Integrazione di
Service Provider e Identity Provider
SiRAC e INF3

SOMMARIO

1. Introduzione 4
1.1. Contenuti del Documento 4
1.2. Distribuzione 5
1.3. Acronimi 5
2. Integrazione di Service Provider 6
2.1. Interventi da eseguire su Service Provider ICAR INF-3 6
2.1.1. Configurazione dei parametri di contesto generali 6
2.1.2. Configurazione del componente request handler 7
2.1.3. Importazione del certificato dei metadati del Gateway fedERa nel trust-store del Service Provider 7
2.2. Interventi da eseguire su Service Provider SIRAC-PEOPLE con utilizzo di infrastruttura SIRAC senza funzionalità di Single-Sign-On 9
2.2.1. Dispiegamento del componente “AssertionConsumerService” 9
2.2.2. Configurazione del componente AccessCheck 11
2.2.3. Configurazione del Gateway SIRAC 2.0.1 12
2.3. Interventi da eseguire su Service Provider SIRAC-PEOPLE con utilizzo di infrastruttura SIRAC-SSO versione 2.0.2 14
2.3.1. Integrazione di SIRAC-SSO con l’Identity Provider fedERa 14
2.3.2. Integrazione di SIRAC-SSO con il Gateway Multiprotocollo fedERa 17
2.4. Interventi da eseguire su Service Provider SIRAC-PEOPLE con utilizzo di infrastruttura SIRAC-SSO versione 2.0.3 o successiva 20
3. Integrazione di Identity Provider 22
3.1. Interventi generali sull’Identity Provider 22
3.2. Interventi specifici per Identity Provider ICAR INF-3 22

3.3. Interventi specifici per Identity Provider SIRAC-PEOPLE 22

APPENDICE A: valori di configurazione predefiniti 23

1. INTRODUZIONE

1.1. CONTENUTI DEL DOCUMENTO

Questo documento ha lo scopo di illustrare le modalità di integrazione di entità/sistemi di tipo Service Provider e Identity Provider di vario tipo, con l'infrastruttura fedERa. Verranno trattati principalmente sistemi che rispettano le specifiche definite nell'ambito del task INF-3 del progetto ICAR e/o le specifiche SIRAC definite nell'ambito del progetto PEOPLE. Essi si basano nativamente sui protocolli derivati dallo standard SAML rispettivamente in versione 2.0 nel caso delle specifiche ICAR INF-3 e 1.1 nel caso di sistemi realizzati in ambito PEOPLE. In particolare, nel caso dei Service Provider, questo documento parte dal presupposto che essi siano già disponibili e funzionanti nei rispettivi ambiti di realizzazione, vale a dire che siano già integrati in un'infrastruttura ICAR INF-3, rispettivamente in un'infrastruttura SIRAC o SIRAC-SSO, nei quali siano quindi adottati tutti i componenti previsti dalle specifiche in tali ambiti. Ad esempio, si assumerà che i portali di servizi SIRAC-PEOPLE facciano uso del kit di integrazione per Service Provider realizzato in tale progetto e costituito dai seguenti componenti:

- Filtro di Autenticazione (AccessCheck)
- Ricevitore di Response SAML 1.1 (AssertionConsumerService)
- Ricevitore di Responsi di Autenticazione (AuthResponseReceiverService)

Nel caso di Service Provider ICAR, invece, si assumerà che essi utilizzino il kit di integrazione messo a disposizione con la Reference Implementation INF-3, costituito da:

- Gestore delle Richieste (Request Handler)
- Ricevitore di Response SAML 2.0 (AssertionConsumerService)

Nel caso di Service Provider SIRAC-PEOPLE, è necessario distinguere tra il caso in cui è utilizzata un'infrastruttura SIRAC fino alla versione 2.0.1, priva di funzionalità di Single-Sign-On (è il caso dei portali PEOPLE fino alla versione 2.0.1), dal caso in cui si impieghi un'infrastruttura SIRAC-SSO versione 2.0.2 o 2.0.3, in quanto le modalità di integrazione differiscono leggermente.

Nel seguito saranno forniti i dettagli sulle modalità operative per integrare Service Provider e Identity Provider in ambito ICAR INF-3 (essi saranno chiamati rispettivamente Service Provider ICAR INF-3 e Identity Provider ICAR INF-3). Successivamente saranno fornite informazioni analoghe, valide per l'integrazione di Service Provider conformi alle specifiche SIRAC-PEOPLE, chiamati nel seguito rispettivamente Service Provider SIRAC-PEOPLE e Identity Provider SIRAC-PEOPLE.

Nelle sezioni seguenti si farà spesso riferimento a parametri relativi all'infrastruttura fedERa che è necessario impostare nella configurazione dei Service Provider e Identity Provider oggetto dell'integrazione. Per conoscere i valori di tali parametri citati nel seguito, relativamente alla configurazione dell'infrastruttura fedERa, è possibile consultare l'Appendice A.

1.2. DISTRIBUZIONE

Il documento è distribuito all'interno del gruppo di lavoro del progetto FedERa.

