

Progetto

Sistema **INFO**rmativo Sa**N**ità Campan**IA** (**SINFONIA**)



Specifiche delle misure di sicurezza dei servizi esposti

Versione 2.0

16 Aprile 2020

DIRITTI DI AUTORE E CLAUSOLE DI RISERVATEZZA

La proprietà del presente documento è regolata dal contratto tra So.Re.Sa. ed il RTI SGI_Consip. Tutti i diritti sono riservati.

A norma della legge sul diritto di autore e del Codice Civile è vietata la riproduzione di questo scritto o di parte di esso con qualsiasi mezzo elettronico, meccanico, per mezzo di fotocopie, microfilm, registratori ed altro, salvo per quanto espressamente autorizzato.

CONTROLLO DELLA CONFIGURAZIONE

Titolo: Specifiche delle misure di sicurezza dei servizi esposti

Riferimento: Specifiche delle misure di sicurezza dei servizi esposti.doc

Storia del Documento

Ver	Stato	Chi	Data	Memorizzato in:
1.00	Bozza	PF	10/12/2019	Specifiche delle misure di sicurezza dei servizi esposti.doc

Storia delle Revisioni

Ver	Modifiche
2.00	Rev. Versione iniziale.

Modifiche Previste

Nessuna.

Tabella Redazione/Approvazione

Responsabile redazione	Responsabile approvazione
Exprivia	Regione Campania

INDICE DEI CONTENUTI

0. Introduzione	4
1. Scopo e Campo di Applicazione	4
2. Termini e definizioni	4
3. Scenari di riferimento per la cooperazione applicativa	4
4. Prerequisiti per l'integrazione.....	5
5. Identificazione, autenticazione ed autorizzazione dei sistemi fruitori	5
5.1. Identificazione ed autenticazione del Sistema Fruitore.....	6
5.2. Identità dell'utente del sistema fruitore	6
5.3. Autorizzazione del Sistema Fruitore	7
5.4. Autorizzazione dell'utente del Sistema Fruitore.....	7
5.5. Esempio di SOAP request con firma dei tag	8
6. Firma dei messaggi di risposta	10
7. Rilascio credenziali applicative.....	12

0. Introduzione

Questo documento descrive le specifiche delle misure di sicurezza dei servizi esposti nell'ambito delle aree applicative del sistema Sinfonia. Il documento specifica i prerequisiti per l'integrazione e le modalità con cui il sistema Sinfonia provvede a verificare l'identità dell'applicativo, autenticarlo ed autorizzarlo all'utilizzo dei servizi.

1. Scopo e Campo di Applicazione

Il presente documento è destinato a progettisti e sviluppatori dei sistemi informativi che devono integrarsi con il sistema Sinfonia. Costituisce quindi la specifica di riferimento per l'integrazione dei servizi per quanto attiene alle problematiche riguardanti l'identificazione, l'autenticazione e l'autenticazione.

2. Termini e definizioni

Sistema Fruitore: sistema informativo cooperante con il sistema Sinfonia che fruisce dei servizi esposti da quest'ultimo secondo le modalità concordate e conformemente alle specifiche tecniche di integrazione.

Sistema Erogatore: sistema informativo che espone servizi (in modalità web service secondo standard SOAP) da poter essere invocati da un sistema fruitore per portare a compimento specifici obiettivi di cooperazione applicativa tra sistemi.

Scenario di Integrazione: descrizione dettagliata delle modalità con cui un sistema fruitore interagisce con un sistema erogatore per portare a compimento specifici obiettivi di cooperazione applicativa.

3. Scenari di riferimento per la cooperazione applicativa

In quanto erogatore di servizi, il sistema Sinfonia espone ciascun servizio in modalità web service secondo lo standard SOAP. Questa modalità copre eventuali casi specifici di interazione tra area applicativa e sistema cooperante, modalità che sarà concordata, di volta in volta, per ciascun sistema fruitore tra RTI, Regione Campania ed organizzazione di riferimento del sistema fruitore.

