SPA-INT

SVILUPPI PERCORSI AZIENDALI - INTEGRAZIONE

SPECIFICHE PER FORNITORI

P1.3-15

PORTALE SOLE - SINGLE SIGN ON

Sostituisce o modifica			
Versione|stato	**Data**	**Oggetto**	**Commento**
1.2/finale	03/07/2013	Documentazione tecnica per fornitori – Portale SOLE Single Sign On	Il nuovo deliverable "P1.3-15 SPF Portale SOLE – Single Sign On" sostituisce il precedente documento di specifiche per uso interno "Documentazione tecnica per fornitori – Portale SOLE Single Sign On", e diventa il nuovo deliverable di riferimento.

Storia delle versioni			
Versione|stato	**Data**	**Autore**	**Sintesi**
1.0/finale	27/04/2015	Alberto Morselli	Prima versione finale

Limiti di utilizzo del documento
La circolazione di questo documento è autorizzata unicamente ai soggetti che partecipano attivamente ai progetti e Servizi ICT per l'area sanitaria e socio sanitaria nei limiti della realizzazione dello stesso. Ogni altro utilizzo in contrasto con il limite suddetto o comunque non autorizzato sarà perseguito a termini di legge.

Scheda Riassuntiva Documento

PROGETTO	
Progetto	**Sviluppi Percorsi Aziendali - Integrazione**
Acronimo Progetto	**SPA-INT**
Capo Progetto	**Cesare Osti**
Referente Regionale	**Fabio Rombini**
Responsabile BU	**Caterina Lena**
Data inizio Piano Operativo	**01/01/2015**
Data fine Piano Operativo	**31/12/2015**
Attività di riferimento	**WP1.1.3**

DOCUMENTO	
Dominio	**SOLE nuovi sviluppi**
Responsabile Tecnico	**Alberto Morselli**
Tipologia	**Specifiche per Fornitori**
Titolo Documento	**Portale SOLE - Single Sign On**
Identificativo	**P1.3-15**
Autore	**Alberto Morselli**
Versione|Stato	**1.0|Finale**
Data	**27/04/2015**
File	c:\documents and settings\mz01\documenti\bozze di sharepoint\p1.3-15 spf portale sole single sign on.doc

Abstract:	Il documento riporta le specifiche per i fornitori che intendano integrarsi con il Single Sign On del Portale SOLE

Keywords:	Portale SOLE, Single Sign On, applicativi esterni

INDICE

INDICE DELLE FIGURE

Non è stata trovata alcuna voce dell'indice delle figure.

1 Introduzione

Scopo del presente documento è fornire una guida ai fornitori che si integreranno con il Single Sign On (a seguire SSO) del Portale SOLE.

La richiesta di autenticazione mediante il meccanismo del SSO può avvenire:

- da Portale SOLE su applicativo esterno
- da applicativo esterno su Portale SOLE

Alcuni sistemi, in seguito all'autenticazione mediante SSO, utilizzano il sistema di web service del Portale SOLE per recuperare le informazioni relative all'utente autenticato (in particolare, il ws getSUtente). Si veda il documento [P1.3-15 SPF Portale SOLE WS] per le specifiche sui web service del Portale SOLE.

2 Single Sign On

2.1 Dataset e gestione della sicurezza

2.1.1 SSO - Richiesta di autenticazione da Portale SOLE verso applicativo esterno

2.1.1.1 Data set

2.1.1.1.1 Input

Ogni invocazione in SSO da un applicativo esterno verso il Portale SOLE dovrà contenere i seguenti parametri:

Dato	Descrizione	Obbligatorietà
ssotimestamp	è un parametro che viene utilizzato per le funzioni di sicurezza nell'invocazione delle richieste SSO e deve contenere la data della richiesta nel formato *yyyymmddhhmmss*, ovvero anno mese giorno ora (da 0 a 23) minuti e secondi	OBB
ssomac	è un codice di controllo calcolato in modo specifico per ogni chiamata. Le modalità di calcolo verranno descritte di seguito	OBB
username	è lo username dell'utente censito sul Portale SOLE	OBB
identity	è un numero che identifica l'identità con cui l'utente sta operando sul Portale SOLE e con la quale dovrà accedere all'applicativo	OBB
dominio	è il dominio sul quale dovrà essere effettuato il	OBB

	SSO. Se l'utente, dopo essersi correttamente autenticato sull'applicativo esterno, vuole tornare al portale SOLE, selezionerà una funzionalità del tipo "torna al portale" prevista sull'applicativo stesso, che riporta la navigazione sulla home del portale SOLE. Il campo "dominio" serve a costruire questo link.	

Per garantire la sicurezza, ad ogni fornitore verrà assegnato un Codice di Sicurezza (*CdS*) che deve essere utilizzato nel calcolo del *ssomac*. Tale codice non verrà usato in nessun caso nella composizione degli URL delle chiamate.