1.3. ACRONIMI

Il seguente elenco riporta gli acronimi utilizzati nel documento:

SIGLA	DEFINIZIONE
IDM	Identity Manager, sistema di gestione delle identità
IDP	Identity Provider, sistema di autenticazione
GW	Gateway Multiprotocolo

2. INTEGRAZIONE DI SERVICE PROVIDER

Le fasi di integrazione di un Service Provider conforme alle specifiche ICAR INF-3 con l'infrastruttura fedERa descritti in questo capitolo partono dal presupposto che il Service Provider sia già integrato con una propria infrastruttura ICAR INF-3, per ulteriori informazioni riguardo questa fase preliminare si rimanda alla documentazione rilasciata nell'ambito del progetto ICAR. Nel caso di Service Provider di tipo SIRAC-PEOPLE, invece, si assume che essi siano già pre-configurati e funzionanti in un'installazione PEOPLE.

2.1. INTERVENTI DA ESEGUIRE SU SERVICE PROVIDER ICAR INF-3

L'integrazione di un Service Provider ICAR INF-3 con l'infrastruttura fedERa prevede la configurazione di alcuni parametri di inizializzazione nel deployment-descriptor (file "WEB-INF/web.xml") dell'applicazione web. Nel seguito sono descritti i frammenti che è necessario modificare, in modo separato per quanto riguarda i parametri di contesto generali con il relativo significato e per quanto riguarda i vari componenti (servlet) necessari.

2.1.1. Configurazione dei parametri di contesto generali

Nel deployment-descriptor è necessario configurare i seguenti parametri di contesto (elementi `<context-param>`):

```
[…]
<context-param>
        <param-name>authorityRegistryMetadataProviderURL</param-name>
        <param-value>URL_METADATI_AUTHORITY_REGISTRY_FEDERA</param-value>
</context-param>
<context-param>
        <param-name>authorityRegistrySubjectNameQualifier</param-name>
        <param-value>NAME_QUALIFIER_AUTHORITY_REGISTRY_FEDERA</param-value>
</context-param>
[…]
```

La seguente tabella descrive i parametri di contesto riportati nel frammento precedente:

NOME PARAMETRO	SIGNIFICATO	TIPO
authorityRegistry MetadataProviderURL	URL del servizio di fornitura metadati dell'Authority Registry del dominio fedERa a cui si intende associare il Service Provider oggetto dell'integrazione	String (URL)
authorityRegistrySubject NameQualifier	Name qualifier utilizzato per il subject nei messaggi AttributeQuery SAML 2.0 prodotti dal Service Provider e diretti all'Authority Registry del dominio fedERa a cui si intende associare il Service Provider oggetto dell'integrazione.	String (URL)

2.1.2. Configurazione del componente request handler

Il componente Request Handler (servlet-filter) svolge la funzione di intercettare le richieste dirette al servizio applicativo e verificare il contesto di autenticazione per la sessione utente. Relativamente a tale componente, nel deployment descriptor è necessario configurare il seguente parametro di inizializzazione (`<init-param>`):

```
[…]
<init-param>
        <param-name>localProxyMetadataProviderURL</param-name>
        <param-value>URL_METADATI_GATEWAY_FEDERA</param-value>
</init-param>
[…]
```

Tale URL rappresenta il servizio di fornitura dei metadati del soggetto a cui inviare le richieste di autenticazione, cioè il Gateway Multiprotocollo del dominio fedERa a cui si intende associare il Service Provider oggetto dell'integrazione.

2.1.3. Importazione del certificato dei metadati del Gateway fedERa nel trust-store del Service Provider

Nel caso i metadati SAML 2.0 del Gateway Multiprotocolo fedERa al quale viene interconnesso il Service Provider siano firmati digitalmente e il controllo di trust sul Service Provider sia abilitato, sarà necessario importare il certificato pubblico utilizzabile per la verifica di tali metadati all'interno del trust-store presso il Service Provider. Tale trust-store è configurabile mediante editazione del deployment descriptor del Service Provider, come nel frammento seguente:

```
[…]
<context-param>
        <param-name>truststorePath</param-name>
        <param-value>PATH_TRUST_STORE_SP</param-value>
</context-param>

<context-param>
        <param-name>truststorePassword</param-name>
        <param-value>PASSWORD_TRUST_STORE_SP</param-value>
</context-param>

<context-param>
        <param-name>trustCheckEnabled</param-name>
        <param-value>true</param-value>
</context-param>
[…]
```

La seguente tabella descrive i parametri di contesto riportati nel frammento precedente:

NOME PARAMETRO	SIGNIFICATO	TIPO
truststorePath	Percorso su file system del file del trust store in formato JKS contenente i certificati considerati affidabili per il controllo di trust	String (pathname relativo alla web application)
truststorePassword	Password del trust store di cui al parametro precedente	String
trustCheckEnabled	Flag booleano per abilitare o disabilitare il controllo di trust sui metadati ottenuti via connessione HTTP/HTTPS	String ("true" o "false")

