

SHIBBOLETH

LINEE GUIDA INTEGRAZIONE PIATTAFORMA SHIBBOLETH - IDENTITY PROVIDER SAML2

VERIFICHE E APPROVAZIONI

VERSIONE	REDAZIONE		CONTROLLO APPROVAZIONE		AUTORIZZAZIONE EMISSIONE	
	NOME	DATA	NOME	DATA	NOME	DATA
V10	IDENTITA DIGITALE	17/04/23	ALFONSINA ARENA	19/04/2023	ROBERTO OTTINO	21/04/2023
V09	IDENTITA DIGITALE	28/02/23	ALFONSINA ARENA	01/03/2023	ROBERTO OTTINO	01/03/2023
V08	A. ARENA	31/05/19	ALFONSINA ARENA	31/05/19	PIER PAOLO GRUERO	06/06/19
V07	A. ARENA	08/02/18	ALFONSINA ARENA	09/12/18	MARIO PISSARDO	09/12/18
V06	D. CERVINO	03/06/16	ALFONSINA ARENA	03/06/16	MARIO PISSARDO	03/06/16
V05	P. MANTOVANI	16/06/15	ALFONSINA ARENA	16/06/15	MARIO PISSARDO	16/06/15
V04	C. MARCHETTI	27/05/15	ALFONSINA ARENA	27/05/15	MARIO PISSARDO	27/05/15
V03	D. CERVINO	28/08/14	ALFONSINA ARENA	28/08/14	MARIO PISSARDO	28/08/14
V02	P. MANTOVANI M. FORMICA	27/11/13	ALFONSINA ARENA	27/11/13	MARIO PISSARDO	27/11/13
V01	P. MANTOVANI M. FORMICA	15/05/13	ALFONSINA ARENA	15/05/13	MARIO PISSARDO	15/05/13

STATO DELLE VARIAZIONI

VERSIONE	PARAGRAFO O PAGINA	DESCRIZIONE DELLA VARIAZIONE
V10	Tutto il documento	Revisione di tutto il documento. Aggiornati riferimento a nuovo IdP Stranieri. Aggiornata tabella par. 3.1
V09	Tutto il documento	Revisione di tutto il documento. Aggiornati riferimenti a IdP ECSI e aggiunti IdP APL e CIFA
V08	Tutto il documento	Aggiornati riferimenti a nuovo IdP Consiglio Regionale
V07	Tutto il documento	Aggiunta IdP Città di Torino
V06	Tutto il documento	Rimossa per il social autenticazione Twitter
V05	Paragrafo 4.2.3	Aggiunta nota recuper attributi header http
V04	Tutto il documento	Aggiunta Idp Social
V03	Tutto il documento	Aggiunta Idp iamidpregp e iamidpcsi. Aggiunta attributo matricola e tipo risorsa
V02	Paragrafo 4.2.1	Aggiunta attributo Shib-Identita-Riscontro
V01	Tutto il documento	Versione iniziale del documento

INDICE

1. SCOPO E CAMPO DI APPLICAZIONE	4
1.1 SCOPO	4
1.2 CAMPO DI APPLICAZIONE	4
1.3 RIFERIMENTI	4
1.4 PREREQUISITI	4
1.5 RESPONSABILITÀ	4
2. IDENTITY PROVIDER.....	5
3. INTEGRAZIONE SHIBBOLETH IN CSI.....	6
3.1 PASSO 1: RICHIESTA CONTESTO SHIBBOLETH.....	7
3.2 PASSO 1: RICHIESTA CONTESTO SHIBBOLETH VARIANTE CIFA.....	9
3.2.1 <i>Service Provider CIFA</i>	9
3.2 PASSO 2: CONFIGURAZIONI DELL'APPLICATIVO.....	10
3.2.1 <i>Attributi forniti</i>	10
3.2.2 <i>Attributi forniti da IDPSOCIAL</i>	12
3.2.3 <i>Recupero attributi header http</i>	12
3.3 PASSO 3: GESTIONE LOGOUT	13
3.4 PASSO 3: GESTIONE LOGOUT VARIANTE CIFA	13
4. APPROFONDIMENTI SULLE SESSIONI	14
4.1 SCADENZA SESSIONI	14
5. APPENDICE A: GLOSSARIO	16

1. Scopo e campo di applicazione

1.1 Scopo

Il presente documento ha lo scopo di fornire le linee guida per l'integrazione di un'applicazione all'interno del framework Shibboleth utilizzato in azienda.