Il *CdS* viene utilizzato per comporre una stringa di controllo, formata dal concatenamento dei valori di *ssotimestamp*, *CdS*, *username*, *identity* e *dominio* (separati, preceduti e seguiti dal carattere #) a cui deve essere applicata la funzione di hash MD5. Il campo *ssomac* viene quindi calcolato trasformando in maiuscolo la stringa così ottenuta.

Il codice *ssomac* deve avere le tutte le lettere maiuscole.

L'ordine dei campi con cui viene composta la stringa è ovviamente fondamentale per il corretto calcolo del campo *ssomac*.

In PHP ciò si traduce nell'istruzione:

```
$ssomac = strtoupper(MD5(
    '#'.$ssotimestamp.'#'.$CdS.'#'.$username.'#'.$identity.'#'.$dominio. '#'
));
```

Esempio chiamata SSO:

Per *CdS*='123456789', la chiamata da effettuare è ad esempio:

```
https://www.applicativo.it/ssologin?
ssotimestamp=20120315143117&
ssomac=57C556518DD9EEC71793209FA7DCD2FB&
username=wsportalesole&identity=9532&dominio=www.progetto-sole.it
```

2.1.1.1.2 Comportamento del SSO

All'invocazione del SSO, l'applicativo invocato provvederà a controllare i dati ricevuti.

Verrà ricalcolato il valore di *ssomac* in funzione di tali valori e verrà confrontato con quello ricevuto.
Un ulteriore controllo verrà fatto sul *ssotimestamp* che dovrà differire al massimo di 5 minuti rispetto all'orario di sistema del server.
Superati i controlli, l'applicativo autorizzerà la richiesta e autenticherà l'utente per operare sul sistema.

2.1.2 SSO - Richiesta di autenticazione da SSI verso Portale SOLE

2.1.2.1 Data set

2.1.2.1.1 Input

Ogni invocazione in SSO da un applicativo esterno verso il Portale SOLE dovrà contenere i seguenti parametri:

Dato	Descrizione	Obbligatorietà
ssoapplicationid	è un codice che viene comunicato al fornitore e che lo identifica univocamente all'interno del Portale SOLE	OBB
ssotimestamp	è un parametro che viene utilizzato per le funzioni di sicurezza nell'invocazione delle richieste SSO e deve contenere la data della richiesta nel formato *yyyymmddhhmmss*, ovvero anno mese giorno ora (da 0 a 23) minuti e secondi	OBB
ssomac	è un codice di controllo calcolato in modo specifico per ogni chiamata. Le modalità per il calcolo verranno descritte successivamente	OBB
username	è lo username dell'utente censito sul Portale	OBB

	SOLE	
identity	è un numero che identifica l'identità con cui l'utente dovrà accedere al Portale SOLE	OBB

Per garantire la sicurezza, ad ogni fornitore verrà assegnato, oltre al ssoapplicationid, un Codice di Sicurezza (*CdS*) che deve essere utilizzato nel calcolo del *ssomac*. Tale codice non deve essere usato in nessun caso nella composizione degli URL delle chiamate o nelle invocazioni dei web service.

Il *CdS* deve essere utilizzato per comporre una stringa di controllo, formata dal concatenamento dei valori di *ssoapplicationid*, *ssotimestamp*, *CdS*, *username* e *identity* (separati, preceduti e seguiti dal carattere #) a cui deve essere applicata la funzione di hash MD5. Il campo *ssomac* viene quindi calcolato trasformando in maiuscolo la stringa così ottenuta.

Il codice *ssomac* deve avere le tutte le lettere maiuscole.

L'ordine dei campi con cui viene composta la stringa è ovviamente fondamentale per il corretto calcolo del campo *ssomac*.

In PHP ciò si traduce nell'istruzione:

```
$ssomac = strtoupper(MD5(
    '#'.$ssoapplicationid.'#'.$ssotimestamp.'#'.$CdS.'#'.$username.'#'.$identity.'#'
));
```

2.1.2.1.2 Comportamento del SSO

All'invocazione del SSO, il Portale SOLE provvederà a controllare i dati ricevuti.

Verrà ricalcolato il valore di *ssomac* in funzione di tali valori e verrà confrontato con quello ricevuto.

Un ulteriore controllo verrà fatto sul *ssotimestamp* che dovrà differire al massimo di 5 minuti rispetto all'orario di sistema del server.

Superati i controlli, il Portale SOLE autorizza la richiesta e autentica l'utente per operare sul sistema.

2.2 Parametri facoltativi

2.2.1 Modalità di trasmissione

Oltre ai parametri obbligatori appena visti, necessari per l'autenticazione, sarà possibile definire un insieme di campi facoltativi, che potrebbero servire per la fruizione di alcune funzionalità specifiche.
I nomi dei campi dovranno essere preventivamente concordati tra il Portale SOLE e l'applicazione integrata in SSO.

