire le specifiche del flusso di integrazione tra i diversi applicativi client per l'invio dei referti con transazione ITI-41 verso FSE usando asserzioni auto-generate.
Ogni richiesta di servizi eseguita da uno specifico client deve necessariamente essere corredata da un'asserzione d'identità (strutturata attraverso lo standard OASIS SAML 2.0)

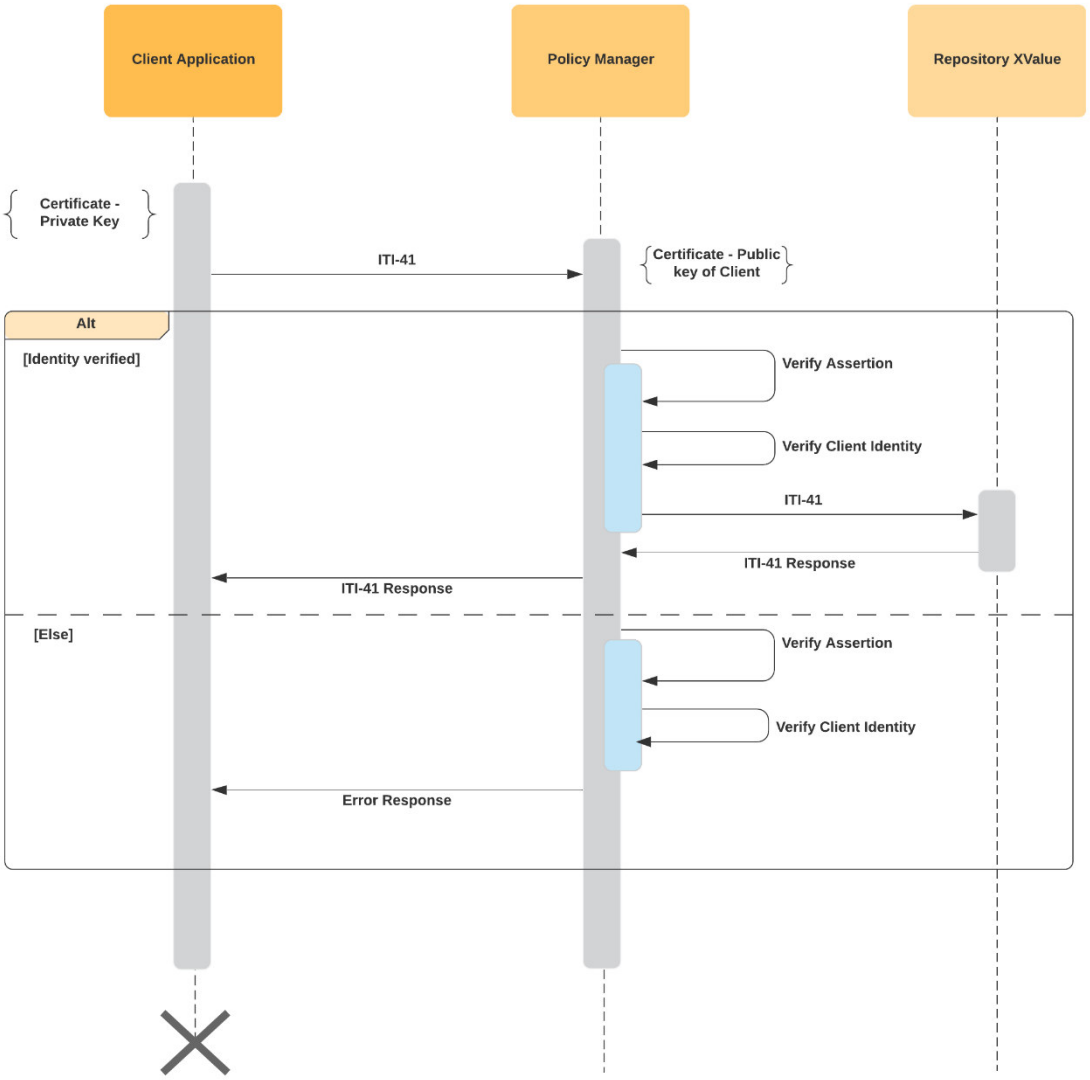
Il presente documento intende inoltre definire le specifiche della struttura di una asserzione d'identità gestita dalla piattaforma XVALUE per il progetto FSE-MARCHE.