1.2 Campo di applicazione

Il documento fornisce le linee guida per l'integrazione di un applicativo con il sistema di autenticazione Shibboleth.

Nello specifico, i destinatari sono:

- Progettisti di architetture di sistemi
- Progettisti di sistemi
- Sviluppatori di sistemi
-

1.3 Riferimenti

[1] Shibboleth: <https://shibboleth.atlassian.net/wiki/spaces>

[2] Linee guida per la protezione web application tramite Shibboleth: <http://kbt.csi.it/sviluppo/best-practice-e-linee-guida/item/715-linee-guida-per-la-protezione-web-application-tramite-shibboleth>

[3] Sezione Shibboleth intranet CSI Piemonte: <https://intranet.csi.it/web/come-fare-per/come-funziona-shibboleth-2/>

[4] Ambienti in cui è dispiegato Shibboleth: Ambienti-Enterprise-dispiegamento-Shibboleth-VXX.xlsx

[5] Libreria per il reperimento delle informazioni da Service Provider Shibboleth:

http://kbt.csi.it/component/docman/doc_download/528-manuale-duso-libreria-client-shibboleth

1.4 Prerequisiti

Ambito utilizzo:

- applicativi web-based

Conoscenze:

- protocolli web
- sistemi SSO
- sistemi distribuiti
- federazioni di identità digitali
- framework shibboleth (nel par. 3 è riportata una descrizione dei concetti fondamentali per la comprensione dei passi d'integrazione).

1.5 Responsabilità

La responsabilità di approvare, aggiornare e migliorare il documento è del gruppo Identità Digitale, responsabile del dispiegamento di componenti Shibboleth in CSI Piemonte.

2. Identity Provider

Sono dispiegate diverse componenti applicative per l'utilizzo dei servizi di autenticazione. Attraverso queste componenti vengono esposti Identity Provider (IdP) Shibboleth SAML 2.0 che permettono di riconoscere le credenziali di autenticazione.

Di seguito le componenti e gli Identity Provider disponibili:

Componente	Identity Provider SAML	Descrizione	Tipologia di credenziali
IAMIDP	Identity Provider RUPAR Internet	Riconosce le credenziali rilasciate alla Pubblica Amministrazione piemontese su rete rupar (intranet)	User, password User, password, pin Credenziale crittografica di tipo CNS
	Identity Provider RUPAR Intranet	Riconosce le credenziali rilasciate alla Pubblica Amministrazione piemontese su rete internet	User, password User, password, pin Credenziale crittografica di tipo CNS
IAMIDPSP	Identity Provider Sistema Piemonte	Riconoscere solo credenziali crittografiche CNS	Credenziale crittografica di tipo CNS
IAMIDPTOFA	Identity Provider Torino Facile	Riconosce solo credenziali crittografiche CNS	Credenziale crittografica di tipo CNS
IAMPRT0	Identity Provider Città metropolitana di Torino	Riconosce le credenziali dei dipendenti della Città metropolitana di Torino	User, password User, password, pin Credenziale crittografica di tipo CNS
IAMIDPREGP	Identity Provider Regione Piemonte	Riconosce le credenziali dei dipendenti della Regione Piemonte – Giunta	Credenziale crittografica di tipo CNS
IAMIDPCSI	Identity Provider CSI Piemonte Intranet	Riconosce le credenziali (posta elettronica) dei dipendenti e consulenti del CSI Piemonte su rete intranet	User, password
	Identity Provider CSI Piemonte Internet	Riconosce le credenziali (posta elettronica) dei dipendenti e consulenti del CSI Piemonte su rete internet	User, password
IAMIDPCOTO	Identity Provider Città di Torino	Riconosce le credenziali dei dipendenti e collaboratori della Città di Torino	User, password User, password, pin
IAMIDPCRP	Identity Provider Consiglio Regionale Intranet	Riconosce le credenziali (posta elettronica) dei dipendenti e collaboratori del consiglio Regionale su rete intranet	User, password