2.2. INTERVENTI DA ESEGUIRE SU SERVICE PROVIDER SIRAC-PEOPLE CON UTILIZZO DI INFRASTRUTTURA SIRAC SENZA FUNZIONALITÀ DI SINGLE-SIGN-ON

Le fasi di integrazione con l'infrastruttura fedERa di un Service Provider SIRAC-PEOPLE già integrato con un'infrastruttura SIRAC fino alla versione 2.0.1 prevedono anzitutto la verifica che sul Service Provider sia dispiegato il componente AssertionConsumerService, che dovrà essere responsabile di ricevere i messaggi Response SAML 1.1 provenienti dal Gateway Multiprotocollo dell'infrastruttura fedERa. Inoltre, il componente AccessCheck dovrà essere configurato per indirizzare il gateway SIRAC di autenticazione, e indicare l'indirizzo del servizio AssertionConsumerService dispiegato presso di sé, per ricevere le risposte. Entrambe le attività comportano un intervento a livello di deployment-descriptor (file "WEB-INF/web.xml) delle applicazioni del Service, come descritto nel seguito. Presso l'applicazione web del gateway SIRAC, invece, dovranno essere configurati gli end-point SAML 1.1 messi a disposizione del Gateway fedERa, per la ricezione delle richieste di autenticazione. Anche tale attività comporta un intervento a livello di deployment-descriptor della relativa applicazione.

Infine, vi sono alcune attività di configurazione da apportare alla configurazione del Gateway Multiprotocollo, che non sono a carico dell'integratore del Service Provider ma che dovranno essere richieste al Gestore dell'infrastruttura fedERa.

2.2.1. Dispiegamento del componente "AssertionConsumerService"

Il dispiegamento del componente AssertionConsumerService responsabile di ricevere i messaggi Response SAML 1.1 provenienti dal Gateway Multiprotocollo fedERa si fa aggiungendo la sezione seguente al deployment-descriptor della web application del Service Provider:

```
[…]
<servlet>
        <servlet-name>AssertionConsumerService</servlet-name>
        <display-name>Sirac Assertion Consumer Service</display-name>
        <description>Sirac Assertion Consumer Service</description>
        <servlet-class>it.people.sirac.web.AssertionConsumerServlet</servlet-class>
        <init-param>
                <param-name>keystorePath</param-name>
                <param-value>PATH_TRUST_STORE_SP</param-value>
        </init-param>
        <init-param>
                <param-name>certificateAlias</param-name>
                <param-value>ALIAS_CERT_VERIFICA_FIRMA_GW_FEDERA</param-value>
```

```
        </init-param>
        <init-param>
                <param-name>keystorePassword</param-name>
                <param-value>PASSWORD_TRUST_STORE_SP</param-value>
        </init-param>
        <init-param>
                <param-name>authenticationResponseReceiverServiceForwardURL</param-name>ì
                <param-value>/AuthResponseReceiverService</param-value>
        </init-param>
        <init-param>
                <param-name>authenticationResponseReceiverServicePOSTURL</param-name>
                <param-alue>URL_ASSOLUTO_SERVIZIO_AUTHRESPONSERECEIVER_SP</param-value>
        </init-param>
        <init-param>
                <param-name>postResponsePage</param-name>
                <param-value>/PostAuthResponse.jsp</param-value>
        </init-param>
</servlet>

<servlet-mapping>
        <servlet-name>AssertionConsumerService</servlet-name>
        <url-pattern>/AssertionConsumerService</url-pattern>
</servlet-mapping>
[…]
```

La seguente tabella descrive i parametri di inizializzazione del componente riportati nel frammento precedente:

NOME PARAMETRO	SIGNIFICATO	TIPO
keystorePath	Percorso, relativo alla web application, del file del trust store in formato JKS contenente il certificato da utilizzare per la verifica della firma e della fiducia dei messaggi SAML Response ricevuti dal Gateway fedERa	String
certificateAlias	Nome dell'alias del certificato nel keystore da utilizzare per la verifica della firma della SAML Response	String
keystorePassword	Password del trust store di cui al parametro precedente	String

authenticationResponse ReceiverServiceForwardURL	URL relativo del servizio di ricezione del responso di autenticazione XML generato dal componente AssertionConsumerService per il Service Provider e inviato in modalità FORWARD. E' possibile mantenere il valore preimpostato.	String (URL relativo)
authenticationResponse ReceiverServicePOSTURL	URL assoluto del servizio di ricezione del responso di autenticazione XML generato dal componente AssertionConsumerService per il Service Provider e inviato in modalità POST. Deve riflettere l'hostname e la porta	String (URL)
postResponsePage	Percorso, relativo alla web application del Service Provider, della pagina JSP utilizzata per l'invio del responso di autenticazione XML in modalità POST	String