Flusso operativo e diagramma.

Le interazioni con i servizi esposti dalla piattaforma prevedono la presenza di asserzioni di identità nei messaggi di richiesta.

Nel contesto di riferimento, si prevede che ogni applicativo client venga dotato di certificato digitale, compresa chiave privata, per poter auto-generare e firmare l'asserzione SAML 2.0 da inserire nei messaggi soap ITI-41 per inviare documenti verso il fascicolo.

La relativa chiave pubblica di ogni client verrà configurata sulla piattaforma XVALUE per poter eseguire la verifica dell'asserzione e della autorizzazione ad effettuare la chiamata al servizio. (vedere paragrafo "Attivazione applicativo inviante").



Specifiche busta SOAP.

Il messaggio creato dovrà essere un messaggio SOAP 1.2 e quindi rispettare lo schema definito da http://www.w3.org/2003/05/soap-envelope.
La struttura dell'header deve essere conforme alle specifiche WS-Addressing 1.0 SOAP Binding permettendo il corretto instradamento e processamento del messaggio di richiesta.

- <wsa:To> = indirizzo URI del destinatario ultimo del messaggio.
- <wsa:Action> = URI che identifica la semantica attesa nel body.
- <wsa:MessageID> = identificativo univoco del messaggio.

Inoltre l'header del messaggio SOAP deve anche contenere un elemento che permette di identificare l'inviante. Questa porzione è strutturata mediante l'utilizzo dello standard WS-Security contenente l'asserzione di identità. Per le specifiche della asserzione SAML 2.0 vedere documento Specifiche asserzione SAML.