	Identity Provider Consiglio Regionale Internet	Riconosce le credenziali (posta elettronica) dei dipendenti e collaboratori del consiglio Regionale su rete internet	User, password
IAMIDPEXT	Identity Provider non RUPAR - Stranieri	Riconosce le credenziali fornite da CSI Piemonte definite no RUPAR e per Stranieri e/o utenti privi di codice fiscale italiano	User, password, pin
IDPAPL	Identity Provider per APL	Riconosce le credenziali dei dipendenti e collaboratori dell'ente APL – Agenzia Piemonte Lavoro	User, password, pin
IDPCIFA	Identity Provider per Città Facile ed Enti Fuori Regione	Riconosce le credenziali fornite da CSI Piemonte agli operatori PA che operano nel circuito Città Facile e/o operatori PA di Enti Fuori Regione	User, password User, password, pin
IDPSOCIAL	Identity provider Social	Riconosce le credenziali registrate sui seguenti provider: facebook, google, yahoo. Può essere usato solo in contesti dove la tipologia di dati trattati non richiedono un livello di autenticazione forte e non è necessario un riscontro certo dell'identità dell'utente. In tale contesto, infatti, non viene fornito il codice fiscale dell'utente	User, password

L'utilizzo del servizio di autenticazione è possibile richiedendo la protezione di un contesto web tramite l'inserimento di direttive opportune.

La possibilità di utilizzare il servizio di autenticazione tramite Shibboleth dipende da una condizione: la presenza e la configurazione del Service Provider Shibboleth per il VH per cui si richiede il contesto web (questo può essere verificato in [4]).

Il Service Provider **deve** essere esposto su protocollo TLS 1.2.

Nel caso in cui il VH per cui viene richiesta la configurazione non sia riportato nell'elenco ([4]) oppure non compaia il portale di autenticazione o l'identity provider voluto, occorre contattare identita.digitale@csi.it per richiedere l'inserimento della configurazione mancante. Se la richiesta non soddisfa alcuni requisiti, Identita Digitale non predisporrà la configurazione.

3. Integrazione Shibboleth in CSI

Le operazioni necessarie per proteggere un applicativo con un Service Provider Shibboleth possono essere così riassunte:

1. richiesta contesto web shibboleth sul web server che ospita il Service Provider
2. configurazioni dell'applicativo e recupero nell'header http degli attributi forniti dall'Identity Provider in relazione all'utente autenticato)
3. gestione del logout per applicativo protetto da Service Provider

3.1 Passo 1: Richiesta contesto shibboleth

È una normale richiesta di configurazione di contesto web su un server web. A titolo di esempio si riporta una configurazione da richiedere per una web application con contesto shibclient:

```
<Location /shibclient >
  ShibRequestSetting applicationId APPLICATION_VH_LIVX_PORTALEAUTH
  AuthType shibboleth
  ShibRequireSession On
  ShibUseHeaders On
  require valid-user

# <... direttive legate all'application server>

</Location>
```

Un applicativo può scegliere il livello di autenticazione minimo necessario per accedere alle funzionalità.

Le scelte possibili sono:

- livello 1: a questi servizi l'utente può accedere con un/pwd, un/pwd/PIN, credenziali crittografiche
- livello 2: a questi servizi l'utente può accedere con un/pwd/PIN, credenziali crittografiche
- livello 3: a questi servizi l'utente può accedere solo con credenziali crittografiche

La modalità con cui si effettua la scelta del livello di autenticazione è attraverso la definizione della location.