2.2.2. Configurazione del componente AccessCheck

Per fare in modo che il Service Provider invii le richieste di autenticazione al Gateway SIRAC, è necessario verificare che il deployment descriptor del Service Provider sia configurato come nel frammento seguente:

```
[…]
<filter>
        <filter-name>SIRAC Authentication Filter</filter-name>
        <filter-class>it.people.sirac.filters.SiracAuthenticationFilter</filter-class>
        <init-param>
                <param-name>SIRACGatewayRedirectURL</param-name>
                <param-value>URL_SERVIZIO_AUTENTICAZIONE_GW SIRAC</param-value>
        </init-param>
        <init-param>
                <param-name>assertionConsumerURL</param-name>
                <param-value>URL</param-value>
        </init-param>
        <init-param>
                <param-name>postAuthRequestPage</param-name>
```

```
            <param-value>/reserved/PostAuthRequest.jsp</param-value>
        </init-param>
</filter>
[…]
```

La seguente tabella descrive i parametri di inizializzazione del componente riportati nel frammento precedente:

NOME PARAMETRO	SIGNIFICATO	TIPO
SIRACGatewayRedirectURL	URL assoluto del servizio di ricezione delle richieste di autenticazione in standard SAML 1.1 e conformi alle specifiche SIRAC, presso il Gateway SIRAC accessibile dal Service Provider SIRAC-PEOPLE in oggetto	String (URL)
assertionConsumerURL	URL assoluto del servizio di ricezione dei messaggi Response in standard SAML 1.1 e conformi alle specifiche SIRAC, presso il Service Provider	String (URL)
postAuthRequestPage	Percorso, relativo alla web application del Service Provider, della pagina JSP utilizzata per l'invio della richiesta di autenticazione al Gateway Multiprotocollo fedERa	String

2.2.3. Configurazione del Gateway SIRAC 2.0.1

Presso il Gateway SIRAC 2.0.1 è necessario impostare l'indirizzo del servizio di ricezione richieste di autenticazione SAML 1.1 del Gateway fedERa intervenendo nel relativo deployment-descriptor come descritto di seguito. Si noti che l'utilizzo di entrambi i gateway SIRAC e fedERa non comporta alcun degrado nella qualità della user-experience, in quanto la scelta dell'Identity Provider è operata soltanto dal secondo gateway, essendo il primo privo di tale funzionalità e della capacità di gestire sessioni di Single-Sign-On.

```
[…]
```

```
<servlet>
        <servlet-name>AuthGatewayServlet</servlet-name>
        <display-name>SIRAC Authentication Gateway Servlet</display-name>
        <description>SIRAC Authentication Gateway Servlet</description>
        <servlet-class>it.people.sirac.web.AuthGatewayServlet</servlet-class>
        <init-param>
                <param-name>weakLoginRedirect</param-name>
                <param-value>URL_SERVIZIO_AUTENTICAZIONE_DEBOLE SAML 1.1 GW FEDERA/PATHINFO</param-
value>
        </init-param>
        <init-param>
                <param-name>strongLoginRedirect</param-name>
                <param-value>URL_SERVIZIO_AUTENTICAZIONE_FORTE SAML 1.1 GW FEDERA/PATHINFO</param-
value>
        </init-param>
</servlet>
[…]
```

La seguente tabella descrive i parametri di inizializzazione del componente riportati nel frammento precedente:

NOME PARAMETRO	SIGNIFICATO	TIPO
weakLoginRedirect	URL assoluto del servizio di ricezione delle richieste di autenticazione debole in standard SAML 1.1 e conformi alle specifiche SIRAC, presso il Gateway fedERa, con l'aggiunta di un *pathinfo* univoco per il servizio che si sta integrando	String (URL)
strongLoginRedirect	URL assoluto del servizio di ricezione delle richieste di autenticazione forte in standard SAML 1.1 e conformi alle specifiche SIRAC, presso il Gateway fedERa, con l'aggiunta di un *pathinfo* univoco per il servizio che si sta integrando	String (URL)

Il *pathinfo* è una stringa utilizzata come identificativo dal fedERa Gateway per associare univocamente i servizi SAML 1.1 alle richieste ricevute. Tale identificatore deve essere richiesto all'amministratore del Gateway, il quale provvederà a fornirne uno non ancora associato ad alcun servizio.