Esempio di busta SOAP.

```
<?xml version="1.0" encoding="utf-8"?>
<soapenv:Envelope xmlns:soapenv="http://www.w3.org/2003/05/soap-envelope">
   <soapenv:Header xmlns:wsa="http://www.w3.org/2005/08/addressing">
      <wsse:Security
         xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
         soapenv:mustUnderstand="true">
         <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
            xmlns:xs="http://www.w3.org/2001/XMLSchema"
ID="_aa6826879ad6b65028fc97c4b215e4ba"
            IssueInstant="2019-07-17T10:07:28.408Z" Version="2.0">
            <saml2:Issuer>clientID</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/2000/09/xmldsig#rsa-sha1"/>
                  <ds:Reference URI="#_aa6826879ad6b65028fc97c4b215e4ba">
                     <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
                            xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                            PrefixList="xs"/>
                        </ds:Transform>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <ds:DigestValue>hokC/eyr5J/8IAVoYO6935uyWok=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>atN...</ds:SignatureValue>
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>MIID...</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </ds:Signature>
        <saml2:Subject>
            <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName"
                >clientID</saml2:NameID>
            <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"
            />
        </saml2:Subject>
        <saml2:Conditions NotBefore="2019-07-17T10:07:28.408Z"
            NotOnOrAfter="2019-07-17T12:54:08.408Z"/>
    </saml2:Assertion>
</wsse:Security>


<wsa:To>http://${application.server}/DocumentRepository_ProvideAndRegisterDocumentSet</wsa:To>
    <wsa:MessageID>urn:uuid:98a7f8f9-de9e-418a-ba88-530633f80f1f</wsa:MessageID>
    <wsa:Action>urn:ihe:iti:2007:ProvideAndRegisterDocumentSet-b</wsa:Action>
</soapenv:Header>
<soapenv:Body>
    <ns4:ProvideAndRegisterDocumentSetRequest
        xmlns="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0" xmlns:ns2="urn:oasis:names:tc:ebxml-
regrep:xsd:rs:3.0"
```

```
        xmlns:ns3="urn:oasis:names:tc:ebxml-regrep:xsd:lcm:3.0"
        xmlns:ns4="urn:ihe:iti:xds-b:2007" xmlns:ns5="urn:oasis:names:tc:ebxml-
regrep:xsd:query:3.0">

        ...
    </ns4:ProvideAndRegisterDocumentSetRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Attivazione applicativo inviante.

Nel momento in cui un applicativo necessiti di utilizzare i servizi esposti secondo le modalità descritte, devono essere eseguite le seguenti azioni:

1. Produzione di nuovo certificato con chiave privata dedicata.
   La gestione dei certificati viene eseguita dalla regione MARCHE utilizzando certificati rilasciati dalla sua certification authority.
2. Rilascio chiave privata ad applicativo client e configurazione chiave pubblica sulla piattaforma XVALUE all'interno della componente del Policy Manager.
3. Creazione clientID associato al certificato creato e configurazione su XVALUE.

Struttura Asserzione di Identità.

L'asserzione rispecchia le specifiche OASIS SAML 2.0. Di seguito i dettagli previsti nel contesto di riferimento.

L'elemento **<saml2:Assertion>** deve contenere i seguenti attributi:

- **Version**: deve essere "2.0"
- **ID**: identificativo univoco dell'asserzione creata
- **IssueInstant**: istante temporale in cui è stata creata l'asserzione

L'elemento <saml2:Assertion> contiene i seguenti elementi:

- **<saml2:Issuer>**: elemento obbligatorio che descrive il creatore dell'Asserzione. Deve essere valorizzato con il codice assegnato all'applicativo inviante (vedere paragrafo "Attivazione applicativo inviante" nel documento Specifiche flusso FSE)
- **<ds:Signature>**: questo elemento è obbligatorio e permette di firmare l'asserzione con un XML signature autenticando l'attore inviante. Questa firma è eseguita in accordo alle specifiche definite dal namespace ds: "http://www.w3.org/2000/09/xmldsig#".

  L'elemento **<ds:Signature>** deve contenere gli elementi **<ds:SignedInfo>** ,

  <ds:SignatureValue> e **<ds:KeyInfo>**.

- Il primo elemento, <ds:SignedInfo>, permette di definire i parametri dell'algoritmo di firma utilizzato, attraverso i seguenti elementi obbligtori:
  - **<ds:CanonicalizationMethod>**: l'attributo Algorithm contiene la definizione dell'algoritmo di canonicalizzazione. Un applicativo conforme a SAML 2.0 dovrebbe utilizzare un algoritmo di canonicalizzazione esclusiva [Excl-C14N] definita dal seguente uri "http://www.w3.org/2001/10/xml-exc-c14n#".
  - - **<ds:SignatureMethod>**: l'attributo Algorithm contiene la definizione dell'algoritmo di firma utilizzato (XML Signature con utilizzo di algoritmo RSA): "http://www.w3.org/2000/09/xmldsig#rsa-sha1"
  - - **<ds:Reference>**: deve essere unico e deve contenere l'attributo URI che fa riferimento all'attributo Assertion/@ID contenuto nell'asserzione preceduto da "#". Questo elemento deve contenere i seguenti elementi:
    - **<ds:DigestMethod>**: l'attributo Algorithm contiene la definizione dell'algoritmo utilizzato per creare il Digest. Deve essere "http://www.w3.org/2000/09/xmldsig#sha1"
    - **<ds:DigestValue>**: questo elemento contiene il valore del Digest in formato base64

  Il secondo elemento, <ds:SignatureValue>, veicola la firma dell'asserzione in formato base64.

  Il terzo elemento, <ds:keyInfo> contiene la chiave pubblica del certificato usato per la firma. Al suo interno conterrà i tag <ds:X509Data> e <ds:X509Certificate> valorizzato con la chiave pubblica

- **<saml2:Subject>**: questo elemento deve essere presente e contiene le informazioni del soggetto dell'asserzione:
  - **<NameID>**:deve contenere identificativo applicativo (vedere paragrafo "Attivazione applicativo inviante" nel documento Specifiche flusso FSE)
  - **<SubjectConfirmation>**: deve contenere attributo "Method" valorizzato con "urn:oasis:names:tc:SAML:2.0:cm:bearer"
- **<saml2:Conditions>**: definisce le condizioni di validità dell'asserzione. Deve avere valorizzati i seguenti attributi:

- **NotBefore** : istante di inizio della validità dell'asserzione
- **NotOnOrAfter** : istante di fine validità dell'asserzione

- **<saml2:AuthnStatment>**:Nel contesto di auto-creazione di asserzioni non è obbligatorio: Se presente, deve contenere i seguenti attributi:
  - **AuthnInstant** : istante dell'avvenuta autenticazione
  - **SessionIndex**: id univoco della sessione di autenticazione
  - **SessionNotOnOrAfter**: durata validità dell'autenticazione

    Deve contenere i seguenti elementi

  - **<saml2:AuthnContext>:** indica il contesto di autenticazione e deve contenere l'elemento <**saml2:AuthnContextClassRef>** specificando il metodo di autenticazione *"urn:oasis:names:tc:SAML:2.0:ac:classes:X509"*
- **<saml2:AttributeStatment>**: sezione che permette di veicolare gli attributi dell'asserzione che sono associati all'applicativo inviante. Ad oggi non sono previsti attributi da usare nel contesto di riferimento.

L'asserzione d'identità ottenuta deve essere veicolata all'interno dei messaggi di richiesta di servizi del Fascicolo Sanitario Elettronico regionale.

Esempio di Asserzione di Identità.