Il parametro ShibRequestSetting applicationId **APPLICATION_VH_LIVX_PORTALEAUTH** è l'identificativo del Service Provider di riferimento dove:

- **VH**: è il nome del virtual host di produzione su cui viene configurato il contesto web
- **LIVX**: assume i valori LIV1, LIV2, LIV3 a seconda del livello minimo di autenticazione scelto dall'applicativo;
- **PORTALEAUTH**: identifica il VH di esposizione dell'Identity Provider usato per l'autenticazione.

I valori di PORTALEAUTH e i VH di esposizione delle componenti sono:

Componente	Identity Provider SAML	PORTALEAUTH	VH
IAMIDP	Identity Provider Rupar Intranet	IRUP	https://portale.ruparpiemonte.it
	Identity Provider Rupar Internet	WRUP	https://secure.ruparpiemonte.it
IAMIDPSP	Identity Provider Sistema Piemonte	SISP	https://secure.sistemapiemonte.it
IAMIDPTOFA	Identity Provider Torino Facile	TOFA	https://servizi.torinofacile.it
IAMPRT0	Identity Provider Città metropolitana di Torino	PROVTO	https://intranet.provincia.torino.it

IAMIDPREGP	Identity Provider Regione Piemonte	IREGP	https://appweb.regione.piemonte.it https://intranet.regione.piemonte.it
IAMIDPCSI	Identity Provider CSI Piemonte Intranet	ICSI	https://intranet.csi.it
	Identity Provider CSI Piemonte Internet	ECSI	https://extranet.csi.it
IAMIDPCOTO	Identity Provider Città di Torino	COTO	https://servizi.comune.torino.it
IAMIDPCRP	Identity Provider Consiglio Regionale Intranet	ICON	https://www.cr.piemonte.it
	Identity Provider Consiglio Regionale Internet	ICON	https://intranet.consiglioregionale.piemonte.it
IAMIDPEXT	Identity Provider non Rupar – Stranieri – Utenti no codice fiscale	EXT	https://secure.sistemapiemonte.it
IDPAPL	Identity Provider per APL	APL	https://id.agenziapiemontelavoro.it
IDPSOCIAL	Identity provider Social	SOCIAL	https://secure.sistemapiemonte.it

NOTA: L'IDPSOCIAL può essere utilizzato solo dai contesti definiti sul vh www.sistemapiemonte.it.

NOTA: la scelta dell'Identity Provider su cui verranno autenticati gli utenti dipende dal valore di PORTALEAUTH dell'applicationId indicato nel contesto web. Non ci sono vincoli su quali Identity Provider possono autenticare gli utenti di un servizio esposto su un VH; pertanto, è possibile chiedere più contesti web per il proprio servizio protetti da shibboleth per autenticare utenti di diverse comunità.

NOTA: sul web server deve essere installato e configurato il mod_shib2. L'elenco dei web server e dei VH per cui Shibboleth è configurato nella filiera aziendale è riportato in [4]

NOTA: la richiesta del contesto web con direttive Shibboleth va fatta al gruppo che gestisce l'ambiente

- Sviluppo: richiesta tramite PAST
- Test: richiesta tramite PAST
- Collaudo: inserendo le direttive del contesto web nella documentazione di rilascio
- Esercizio: inserendo le direttive del contesto web nella documentazione di rilascio

NOTA: la protezione di un contesto web con shibboleth comporta la protezione di tutte le risorse contenute in tale contesto. Se si ha necessità di proteggere solo alcune risorse di un applicativo web, è necessario definire la location per shibboleth in modo che vengano protette solo tali risorse. Si veda [2] per maggiori indicazioni

3.2 Passo 1: Richiesta contesto shibboleth variante CIFA

Nel caso dell'Identity Provider CIFA, il Service Provider deve riportare nella nomenclatura anche l'Ente a cui il Service Provider appartiene. A titolo di esempio si riporta una configurazione da richiedere per una web application con contesto shibclient:

```
<Location /shibclient >
  ShibRequestSetting applicationId APPLICATION_ENTE_VH_LIVX_PORTALEAUTH
  AuthType shibboleth
  ShibRequireSession On
  ShibUseHeaders On
  require valid-user

# <... direttive legate all'application server>

</Location>
```

Un applicativo può scegliere il livello di autenticazione minimo necessario per accedere alle funzionalità.