2.3. INTERVENTI DA ESEGUIRE SU SERVICE PROVIDER SIRAC-PEOPLE CON UTILIZZO DI INFRASTRUTTURA SIRAC-SSO VERSIONE 2.0.2

Se il Service Provider da integrare utilizza già un'infrastruttura SIRAC-SSO in versione 2.0.2[1], le operazioni di integrazione prevedono di mantenere tale infrastruttura che svolge già funzionalità di single-sign-on e federazione di Identity Provider così come offerte dal Gateway Multiprotocollo fedERa. Il Service Provider continuerebbe pertanto ad utilizzare SIRAC-SSO per inviare le richieste di autenticazione e continuerebbe a ricevere da esso i messaggi di responso di autenticazione XML come definito dalla specifica SIRAC-PEOPLE. Nessun intervento è pertanto necessario a livello di Service Provider. Tuttavia, per consentire l'autenticazione di utenti che dispongono di account presso uno degli Identity Provider fedERa, è possibile aggiungere alla configurazione di SIRAC-SSO le coordinate necessarie per indirizzare uno o più di tali Identity Provider, che offrono un'interfaccia per la ricezione di richieste di autenticazione e la produzione delle relative risposte, in standard SAML 1.1 e in conformità alle specifiche SIRAC-PEOPLE. In alternativa, è possibile aggiungere alla configurazione di SIRAC-SSO anche il Gateway Multiprotocollo fedERa, nei confronti del quale SIRAC-SSO apparirebbe come un Service Provider. Ciò consentirebbe di demandare ulteriormente la gestione dell'autenticazione all'infrastruttura fedERa nel suo complesso, includendo anche aspetti come la gestione dei Circle-of-Trust ed evitando di ridefinire tutti gli Identity Provider utilizzabili dagli utenti dei servizi a loro volta integrati in SIRAC-SSO. Tali due alternative saranno descritte nel seguito.

2.3.1. Integrazione di SIRAC-SSO con l'Identity Provider fedERa

L'interconnessione tra SIRAC-SSO e il sistema di autenticazione (IdP) disponibile presso

[1] La versione 2.0.2 dell'infrastruttura SIRAC-SSO è stata rilasciata nell'ambito del progetto PEOPLE, in corrispondenza con la versione 2.0.2 del Framework.

l'infrastruttura fedERa viene effettuata modificando il file di configurazione "WEB-INF/sirac-config.xml" presente nella web application "sirac-sso" e aggiungendo un frammento come il seguente:

```
[…]
<IdP trustLevel="TRUSTED">
        <Name>NOME_IDP_FEDERA</Name>
        <Description>DESCRIZIONE_IDP_FEDERA</Description>
        <AssertionIssuer>ISSUER_ASSERZIONI_IDP_FEDERA</AssertionIssuer>
        <AuthenticationServices>
               <AuthenticationService>
                      <Method>WEAK</Method>
                      <Location>URL_SERVIZIO_AUTENTICAZIONE_SAML_1.1_DEBOLE</Location>
               </AuthenticationService>
               <AuthenticationService>
                      <Method>STRONG</Method>
                      <Location>URL_SERVIZIO_AUTENTICAZIONE_SAML_1.1_FORTE</Location>
               </AuthenticationService>
        </AuthenticationServices>
        <SigningInfo trustVerification="disabled">
               <X509Certificate subject="SUBJ_CERT_IDP_FEDERA" issuer="ISSUER_CERT_IDP_FEDERA"
                                alias="ALIAS_CERT_IDP_FEDERA">
                      <X509Data>CERT_IDP_FEDERA_BASE64</X509Data>
               </X509Certificate>
        </SigningInfo>
</IdP>
[…]
```

La tabella seguente descrive i parametri oggetto di configurazione evidenziati nel frammento del file sirac-config.xml illustrato sopra:

NOME PARAMETRO	SIGNIFICATO	TIPO
NOME_IDP_FEDERA	E' un nome, scelto univocamente tra quelli presenti nel file sirac-config.xml, per identificare l'Identity Provider fedERa SAML 1.1 che si vuole registrare	String
DESCRIZIONE_IDP_FEDERA	Descrizione testuale dell'Identity	String

	Provider fedERa SAML 1.1 che si vuole registrare	
ISSUER_ASSERZIONI_ IDP_FEDERA	E' l'issuer delle asserzioni di autenticazione e attributo SAML 1.1 prodotte dall'IdP fedERa che si vuole registrare	String (URI)
URL_SERVIZIO_ AUTENTICAZIONE_SAML_ 1.1_DEBOLE	E' l'URL assoluto del servizio di ricezione delle richieste di autenticazione deboli in standard SAML 1.1 e conformi alle specifiche SIRAC, presso l'Identity Provider fedERa che si vuole censire	String (URL)
URL_SERVIZIO_ AUTENTICAZIONE_SAML_1.1_FORTE	E' l'URL assoluto del servizio di ricezione delle richieste di autenticazione forti in standard SAML 1.1 e conformi alle specifiche SIRAC, presso l'Identity Provider fedERa che si vuole censire	String (URL)
SUBJ_CERT_IDP_FEDERA, ISSUER_CERT_IDP_FEDERA e ALIAS_CERT_IDP_FEDERA	Stringhe utili per identificare il certificato usato da SIRAC-SSO per verificare le firme apposte alle asserzioni di autenticazioni inviate dall'IDP fedERa SAML 1.1. Rappresentano rispettivamente il soggetto a cui è stato assegnato il certificato, il soggetto che l'ha emesso e un alias	String
CERT_IDP_FEDERA_BASE64	Codifica in formato Base64 del certificato X.509 da utilizzare per verificare la firma delle asserzioni prodotte dall'Identity Provider fedERa oggetto dell'integrazione	String

Per quanto riguarda il significato degli altri elementi non descritti si rimanda alla documentazione dell'infrastruttura SIRAC-SSO.