4. Prerequisiti per l'integrazione

L'integrazione dei servizi di Sinfonia da parte di un sistema terzo richiede la preliminare autorizzazione all'integrazione da parte della Regione Campania.

Tale autorizzazione avviene a seguito di verifica della rispondenza tecnica e funzionale del sistema terzo a un insieme di requisiti che sono definiti dalla Regione Campania.

Successivamente alla verifica e all'autorizzazione il soggetto che effettua la conduzione tecnica del sistema Sinfonia provvede a censire il sistema terzo nell'archivio dei sistemi fruitori.

Rientra tra le responsabilità del sistema terzo l'identificazione, l'autenticazione e l'autorizzazione dei suoi stessi utenti.

Rientra tra le responsabilità del sistema Sinfonia l'identificazione e l'autenticazione del sistema terzo.

5. Identificazione, autenticazione ed autorizzazione dei sistemi fruitori

Di seguito è illustrato il processo complessivo di interazione tra sistemi cooperanti, evidenziando le modalità di identificazione, autenticazione e autorizzazione, applicate dal sistema Sinfonia. Per Sistema Erogatore si intende, in questo specifico contesto, la generica istanza Sinfonia.

1. Il Sistema Erogatore riceve un messaggio SOAP contenente il certificato X.509v3 del Sistema Fruitore in conformità alla specifica "X.509 Certificate Token Profile" fornito da WS-Security. L'integrità del messaggio è garantita dalla firma digitale apposta con certificato X.509v3.
2. Il Sistema Erogatore verifica l'integrità sintattica del messaggio verificando la rispondenza all'xsd. In particolare viene estratto dal messaggio di input il token X.509v3, rappresentante il Sistema Fruitore. Successivamente si applicano tutti i controlli necessari a verificare la validità del certificato. Ottenuta la validazione del certificato, il Sistema Erogatore accerta la validità dell'identità del Sistema Fruitore interfacciandosi con i servizi esposti dalla propria Anagrafica Sistemi Fruitori. In particolare il Sistema Erogatore verifica che il common-name del certificato X.509v3 risulti presente ed abilitato nell'Anagrafe dei Sistemi Fruitori autorizzati ad interagire con il Sistema Erogatore.
3. Il Sistema Erogatore, superati tutti i controlli del passo precedente ed in conformità con quanto definito nei successivi paragrafi relativi all'autorizzazione per i servizi di cooperazione, provvede ad erogare il servizio richiesto.
4. Il Sistema Erogatore accerta la conformità della richiesta applicativa rispetto alle eventuali politiche di sicurezza aggiuntive specifiche del servizio applicativo richiesto.
5. Il messaggio SOAP di response inviato al Sistema Fruitore soddisferà, analogamente al messaggio SOAP di request, la specifica "X.509 Certificate Token Profile" fornito WS-Security.

Si faccia riferimento all'appendice A per i messaggi applicativi restituiti dai servizi in corrispondenza delle eccezioni derivanti da controlli preliminari all'esecuzione del servizio e riguardanti:

- validità sintattica della richiesta
- validità del certificato
- validità della firma digitale del messaggio
- corretta identità del sistema fruitore
- autorizzazione del sistema fruitore all'esecuzione del servizio
- autorizzazione del ruolo dell'utente finale all'esecuzione del servizio.

5.1. Identificazione ed autenticazione del Sistema Fruitore

L'identificazione e l'autenticazione del Sistema Fruitore è basata sull'utilizzo del certificato X.509v3 di autenticazione del Sistema Fruitore, secondo lo standard Web Services Security X.509 *Certificate Token Profile* (<http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-x509TokenProfile.pdf>).

L'identificazione del sistema fruitore deve individuare in modo univoco e certo lo specifico sistema che sta invocando il servizio esposto.

Ne consegue che ogni sistema fruitore, sia interdominio che intradominio, deve essere dotato di un certificato X.509v3 il cui *commonname* deve essere preliminarmente censito nell'anagrafe dei certificati X.509v3 associati ai sistemi fruitori ed autorizzati ad interagire con il sistema erogatore.