Le scelte possibili sono:

- livello 1: a questi servizi l'utente può accedere con un/pwd, un/pwd/PIN
- livello 2: a questi servizi l'utente può accedere con un/pwd/PIN

La modalità con cui si effettua la scelta del livello di autenticazione è attraverso la definizione della location.

Il parametro ShibRequestSetting applicationId **APPLICATION_ENTE_VH_LIVX_PORTALEAUTH** può assumere i seguenti valori

- **ENTE**: è l'identificativo, ovvero codice ipa, dell'Ente a cui appartiene il Service Provider
- **VH**: è il nome del virtual host di produzione su cui viene configurata la location
- **LIVX**: assume i valori LIV1, LIV2 a seconda del livello minimo di autenticazione scelto dall'applicativo;
- **PORTALEAUTH**: identifica il VH di esposizione dell'IDP usato per l'autenticazione.

Il valore di ENTE, PORTALEAUTH e i VH di esposizione della componente sono:

Componente	Identity Provider SAML	Ente	PORTALEAUTH	VH
IDPCIFA	Identity Provider Città Facile	Codice IPA dell'ente	CIFA	https://identity.csipiemonte.it/

3.2.1 Service Provider CIFA

L'Identity Provider CIFA deve essere usato solo per gli operatori di Città Facile e/o operatori Enti fuori Regione.

Non saranno definiti Service Provider federati con CIFA sui web server della webfarm Enterprise CSI. I Service Provider, con relativi webserver e virtual host, devono essere riferiti all'Ente a cui lo stesso appartiene.

3.2 Passo 2: Configurazioni dell'applicativo

Gli Identity Provider forniscono all'applicazione web un set di attributi riportati in 3.2.1.

Nel par. 3.2.3 è riportata, a titolo di esempio, una jsp che recupera gli attributi restituiti da un Identity Provider Shibboleth.

3.2.1 Attributi forniti

Gli attributi da recuperare nel header http sono:

Nome header	Contenuto
Shib-Identita-Nome	nome
Shib-Identita-Cognome	cognome
Shib-Identita-CodiceFiscale	codice fiscale
Shib-Identita-LivAuth	livello di autenticazione che può assumere uno dei valori definiti in [7]
Shib-Iride-IdentitaDigitale	identità digitale IRIDE
Shib-Identita-TimeStamp (*)	istante in cui è stata operata l'autenticazione
Shib-Identity-Provider (*)	campo di interesse solo per IRIDE, rappresenta il provider di identità che ha riconosciuto l'utente e responsabile delle credenziali fornita
Shib-Identita-loa	livello di autenticazione che può assumere uno dei valori definiti in [7]
Shib-idpUrl	URL di disconnect dell'IDP
Shib-community	Comunità a cui appartiene l'utente. Può assumere ad esempio: DIPENDENTE_CRP DIPENDENTE_PA CITTADINO DIPENDENTE_PROVINCIA_TORINO DIPENDENTE_REGIONE_PIEMONTE DIPENDENTE_CSI <ENTE_APPARTENENZA> (per CIFA)
Shib-Identita-Riscontro (solo per IAMIDPSP)	Per autenticazione con user, password e PIN: <ul style="list-style-type: none"> • S per utente riscontrato allo sportello • N non riscontrato Per autenticazione con username e password e certificato assume valore vuoto
Shib-Identita-Matricola (solo per IAMIDPCSI e IAMIDPCRP)	Matricola
Shib-Mail (solo per IAMIDPCRP, IDPCIFA)	E-mail dell'utente

Shib-Tipo-Risorsa (solo per IAMIDPCSI e IAMIDPCRP)