2.3.2. Integrazione di SIRAC-SSO con il Gateway Multiprotocollo fedERa

Connettere direttamente l'infrastruttura SIRAC-SSO al Gateway Multiprotocollo comporta l'avere due livelli di intermediazione durante la fase di autenticazione all'accesso ai servizi, per mettere in comunicazione il generico Service Provider coinvolto con i vari Identity Provider selezionabili dall'utente. Il primo livello è infatti costituito dalla comunicazione tra i Service Provider e l'infrastruttura SIRAC-SSO la quale abilita già un primo livello di Single-Sign-On tra tutti i Service Provider ad essa afferenti e consente di selezionare uno tra gli Identity Provider registrati. Nel caso di connessione al Gateway Multiprotocollo, quest'ultimo deve essere registrato presso SIRAC-SSO proprio come Identity Provider così che possa essere selezionabile dall'utente durante l'autenticazione. Si noti tuttavia che, a sua volta, il Gateway Multiprotocollo, che rappresenta il secondo livello di intermediazione, presenta all'utente la scelta dell'Identity Provider dove autenticarsi. E' pertanto opportuno che sia soltanto quest'ultimo sistema a proporre questa scelta e che quindi l'analoga funzionalità presso SIRAC-SSO venga disabilitata. Ciò si traduce nel de-registrare da SIRAC-SSO tutti gli altri Identity Provider ad eccezione del Gateway. Nel file di configurazione "WEB-INF/sirac-config.xml" presente nella web application "sirac-sso" e la sezione <IdPConfig> dovrà pertanto essere popolata con un unico Identity Provider, nel seguente modo:

```
[…]
<IdP trustLevel="TRUSTED">
        <Name>NOME_GATEWAY_FEDERA</Name>
        <Description>DESCRIZIONE_GATEWAY_FEDERA</Description>
        <AssertionIssuer>ISSUER_ASSERZIONI_GATEWAY_FEDERA</AssertionIssuer>
        <AuthenticationServices>
                <AuthenticationService>
                        <Method>WEAK</Method>
                        <Location>URL_SERVIZIO_AUTENTICAZIONE_SAML_1.1_DEBOLE/PATHINFO</Location>
                </AuthenticationService>
                <AuthenticationService>
                        <Method>STRONG</Method>
                        <Location>URL_SERVIZIO_AUTENTICAZIONE_SAML_1.1_FORTE/PATHINFO</Location>
                </AuthenticationService>
        </AuthenticationServices>
        <SigningInfo trustVerification="disabled">
```

```
                <X509Certificate subject="SUBJ_CERT_GW_FEDERA" issuer="ISSUER_CERT_GW_FEDERA"
                                 alias="ALIAS_CERT_GW_FEDERA">
                        <X509Data>CERT_GW_FEDERA_BASE64</X509Data>
                </X509Certificate>
        </SigningInfo>
</IdP>
[…]
```

La tabella seguente descrive i parametri oggetto di configurazione evidenziati nel frammento del file sirac-config.xml illustrato sopra:

NOME PARAMETRO	SIGNIFICATO	TIPO
NOME_GATEWAY_FEDERA	E' un nome, scelto univocamente tra quelli presenti nel file sirac-config.xml, per identificare il Gateway Multiprotocollo fedERa SAML 1.1 che si vuole registrare come IdP	String
DESCRIZIONE_GATEWAY_FEDERA	Descrizione testuale del Gateway Multiprotocollo fedERa SAML 1.1 che si vuole registrare	String
ISSUER_ASSERZIONI_ GATEWAY_FEDERA	E' l'issuer delle asserzioni di autenticazione e attributo SAML 1.1 prodotte dal Gateway Multiprotocollo fedERa che si vuole registrare. Corrisponde all'entityID del Gateway	String (URI)
URL_SERVIZIO_AUTENTICAZIONE_ SAML_1.1_DEBOLE	E' l'URL assoluto del servizio di ricezione delle richieste di autenticazione deboli in standard SAML 1.1 e conformi alle specifiche SIRAC, presso il Gateway Multiprotocollo fedERa che si vuole censire, con l'aggiunta di un *pathinfo* univoco per il servizio che si sta	String (URL)

	integrando	
URL__SERVIZIO_ AUTENTICAZIONE_SAML_1.1_FORTE	E' l'URL assoluto del servizio di ricezione delle richieste di autenticazione forti in standard SAML 1.1 e conformi alle specifiche SIRAC, presso il Gateway Multiprotocollo fedERa che si vuole censire, con l'aggiunta di un *pathinfo* univoco per il servizio che si sta integrando	String (URL)
SUBJ_CERT_GW_FEDERA, ISSUER_CERT_GW_FEDERA e ALIAS_CERT_GW_FEDERA	Stringhe utili per identificare il certificato usato da SIRAC-SSO per verificare le firme apposte alle asserzioni di autenticazione SAML 1.1 inviate dal Gateway Multiprotocollo fedERa. Rappresentano rispettivamente il soggetto a cui è stato assegnato il certificato, il soggetto che l'ha emesso e un alias	String
CERT_GW_FEDERA_BASE64	Codifica in formato Base64 del certificato X.509 da utilizzare per verificare la firma delle asserzioni prodotte dal Gateway Multiprotocollo fedERa oggetto dell'integrazione	String

Il *pathinfo* è una stringa utilizzata come identificativo dal fedERa Gateway per associare univocamente i servizi SAML 1.1 alle richieste ricevute. Tale identificatore deve essere richiesto all'amministratore del Gateway, il quale provvederà a fornirne uno non ancora associato ad alcun servizio. Per quanto riguarda il significato degli altri elementi non descritti si rimanda alla documentazione dell'infrastruttura SIRAC-SSO.