Come da standard WS-Security, il certificato di autenticazione X.509v3 sarà utilizzato per la firma dei seguenti tag della SOAP request:

- il tag <Timestamp>, previsto nell'header del messaggio SOAP;
- il tag <To>, previsto nell'header del messaggio SOAP;
- il tag <Action>, previsto nell'header del messaggio SOAP;
- il tag <MessageID>, previsto nell'header del messaggio SOAP;
- il tag <ReplyTo>, previsto nell'header del messaggio SOAP;
- il tag <AttributiAutorizzativi>, presente nell'header del messaggio SOAP;
- il tag del contenuto applicativo, primo ed unico figlio del tag <Body>.

Le policy di sicurezza sono formalmente definite nel *wsdl* dello specifico servizio.

5.2. Identità dell'utente del sistema fruitore

L'individuazione dell'identità dell'utente del sistema fruitore è una responsabilità del sistema fruitore, il sistema erogatore non dispone quindi dell'elenco delle identità degli utenti finali dei sistemi fruitori e “*si fida*”, dell'identificazione, dell'autenticazione dell'utente eseguita dal sistema fruitore e dell'autorizzazione all'invocazione del servizio esposto.

L'identità dell'utente è rappresentata, nella richiesta di servizio, tramite un identificativo significativo per il sistema fruitore che consenta allo stesso sistema fruitore, in caso di necessità, di risalire all'identità reale dell'utente finale. **È raccomandabile l'utilizzo del codice fiscale.**

L'identità dell'utente è presente in ogni richiesta di servizio, negli attributi autorizzativi presenti nell'header del messaggio (tag <IdentificativoUtente>), ed è utilizzata dal sistema Sinfonia per fini di tracciamento delle operazioni e, quando necessario, per finalità legate allo specifico servizio applicativo richiesto.

5.3. Autorizzazione del Sistema Fruitore

Il Sistema Erogatore dopo aver autenticato e identificato il Sistema Fruitore verifica che quest'ultimo sia abilitato ad interrogare lo specifico web services invocato.

5.4. Autorizzazione dell'utente del Sistema Fruitore

Tale autorizzazione si avvale di una struttura dati denominata <AttributiAutorizzativi>, presente nell'header del messaggio SOAP, che contiene un gruppo fisso minimo di attributi.

La struttura <AttributiAutorizzativi> risulta così definita:

```
<AttributiAutorizzativi>
  <IdentificativoServizio/>
  <IdentificativoUtente/>
  <RuoloIstituzionale/>
</AttributiAutorizzativi>
```

Ove:

IdentificativoServizio	Nome del servizio invocato.
IdentificativoUtente	Identificatore dell'utente finale la cui attività ha determinato l'invocazione del servizio esposto.
RuoloIstituzionale	Ruolo istituzionale dell'utente finale.

La struttura è firmata con il certificato X.509v3 del sistema fruitore per garantire l'integrità e il non ripudio delle informazioni sulla cui base si attua il processo autorizzativo.