Può assumere i seguenti valori:

IAMIDPCSI

- csi_piemonte = dipendente CSI;
- csi_piemonte_consulenti = consulente/collaboratore CSI

IAMIDPCRP

- cr_piemonte = dipendente CRP;
- cr_piemonte_consulenti = consulente/collaboratore CRP

NOTA: Per quanto riguarda l'attributo identità digitale, si tratta di un codice univoco dell'avvenuta autenticazione usato da IRIDE. Prende la forma di una stringa in cui vi sono alcuni campi separati dal carattere "/" secondo questo formato:

<nome>/<cognome>/<codice fiscale>/<codice provider IRIDE>/<livello di autenticazione>/<timestamp>/<codice di verifica>

Dove:

Campo	Significato
codice provider IRIDE	campo di interesse solo per IRIDE, rappresenta il provider di identità che ha riconosciuto e garantisce le credenziali
livello di autenticazione	Può assumere i seguenti valori: 1 = username e password di utenti auto-registrati; 2 = username e password di utenti con identità verificati; 4 = username, password e PIN di utenti con identità verificati; 8 = certificati X.509 di CA non qualificate; 16= certificati X.509 di CA qualificate
timestamp	istante in cui è stata operata l'autenticazione
codice di verifica	campo usato internamente da IRIDE

NOTA: il livello di autenticazione presente nell'attributo Shib-Iride-IdentitaDigitale è quello gestito da IRIDE i cui valori sono descritti in tabella.

NOTA: l'attributo che contiene l'identità digitale (Shib-Iride-IdentitaDigitale) è necessario per utilizzare i servizi di autorizzazione offerti da IRIDE. Nel caso l'applicativo utilizzi solo i servizi di autenticazione e non si appoggi alla successiva profilazione di IRIDE, tale attributo può essere ignorato poiché le informazioni di autenticazione in esso contenute sono già disponibili negli attributi Shib-Identita-Nome, Shib-Identita-Cognome e Shib-Identita-CodiceFiscale.

NOTA: alcuni attributi forniti dall'IdP possono non essere valorizzati. Questo dipende dal fatto che alcune tipologie di credenziali presentate dall'utente possono non avere alcuni attributi. È il caso di alcune CNS (Carta Nazionale Servizi) nelle quali nome e cognome non sono presenti nel certificato di autenticazione e quindi non possono essere reperiti dall'IdP. In tal caso, nome e cognome e i rispettivi attributi dell'identità digitale saranno valorizzati con la stringa "-" (trattino)

NOTA: si richiede (solo per alcuni service provider esterni a CSI) all'utente cittadino il consenso per l'invio dei dati personali (codice fiscale, nome, cognome) ad un servizio terzo. Se l'utente non accetta

e l'autenticazione è andato a buon fine, gli attributi nome, cognome e codice fiscale e i rispettivi valori dell'identità digitale saranno valorizzati con una stringa predefinita ("UTENTE NON ACCETTA INFORMATIVA")

NOTA: è disponibile una libreria realizzata dalla direzione DP che centralizza il reperimento delle informazioni di interesse dall'header http. Per maggiori informazioni si veda [5]

NOTA: L'attributo **Shib-Identita-Riscontro** è fornito solo dall' identity provider IAMIDPSP nel caso di autenticazione con livello 2. L' attributo assume valore S se è avvenuto il riscontro allo sportello, "de visu", dell'utente, altrimenti valore N. L'attributo assume valore nullo per il livello di autenticazione 1, username e password, e per il livello 3, autenticazione con certificato.

