FedERa - Specifiche di integrazione con la procedura di logout federato

Revisione 1.2.0

Cronologia delle revisioni

Numero	Data	Descrizione
1.0.0	22/10/2013	Stesura iniziale
1.1.0	31/05/2016	Aggiunta caso particolare di richiesta di logout proveniente da un servizio di un Service Provider
1.2.0	22/05/2018	Adeguato url di logout di federa per evitare redirect in caso di invocazione con metodo POST, che causa perdita del form-data

Introduzione

Questo documento descrive lo scenario di logout federato all'interno dell'infrastruttura FedERa, e le specifiche che devono adottare Service Provider e Identity Provider affinchè la procedura abbia luogo.

Descrizione

Il logout federato permette ad un utente autenticato in FedERa che ha eseguito l'accesso ad un servizio offerto da un Service Provider, di effettuare in un'unica operazione il logout dall'intera federazione.
Il logout dall'intera federazione consiste nell'eliminazione della sessione utente all'interno delle seguenti entità:

- Service Provider presso cui l'utente aveva acceduto autenticandosi tramite FedERa, e nel quale esprime la volontà di effettuare il logout.
- Gateway FedERa. La sessione dell'utente nel Gateway FedERa permette la funzionalità di SSO (Single Sign On), non richiedendo di nuovo di autenticarsi all'utente che cerca ad altri Service Provider appartenenti allo stesso COT (Circle Of Trust) in cui risiede il Service Provider presso il quale ha avuto accesso autenticandosi tramite FedERa.
- Identity Provider presso cui l'utente si è autenticato per accedere al Service Provider.

Legenda

SP	Service Provider
GW	Gateway Multiprotocollo FedERa
IDP	Identity Provider
IDP interno	IDP localizzati fisicamente all'interno dell'infrastruttura FedERa, gestiti direttamente da Lepida
IDP esterno	IDP federati, localizzati fisicamente al di fuori dell'infrastruttura e implementati e gestiti

	direttamente dall'ente amministratore

Specifiche per gestori di SP

L'SP deve creare un servizio di logout che:

- cancella la sessione dell'utente autenticato (in genere cancellerà i cookie di sessione del servizio stesso).
- redirige l'utente al servizio di logout di FedERa (https://federa.lepida.it/logout/), inviando tramite GET oppure POST gli attributi:
    - "spid", con valore:
        - uguale all'entityid del SP, se la richiesta di logout è per il SP in cui l'utente si è autenticato.
        - uguale all'entityid del SP seguito dalla stringa "%23" e un numero pari al valore dell'attribute consuming service index del servizio in questione (esposto nei metadata del SP), se la richiesta di logout è per uno specifico servizio del SP in cui l'utente si è autenticato.
    - "spurl", con valore uguale all'url a cui l'SP vuole che l'utente venga redirezionato al termine della procedura di logout.
      il valore di tale attributo deve essere in formato x-www-form-urlencoded.
      (http://www.w3schools.com/tags/ref_urlencode.asp)

Specifiche per gestori di IDP esterni

L'IDP esterno deve creare un servizio di logout che:

- riceve tramite GET gli attributi:
    - "spid", con valore uguale all'entityid del SP.
    - "spurl", con valore uguale all'url a cui l'SP vuole che l'utente venga redirezionato al termine della procedura di logout.
- cancella la sessione dell'utente autenticato sull'IDP.
- redirige l'utente al servizio di logout di FedERa (https://federa.lepida.it/logout/), inviando tramite GET oppure POST gli attributi:
    - "spid", con valore uguale all'attributo GET "spid" ricevuto.
    - "spurl", con valore uguale all'attributo GET "spurl" ricevuto.
      il valore di tale attributo deve essere in formato x-www-form-urlencoded.
      (http://www.w3schools.com/tags/ref_urlencode.asp)
    - "idpid", con valore uguale all'entityid dell'IDP.

Affinchè venga censito in FedERa e reso utilizzabile il servizio di logout dell'IDP esterno, il gestore dell'IDP deve comunicare agli amministratori del GW (serviziabilitanti@lepida.it, gianluca.casati@lepida.it):

- l'entityid dell'IDP
- l'url del servizio di logout fornito dall'IDP

Casi d'uso risultanti

Di seguito, a seconda dell'evento che accade, viene riportato lo stato della sessione dell'utente presso ogni entità, e l'output per l'utente presso l'entità della federazione in cui si ferma la procedura di logout federato.

Se la sessione utente viene rimossa, viene inserito tra parentesi un numero caratterizzante l'ordine di rimozione della sessione all'interno del processo di logout federato.

Se l'utente si è autenticato presso un IDP interno:

Evento	SESSIONE SU SP	SESSIONE SU GW E TUTTI GLI IDP INTERNI
Il SP non invia correttamente al GW gli attributi GET o POST	RIMOSSA (1)	ATTIVA Output: pagina di errore
Il logout avviene correttamente in ogni entità	RIMOSSA (1)	RIMOSSA (2) Output: pagina di avvenuto logout, con link per tornare al SP

Se l'utente si è autenticato presso un IDP esterno:

Evento	SESSIONE SU SP	SESSIONE SU GW	SESSIONE SU IDP ESTERNO
Il SP non invia correttamente al GW gli attributi GET o POST	RIMOSSA (1)	ATTIVA Output: pagina di errore	ATTIVA
L'IDP non fornisce un servizio di logout	RIMOSSA (1)	ATTIVA Output: pagina di errore	ATTIVA
L'IDP fornisce un servizio di logout che non rimuove la sessione e non redireziona poi l'utente al GW	RIMOSSA (1)	ATTIVA	ATTIVA Output: pagina desiderata dall'IDP
L'IDP fornisce un servizio di logout che non invia correttamente al GW gli attributi GET o POST	RIMOSSA (1)	ATTIVA Output: pagina di errore	RIMOSSA (2)
Il logout avviene correttamente in ogni entità	RIMOSSA (1)	RIMOSSA (3) Output: pagina di avvenuto logout, con link per tornare al SP	RIMOSSA (2)