2.4. INTERVENTI DA ESEGUIRE SU SERVICE PROVIDER SIRAC-PEOPLE CON UTILIZZO DI INFRASTRUTTURA SIRAC-SSO VERSIONE 2.0.3 O SUCCESSIVA

Nel caso di Service Provider già integrati con un'infrastruttura SIRAC-SSO in versione 2.0.3 o successiva, valgono le medesime considerazioni presentate nella sezione precedente. L'unico elemento di differenza è la struttura del frammento che rappresenta l'Identity Provider fedERa, all'interno del file di configurazione "sirac-config.xml". In questo caso il frammento è come il seguente. Per quanto riguarda il significato dei parametri oggetto della configurazione (evidenziati in neretto come per i frammenti riportati in precedenza), si rimanda alla sezione precedente.

```
[…]
<IdP protocolHandlerName="IDP-SAML11" trustLevel="TRUSTED">
       <Name>NOME_IDP_FEDERA</Name>
        <Description>DESCRIZIONE_IDP_FEDERA</Description>
        <AssertionIssuer>ISSUER_ASSERZIONI_IDP_FEDERA</AssertionIssuer>
        <AssertionIntendedRecipient>URL_SIRAC-SSO_ASSERTION_CONSUMER</AssertionIntendedRecipient>
        <AuthenticationServices>
               <AuthenticationService>
                      <Method>WEAK</Method>
                      <Location>URL_SERVIZIO_AUTENTICAZIONE_SAML_1.1_DEBOLE</Location>
               </AuthenticationService>
               <AuthenticationService>
                      <Method>STRONG</Method>
                      <Location>URL_SERVIZIO_AUTENTICAZIONE_SAML_1.1_FORTE</Location>
               </AuthenticationService>
        </AuthenticationServices>
        <SigningInfo trustVerification="<enabled|disabled>">
               <X509Certificate subject="SUBJ_CERT_IDP_FEDERA" issuer="ISSUER_CERT_IDP_FEDERA"
                                alias="ALIAS_CERT_IDP_FEDERA">
                    <X509Data>CERT_IDP_FEDERA_BASE64</X509Data>
               </X509Certificate>
        </SigningInfo>
</IdP>
[…]
```

Nel frammento sopra presentato, l'unico parametro aggiuntivo che si intende evidenziare, rispetto alla versione 2.0.2, è descritto nella tabella seguente. Come sopra, per i restanti parametri non descritti si rimanda alla documentazione dell'infrastruttura SIRAC-SSO.

NOME PARAMETRO	SIGNIFICATO	TIPO
URL_SIRAC-SSO_ ASSERTION_CONSUMER	E' l'indirizzo (URL) assoluto del servizio di ricezione dei messaggi Response SAML 1.1 presso l'infrastruttura SIRAC-SSO	String (URL)

Considerazioni analoghe valgono nel caso di connessione al Gateway Multiprotocollo invece che direttamente all'Identity Provider, come indicato nella sezione 2.3.2 a cui si rimanda.

3. INTEGRAZIONE DI IDENTITY PROVIDER

L'integrazione di un Identity Provider con l'infrastruttura fedERa richiede sui primi l'esecuzione di alcuni interventi dei quali alcuni di tipo generali e comuni alla maggior parte degli IdP di tale tipologia, e altri specifici di ciascuna di esse, trattati separatamente per gli Identity Provider ICAR INF-3 e SIRAC-PEOPLE. Altre attività infine saranno necessarie sull'infrastruttura fedERa, come descritto nel seguito.

3.1. INTERVENTI GENERALI SULL'IDENTITY PROVIDER

L'Identity Provider SAML 2.0 da integrare può richiedere di conoscere i metadati del mittente dei messaggi SAML di richiesta di autenticazione in ingresso, cioè il Gateway Multiprotocollo fedERa. Tale richiesta può essere di tipo statico, nel qual caso è sufficiente trasferire presso l'IdP il relativo file XML, oppure di tipo dinamico, mediante connessione al servizio di pubblicazione dei metadati, offerto dal Gateway. Quest'ultimo è il caso, ad esempio degli Identity Provider SAML 2.0 che fanno uso del layer di integrazione sviluppato in ICAR INF-3. Essendo il servizio di pubblicazione metadati del Gateway fedERa disponibile su protocollo HTTPS, sarà necessario che il gestore dell'Identity Provider aggiunga al trust store utilizzato dall'IdP per stabilire connessioni HTTPS anche il certificato pubblico del Gateway fedERa.