3.2.2 Attributi forniti da IDPSOCIAL

Gli attributi forniti dall'IdP da recuperare nel header http sono:

Nome header	Contenuto
Shib-Identita-Cognome	Cognome
Shib-Identita-Nome	Nome
socialUniqueID	Codice univoco
socialMail	Indirizzo email

3.2.3 Recupero attributi header http

Un esempio di jsp che recupera attributi:

```
<u><b>SHIB HEADERS</b></u><br/>

<table>

<%

String h = null;

java.util.Enumeration headers = request.getHeaderNames();

while (headers != null && headers.hasMoreElements()) {

    h = (String)headers.nextElement();

    %>

    <%

        if (!h.equals("Shib-Attributes") && !h.equals("Shib-Application-ID") &&
            ((h.startsWith("Shib-") || h.equalsIgnoreCase("remote_user")))) {

            %>

                <tr><td><%= h %> is: </td><td><b><%= request.getHeader(h)
            %></b></td></tr>

        <%

    %>
```

```
}  
  
%>  
  
<% } %>
```

NOTA: è disponibile una libreria che centralizza il reperimento delle informazioni di interesse dall'header http. Si veda [5]

NOTA: gli attributi che restituisce l'Identity Provider arrivano in get e vengono recuperati da header http. Per questo motivo si consiglia di decodificare sempre i singoli valori attraverso la codifica dei caratteri Unicode (UTF-8)

Per altri esempi di lettura degli attributi da applicazioni scritte in altri linguaggi, si veda [4]

3.3 Passo 3: Gestione logout

Un applicativo per eseguire il logout dovrà richiamare una url del tipo:

<protocollo>:<vh-sp><:porta>/<contesto hurl>/Shibboleth.sso/Logout

dove <contesto hurl> è definito in [5] ed è dipendente dal **APPLICATION_VH_LIVX_PORTALEAUTH**

Chiamando questa url verrà cancellata la sessione del SP e richiamata la url per disconnettere l'utente dall'IdP su cui si è autenticato (NB: se si prevede di autenticare utenti su IdP diversi occorrerà chiamare il **<contesto hurl>/** relativo al corretto APPLICATION_VH_LIVX_PORTALEAUTH. L'utente verrà quindi rediretto su una url di post logout definita sulla base del valore di APPLICATION_VH_LIVX_PORTALEAUTH

3.4 Passo 3: Gestione logout variante CIFA

Un applicativo per eseguire il logout dovrà richiamare una url del tipo:

<protocollo>:<vh-sp><:porta>/<contesto hurl>/Shibboleth.sso/Logout

dove <contesto hurl> è definito in [5] ed è dipendente da **APPLICATION_ENTE_VH_LIVX_PORTALEAUTH**

Chiamando questa url verrà cancellata la sessione del SP e richiamata la url per disconnettere l'utente dall'IdP su cui si è autenticato (NB: se si prevede di autenticare utenti su IdP diversi occorrerà chiamare il **<contesto hurl>/** relativo al APPLICATION_ENTE_VH_LIVX_PORTALEAUTH. L'utente verrà quindi rediretto su una url di post logout definita sulla base del valore di APPLICATION_ENTE_VH_LIVX_PORTALEAUTH

4. Approfondimenti sulle Sessioni

L'integrazione con Shibboleth comporta la creazione di sessioni sulle diverse componenti del framework di autenticazione. La comprensione delle sessioni create e della loro durata permette di utilizzare e configurare al meglio la protezione del contesto web del proprio applicativo.

È l'identity provider Shibboleth a farsi carico della gestione del SSO dell'utente sui diversi servizi applicativi protetti dall'identity provider.

Quando l'utente accede ad uno o più servizi tramite shibboleth vengono aperte diverse sessioni, la maggior parte di queste sessioni sono mantenute attraverso cookies. Le tipologie di sessione create sono:

- **sessioni collegate al IdP:** sessione utente, sessione legata al metodo di autenticazione. Sono utilizzate per fornire il SSO, eliminando la necessità di un'ulteriore autenticazione.
- **sessioni collegate al SP:** sessione utente
- **sessioni lato applicativo:** ogni applicazione può (e di solito lo fa) mantenere sessioni distinte con il browser.

Tutte queste sessioni sono distinte e più o meno indipendenti le une dalle altre: ogni sessione può esistere con o senza le altre, e la scadenza di una qualunque di esse non implica la scadenza delle altre.