In particolare il processo autorizzativo verifica che il ruolo istituzionale posseduto dall'utente, così come asserito dal sistema fruitore, possa invocare il servizio. In altri termini il Sistema Erogatore verifica che la coppia servizio – ruolo operativo(i) sia abilitata, dove ruolo operativo(i) sia uno dei ruoli operativi definiti a partire dal ruolo istituzionale dichiarato dal Sistema Fruitore. Il processo di risoluzione del ruolo Istituzionale in più ruoli Operativi è a carico del Sistema Erogatore.


```

</ds:Reference>
<ds:Reference URI="#tagTo">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:Digest Value>Q1s9I9dzz2pfxe9io0BH6KvJOc4=</ds:Digest Value>
</ds:Reference>
<ds:Reference URI="#tagAction">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:Digest Value>Fmsi0ui26BejuoZ2SRA5s2Ak4z8=</ds:Digest Value>
</ds:Reference>
<ds:Reference URI="#tagMessageID">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:Digest Value>+d8jqITYjJdZ1PsFIHTtar49Uhg=</ds:Digest Value>
</ds:Reference>
<ds:Reference URI="#tagReplyTo">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:Digest Value>3HcZSaCHA004zv6Z2j8POICda6w=</ds:Digest Value>
</ds:Reference>
<ds:Reference URI="#body">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:Digest Value>V7WUv9kIv74ZNnJu5R0RA577+eQ=</ds:Digest Value>
</ds:Reference>
<ds:Reference URI="#wsTime">
  <ds:Transforms>
    <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
  </ds:Transforms>
  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
  <ds:Digest Value>mhq/MJRUYel9NKXFsB9nXJFzyw8=</ds:Digest Value>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
  IPCa85v7dTkec3m++heCIRXEJOnJWNqA0SPnSFJEbAZZ07oiFvvsCbUhNwP22ax1740OhNeig6lX
  /XU7+I6MBn2alqUgFy0IwxNoQ0eTUvdOyU7xZxlwfaq7OLNnmRAsn4AYXYIJDD1KwsykWqn30S
  wt/ErQIRt8UPoEEjXVY=
</ds:SignatureValue>
<ds:KeyInfo>
  <wsse:SecurityTokenReference>
    <wsse:Reference URI="#X509TokenRef" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
    1.0#X509v3"/>
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</S:Header>
<S:Body>
  <ns2:getAssistibileInAnagrafe xmlns:ns2="http://www.sinfonia.campania.it/Schemas/" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-
  200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="body">
    <request>
      <codAssistito>XXXDNTXXXXXXXXXX</codAssistito>
      <dataRiferimento>01/03/2020</dataRiferimento>
    </request>
  </ns2:getAssistibileInAnagrafe>
</S:Body>
</S:Envelope>

```



```
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>8SY6Wz36TUIZtY+31Z5EpESs5JM=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#_5004">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<exc14n:InclusiveNamespaces PrefixList="S" />
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>IDdfAZSNa587HfNFS9x+7jJN9I=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#_5005">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<exc14n:InclusiveNamespaces PrefixList="S" />
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>otFO7dNipmHNQZAqdbUnn1PLA3g=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#_5006">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<exc14n:InclusiveNamespaces PrefixList="S" />
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>2HiAPPmFg/v9b0zyZSBnG/DO+kk=</ds:DigestValue>
</ds:Reference>
<ds:Reference URI="#_3">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
<exc14n:InclusiveNamespaces PrefixList="wsu wsse S" />
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>ug/VomtexDQbmMv45mPqAbYghXk=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:Signature Value="ei2Lzi4+wQjAyx41xBi/UcPm5zTYSX7q+wCMxQekjKTrHyLvrreibIAkJMTcPFgg+cNFkr4o3G+iK8yYZCo4x6nCwa+OCa83yy3wCXyZ8mIKZX5aByaW+CpBVjuxSiTjxBbj2BllkMPPspQP05KfdePGVa3joMDI7SU/4flkeCYMHnZB2jO96AiZNld2c7/sY0p/6UpJgo1VxYJrhLYTy11i57a5OWY2FYvxb2LkkN1rmm+72BYo1jMwPgBpSDHc+KrfDTmPHGXNTDl5dFlwHP8aGuXjggPMWd59jv60/Rb4i1s13lrzL5v27wmDXZHd6eRQYLPGPiEEgpGtKvW=="></ds:SignatureValue>
<ds:KeyInfo>
<wsse:SecurityTokenReference>
<ds:X509Data>
<ds:X509IssuerSerial>
<ds:X509IssuerName>CN=SINFONIA_TEST, C=IT</ds:X509IssuerName>
<ds:X509SerialNumber>1511261306</ds:X509SerialNumber>
</ds:X509IssuerSerial>
</ds:X509Data>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
</ds:Signature>
</wsse:Security>
</S:Header>
<S:Body>
<ns2:getAssistibileInAnagrafeResponse xmlns:ns2="http://www.sinfonia.campania.it/Schemas/" wsu:Id="#_5006">
<return>
<codFiscale>XXXDNTXXXXXXXXXX</codFiscale>
<codIstAtCittadinanza>100</codIstAtCittadinanza>
<codIstAtComuneNascita>XXXXXX</codIstAtComuneNascita>
<codIstAtComuneResidenza>XXXXXX</codIstAtComuneResidenza>
<codStatoCivile>0</codStatoCivile>
<codTipoAssistibile>1</codTipoAssistibile>
<codCognome>XXXXXX</codCognome>
<comuneNascita>XXXXXX</comuneNascita>
<comuneResidenza>XXXXXX</comuneResidenza>
<dataDecesso>XX/XX/2018</dataDecesso>
<dataFineResidenza>XX/XX/2018</dataFineResidenza>
<dataInizioResidenza>XX/XX/2009</dataInizioResidenza>
<dataNascita>XX/XX/1938</dataNascita>
<dataIscrizioneUSL>
<codMotivoFineIscrizione>26</codMotivoFineIscrizione>
<codMotivoIscrizione>9</codMotivoIscrizione>
<codNazionaleUSL>150205</codNazionaleUSL>
<dataFineIscrizione>XX/XX/2018</dataFineIscrizione>
<dataInizioIscrizione>XX/XX/2009</dataInizioIscrizione>
<denominazioneUSL>ASL NAPOLI 2</denominazioneUSL>
<descMotivoFineIscrizione>ALTRO</descMotivoFineIscrizione>
<descMotivoIscrizione>PRIMA ISCRIZIONE</descMotivoIscrizione>