```
<saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
ID="_177b1adea89803d8daa7f4a5a7ad6ed8"
        IssueInstant="2019-07-17T13:44:24.824Z" Version="2.0">
        <saml2:Issuer>clientID</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/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#_177b1adea89803d8daa7f4a5a7ad6ed8">
              <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
                    xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
                    PrefixList="xs"/>
                </ds:Transform>
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <ds:DigestValue>yn2brLN0VGeeVivFblz0ituodx4=</ds:DigestValue>
            </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>SUa...</ds:SignatureValue>
          <ds:KeyInfo>
            <ds:X509Data>
              <ds:X509Certificate>MII...</ds:X509Certificate>
            </ds:X509Data>
          </ds:KeyInfo>
        </ds:Signature>
        <saml2:Subject>
          <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName"
            >clientID</saml2:NameID>
          <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"/>
```

```
            </saml2:Subject>
            <saml2:Conditions NotBefore="2019-07-17T13:44:24.824Z"
               NotOnOrAfter="2019-07-17T16:31:04.824Z"/>
            <saml2:AuthnStatement AuthnInstant="2019-07-17T13:44:24.846Z"
               SessionIndex="x1v1-sts-2.0-session__622e55971d6c301067c5420ce59e83b8"
               SessionNotOnOrAfter="2019-07-17T14:01:04.846Z">
               <saml2:AuthnContext>

<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:X509</saml2:AuthnContextCla
ssRef>
               </saml2:AuthnContext>
            </saml2:AuthnStatement>
         </saml2:Assertion>
```

Allegato 2 – FAC simile Richiesta certificato X.509 per la messa in sicurezza di Web-Service

Al Servizio sanità della Regione Marche

Oggetto: richiesta rilascio di n. … certificati X.509 finalizzati all'integrazione applicativa di applicativi sanitari con l'infrastruttura FSE per l'invio di referti con transazione ITI-41 e ITI-42

Il sottoscritto

Nome_____ Cognome_____ per conto di

- ☐ Azienda Ospedaliera Ospedali Riunti Marche Nord
- ☐ Azienda Ospedaliera Universitaria ospedali riuniti di Ancona
- ☐ Azienda Sanitaria Unica Regionale
- ☐ INRCA - Istituto di Ricovero e Cura a Carattere Scientifico
- ☐ Altro: _____

richiede il rilascio di n. … certificati X.509 per i fini di cui in oggetto così configurato

Parametro	**Valore**
Name:	
E-mail:	
Company:	
Department:	
City:	
State:	
Country:	
Durata: (max 4 anni)	

Per i seguenti applicativi:

#	**Applicativo**
1	
2	
3	
4	
5	

Si richiede la consegna del file .pfx contenente certificato X.509 con la relativa chiave privata protetta da password all'indirizzo E-Mail _____ e la consegna della password per l'estrazione della chiave privata mediante SMS al n. Tel _____.

Il sottoscritto dichiara di avere ricevuto il documento "Termini e condizioni di utilizzo Specifica Asserzione Applicativa con Certificati" per l'alimentazione del FSE" e impegna l'organizzazione da me rappresentata al rispetto della stessa.

Il Rappresentante legale della organizzazione