4.1 Scadenza sessioni

Di seguito viene descritto il comportamento del sistema in caso di scadenza delle sessioni.

Scadenza sessione applicativa:

- se sono su un contesto protetto da shibboleth allora viene verificata la sessione del service provider
- se sono su un contesto non protetto da shibboleth allora termina la fruizione dell'applicativo (e le altre sessioni potrebbero rimanere vive).

Scadenza sessione service provider:

- scade dopo il tempo di vita
- scade se l'utente non fa nessuna operazione per inattività

Se l'utente chiama un contesto protetto da shibboleth dopo la scadenza della sessione (indipendentemente dalla sessione applicativa) allora l'utente viene rediretto sull'IdP, dove se esiste ancora la sessione dell'IdP non viene nuovamente autenticato

Scadenza sessione dell'identity provider:

- scade per inattività. All'utente viene richiesta una nuova autenticazione (l'utente arriva sull'identity provider solo a seguito della scadenza della sessione sul service provider)

Esempi:

1. un utente accede ad un applicativo x protetto da un service provider, poi accede ad un applicativo y protetto dallo stesso service provider dopo un tempo minore del tempo di sessione del service provider. Il service provider non contatta l'IdP per l'autenticazione e permette l'accesso all'utente;
2. un utente accede ad un applicativo x protetto da un service provider, poi accede ad un applicativo y protetto dallo stesso service provider dopo un tempo maggiore del tempo di sessione del service provider. Il service provider contatta l'IdP per l'autenticazione, se il tempo di sessione dell'IdP non è superato l'utente non si deve riautenticare, se il tempo di sessione dell'IdP è superato l'utente deve reinserire le credenziali per l'autenticazione;
3. un utente accede ad un applicativo x protetto da un service provider, poi accede ad un applicativo y protetto da un altro service provider. Il service provider contatta l'IdP per l'autenticazione, se il tempo di sessione dell'IdP non è superato allora l'utente non si deve riautenticare, se il tempo di sessione dell'IdP è superato allora l'utente deve reinserire le credenziali per l'autenticazione.

5. Appendice A: Glossario

SHIBBOLETH

Architettura che permette la comunicazione tra IdP , SP e WAYF secondo protocolli standard.

IDP

Identity Provider Shibboleth. È l'entità che attesta credenziali di utenti.

SP

Service Provider Shibboleth. È l'entità che eroga servizi applicativi.

WAYF

È l'entità che indirizza un utente all'Identity Provider in grado di riconoscere le sue credenziali. Non necessariamente sempre presente in un'architettura Shibboleth.

SOAP

Protocollo leggero per lo scambio di messaggi tra componenti software. SOAP può muoversi sopra tutti i protocolli di Internet, ma HTTP è il più comunemente utilizzato e l'unico ad essere stato standardizzato dal W3C. SOAP si basa sul metalinguaggio XML

SAML

Security Assertion Markup Language. È uno standard XML che permette lo scambio di autenticazione e autorizzazione. È un prodotto di OASIS Security Services Technical Committee.

HTTP

È l'acronimo di **HyperText Transfer Protocol** (protocollo di trasferimento di un ipertesto). Usato come principale sistema per la trasmissione di informazioni sul web. Le specifiche del protocollo sono attualmente in carica al W3C (World Wide Web Consortium).

HEADER HTTP

Porzione della richiesta e della response http.

SSO

Il Single sign-on (SSO, traducibile come autenticazione unica o identificazione unica) è un sistema specializzato che permette a un utente di autenticarsi una sola volta e di accedere a tutte le risorse informatiche alle quali è abilitato.

MOD SHIB

Modulo shibboleth che si configura su web server Apache. È materializzato da un processo, un demone sotto Unix o un servizio sotto Windows, in grado di parlare con un IdP secondo i profili previsti dalle specifiche Shibboleth.

MOD WL

Plug-in che si configura su web server Apache. Permette di far transitare richieste da Apache HTTP Server a WebLogic Server.