3.2. INTERVENTI SPECIFICI PER IDENTITY PROVIDER ICAR INF-3

Nessuna attività supplementare è richiesta: l'Identity Provider accede all'Authority Registry per ottenere informazioni riguardo il Gateway Multiprotocollo che deve esservi censito (vedi oltre) e verificare le firme digitali apposte ai messaggi di richiesta di autenticazione.

3.3. INTERVENTI SPECIFICI PER IDENTITY PROVIDER SIRAC-PEOPLE

Nessuna attività supplementare è richiesta: non esistendo il corrispondente SAML 1.1 dei messaggi di autenticazione (AuthnRequest) SAML 2.0, non vi sono firme digitali da verificare e quindi non è necessario che l'Identity Provider acceda ad informazioni relative al Gateway fedERa. Si noti che un IdP PEOPLE produce un elenco di attributi, all'interno delle asserzioni di autenticazione, conforme alle specifiche tecniche SIRAC-PEOPLE,già supportati da fedERa.

APPENDICE A: VALORI DI CONFIGURAZIONE PREDEFINITI

In questa sezione vengono riportati gli URL predefiniti presso l'infrastruttura fedERa, relativamente ai vari punti di configurazione citati nel presente documento, suddivisi per sottosistema di interesse.

AUTHORITY REGISTRY FEDERA

NOME PARAMETRO	VALORE PREDEFINITO
EntityID dell'Authority Registry	https://federa.lepida.it/ar/metadata
URL del servizio di fornitura metadati SAML 2.0	https://federa.lepida.it/ar/metadata
Subject Name Qualifier da utilizzare per le interrogazioni SAML 2.0 all'Authority Registry	https://federa.lepida.it/ar

GATEWAY MULTIPROTOCOLLO FEDERA

NOME PARAMETRO	VALORE PREDEFINITO
EntityID del Gateway	https://federa.lepida.it/gw/metadata
URL del servizio di fornitura metadati SAML 2.0	https://federa.lepida.it/gw/metadata
URL del servizio di ricezione richieste di autenticazione debole in standard SAML 1.1 (PEOPLE-SIRAC)	https://federa.lepida.it/gw/SSOProxy/SAML1/WEAK
URL del servizio di ricezione richieste di autenticazione forte in standard SAML 1.1 (PEOPLE-SIRAC)	https://federa.lepida.it/gw/SSOProxy/SAML1/STRONG

URL del servizio di ricezione richieste di autenticazione in standard SAML 2.0 (ICAR INF-3)	https://federa.lepida.it/gw/SSOProxy/SAML2
URL del servizio di ricezione di Response di autenticazione SAML 1.1 e SAML 2.0	https://federa.lepida.it/gw/AssertionConsumerProxy

IDENTITY PROVIDER FEDERA

Nella seguito si farà riferimento ad un generico IdP fedERa afferente al dominio di autenticazione "federa.it". Sarà sufficiente sostituire tale valore con l'identificativo del dominio di interesse per ottenere il valore corretto per tale dominio. Per ciascun Identity Provider fedERa, il livello minimo di affidabilità complessiva dell'identità supportato è indicato con un valore numerico da 1 a 5. Ciascun valore può essere messo in corrispondenza con il livello di affidabilità dell'identità degli utenti che possono autenticarsi presso tale IdP e con il livello di password policy minima ammessa per l'autenticazione con tale strumento, presso lo stesso IdP. Come sopra, negli URL relativi agli IdP fedERa compare il livello minimo accettato per l'autenticazione. Sarà sufficiente variare tale valore da 1 a 5 per specificare un livello differente, secondo la tabella di corrispondenza seguente:

LIVELLO COMPLESSIVO	AFFIDABILITA' DEL PROCESSO DI IDENTIFICAZIONE	LIVELLO PASSWORD POLICY
1	Utenti non identificati	Nessuna policy
2	Utenti identificati in modo indiretto	Nessuna policy
3	Utenti identificati in modo certo	Nessuna policy
4	Utenti identificati in modo certo	Dati personali
5	Utenti identificati in modo certo	Dati sensibili

La tabella seguente illustra i parametri relativi al generico IdP fedERa del dominio "federa.it" e di livello 1.

NOME PARAMETRO	VALORE PREDEFINITO
EntityID dell'Identity Provider	https://federa.lepida.it/idp/profile/Metadata/federa.it/1
URL del servizio di fornitura metadati SAML 2.0	https://federa.lepida.it/idp/profile/Metadata/federa.it/1
URL del servizio di ricezione richieste di autenticazione deboli in standard SAML 1.1 (PEOPLE-SIRAC)	https://federa.lepida.it/idp/profile/SAML1/WEAK/SSO/federa.it/1
URL del servizio di ricezione richieste di autenticazione forti in standard SAML 1.1 (PEOPLE-SIRAC)	https://federa.lepida.it/idp/profile/SAML1/STRONG/SSO/federa.it/1
URL del servizio di ricezione richieste di autenticazione in standard SAML 2.0 (ICAR INF-3)	https://federa.lepida.it/idp/profile/SAML2/SSO/federa.it/1