```

```

<flagIscrizioneTemporanea>false</flagIscrizioneTemporanea>
<siglaUSL>NA/2</siglaUSL>
</datiIscrizioneUSL>
<datiSceltaMedico>
<codDeroga>0</codDeroga>
<codFiscaleMedico>XXXGPPXXXXXXXXXX</codFiscaleMedico>
<codMotivoFineScelta>7</codMotivoFineScelta>
<codMotivoInizioScelta>1</codMotivoInizioScelta>
<codiceMedico>XXXXXX</codiceMedico>
<cognomeMedico>XXXXXX</cognomeMedico>
<dataFineScelta>XX/XX/2018</dataFineScelta>
<dataInizioScelta>XX/XX/2009</dataInizioScelta>
<deroga>NESSUNA</deroga>
<descrizioneMotivoFineScelta>D'UFFICIO PER DECESSO</descrizioneMotivoFineScelta>
<descrizioneMotivoInizioScelta>SCELTA OPERATA DA ASSISTIBILE</descrizioneMotivoInizioScelta>
<nomeMedico>XXXXXX</nomeMedico>
<numTelefono>XXXXXX</numTelefono>
</datiSceltaMedico>
<descCittadinanza>ITALIANA</descCittadinanza>
<indResidenza>VIA XXXXXX N XX</indResidenza>
<nome>XXXXXX</nome>
<numDistrettoResidenza>XX</numDistrettoResidenza>
<numTelefono>XXXXXX</numTelefono>
<seesso>M</seesso>
<statoCivile>NON DEFINITO</statoCivile>
<tipoAssistibile>ASSISTITO DELLA REGIONE</tipoAssistibile>
</return>
</ns2:getAssistibileInAnagrafeResponse>
</S:Body>
</S:Envelope>

```

7. Rilascio credenziali applicative

Il RTI Sinfonia, provvederà a profilare il sistema fornitore sul sistema di test Sinfonia e a far pervenire al soggetto integratore il certificato x.509v3 e il Ruolo Istituzionale da utilizzarsi conformemente alle specifiche previste per le misure di sicurezza nell'ambito dell'implementazione degli scenari di interazione con i servizi di cooperazione applicativa o i web services.