I campi facoltativi dovranno essere trasmessi (in entrambe le direzioni) inserendo un nuovo parametro nella richiesta SSO:

- ***params***: è una stringa contenente i campi facoltativi codificati.

I campi facoltativi dovranno formare un oggetto JSON di coppie chiave/valore (con codifica UTF8), che verrà criptato mediante l'algoritmo AES 128bit. Per effettuare l'operazione di crittazione viene usata come chiave la codifica MD5 del *CdS* già utilizzato nel calcolo del *ssomac*.
Il valore di params viene quindi calcolato effettuando la conversione in base64 della stringa criptata così ottenuta.

In PHP ciò si traduce nelle istruzioni:

```
/***********************
* Funzione di codifica *
***********************/

//Preparo l'array con i parametri
$parametri = array(
    'campo1' => 'valore1',
    'campo2' => 'valore2',
    ...
    'campoN' => 'valoreN'
);

//Cripto i dati
$key = strtoupper(md5($CdS));
$parametri = array_map('utf8_encode', $parametri);
```

```
$plaintext = json_encode($parametri);
$iv_size = mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC);
$iv = mcrypt_create_iv($iv_size, MCRYPT_RAND);
$ciphertext = mcrypt_encrypt(
    MCRYPT_RIJNDAEL_128, $key, $plaintext, MCRYPT_MODE_CBC, $iv
);
$ciphertext = $iv.$ciphertext;
$params = base64_encode($ciphertext);

//Uso i dati nella composizione della chiamata
$url = $url_per_sso . '&params=' . urlencode($params);

/*************************
* Funzione di decodifica *
*************************/

//Leggo i parametri dalla richiesta in GET
$params = $_GET['params'];

//Decripto i dati
$key = strtoupper(md5($CdS));
$ciphertext_dec = base64_decode($params);
$iv_size = mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC);
$iv_dec = substr($ciphertext_dec, 0, $iv_size);
$ciphertext_dec = substr($ciphertext_dec, $iv_size);
$plaintext_dec = mcrypt_decrypt(
    MCRYPT_RIJNDAEL_128, $key, $ciphertext_dec, MCRYPT_MODE_CBC, $iv_dec
);
$parametri = json_decode(trim($plaintext_dec), true);
$parametri = array_map('utf8_decode', $parametri);

//Uso i dati, contenuti in un array associativo
```

Esempio chiamata SSO:

Per *CdS*=`'123456789'` e utilizzando il seguente elenco di campi opzionali:

```
pagina = 'Main.php'
cfassistito = 'MRSLRT72A18A944D'
```

il valore del parametro params è ad esempio:

```
params=83pKmMKEv5z%2BHTmPknb6ZxcBYrE0aDDkdcIdsdGBJf7w9nuH0DQq0dkLcNAPym%2FwSX
jceN3B2Tj%2BSiEJc2YNcYzMiC5nsMop4PDZo9sdlAibpLWh6xC1X8RPpUh%2B9kw5
```

Si fa presente che in per il padding dei dati viene utilizzato l'algoritmo PKCS#7.

2.2.2 Parametri facoltativi già disponibili

CAMPO	APPLICAZIONE	USO
pagina	Tutti	Definisce la landing page da visualizzare dopo che è stato effettuato l'accesso SSO
cfassistito	ADI Online	Fornisce il codice fiscale dell'assisitito da visualizzare sul Fascicolo Professionisti
sourceappid	Portale SOLE	Se il Portale SOLE effettua una chiamata SSO, comunicando dei parametri opzionali che provengono da un precedente meccanismo di SSO da un applicativo terzo verso il Portale SOLE, in questo campo è presente l'identificativo interno di tale applicativo di origine.
destappid	Tutti	Definisce l'applicativoa cui l'utente deve accedere (valori disponibili FSEPROF).Se assente l'utente accede al Portale SOLE
typedoc	FSEPROF	Nel caso l'applicativo di destinazione sia FSE professionisti è possibile filtrare i documenti dell'assistito scelto con il parametro cfassistito Valori possibili: uno fra i seguenti PSS (Profilo sintetico stato di salute), REF (tutti i referti), LED (lettere di dimissione)
contesto	FSEPROF	Nel caso l'applicativo di destinazione sia FSE professionisti è possibile indicare il contesto di accesso Valori possibili: uno fra i seguenti AP (Accesso programmato), EU (emergenza/urgenza)

3 Gestione errori

All'invocazione del SSO, il Portale SOLE (nel caso di SSO da applicativo esterno) o l'applicativo esterno (nel caso di SSO da Portale SOLE) provvederanno a controllare i dati ricevuti.
Nel caso questi non vengano superati, verrà restituito un messaggio con errore di autenticazione.

4 Riferimenti

ID Riferimento	Descrizione
[P1.3-15 SPF Portale SOLE WS]	P1.3-15 "Specifiche per fornitori Portale SOLE – Web Service"