

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

CORSO DI LAUREA IN INFORMATICA



**Autenticazione per Zimbra Collaboration
Suite (ZCS) tramite protocollo SAML**

Tesi di laurea triennale

Relatore

Prof. Tullio Vardanega

Laureando

Francesco De Filippis

ANNO ACCADEMICO 2019-2020

Dedicato a ...

Sommario

Il presente documento descrive il lavoro svolto durante il periodo di stage, della durata di 304 ore, dal laureando Francesco De Filippis presso l'azienda Zextras S.r.l di Torri di Quartesolo (VI). Gli obiettivi da raggiungere erano molteplici.

La prima funzionalità richiesta dall'azienda era l'autenticazione di un utente presente su [Zimbra Collaboration Suite \(ZCS\)](#) attraverso l'[Identity Provider \(IdP\) Okta](#), il quale supporta il protocollo [Security Assertion Markup Language \(SAML\)](#). Oltre all'autenticazione per gli utenti già esistenti su [Zimbra](#) era richiesto anche il [Provisioning](#). In particolare si trattava di creare un nuovo account su [Zimbra](#) al primo tentativo di login dell'utente con conseguente autenticazione. I dati per la creazione dell'utente venivano forniti da [Okta](#) attraverso una [SAML Assertion](#). Utilizzando questi dati era richiesta la configurazione dell'account creato.

Il documento è così suddiviso:

- [Il primo capitolo](#) descrive l'azienda presso cui ho svolto lo stage. In particolare viene illustrata la sua storia, i suoi prodotti e il modo in cui opera;
- [Il secondo capitolo](#) descrive gli obiettivi dello stage in relazione alle aspettative aziendali e personali;
- [Il terzo capitolo](#) descrive le scelte progettuali che ho compiuto al fine di proporre una soluzione per soddisfare gli obiettivi prefissati dallo stage;
- [Il quarto capitolo](#) presenta una valutazione dello stage in relazione agli obiettivi dell'azienda e all'esperienza da me acquisita nel corso del suo svolgimento.

Indice

1	L'azienda	1
1.1	Profilo aziendale	1
1.2	Dominio applicativo	1
1.2.1	Zimbra Open Source Edition	1
1.2.2	Zextras Suite	2
1.3	Struttura interna	2
1.4	Processi aziendali	3
1.4.1	Fornitura	3
1.4.2	Comunicazione	3
1.4.3	Metodologia di sviluppo	3
1.4.4	Gestione di progetto	3
1.4.5	Configurazione	3
1.4.6	Documentazione	3
1.4.7	Verifica	3
2	Obiettivi dello stage	5
2.1	Presentazione del progetto	5
2.1.1	Analisi stato dell'arte protocolli di autenticazione	5
2.1.2	Progettazione di un sistema di autenticazione	5
2.2	Vantaggi aziendali	5
2.3	Vincoli	5
2.3.1	Vincoli metodologici	5
2.3.2	Vincoli temporali	5
2.3.3	Vincoli tecnologici	5
2.4	Aspettative aziendali	5
2.5	Aspettative personali	6
3	Resoconto dello stage	7
3.1	Descrizione del progetto	7
3.2	Analisi	7
3.3	Pianificazione	7
3.4	Scelta del protocollo di autenticazione	7
3.4.1	Confronto SAML e OpenID	7
3.4.2	SAML	7
3.5	Progettazione	7
3.5.1	Configurazione applicazione Okta	8
3.5.2	Progettazione handler HTTP	8
3.5.3	Configurazione Zimbra	8

3.6	Sviluppo	8
3.6.1	Parsing SAML assertion	8
3.6.2	Adattamento libreria HTTP	8
3.7	Verifica e Validazione	8
3.7.1	Verifica	8
3.7.2	Validazione	8
4	Valutazione retrospettiva	9
4.1	Soddisfacimento degli obiettivi	9
4.2	Conoscenze e abilità acquisite	9
4.3	Valutazione personale	9
	Glossario	11
	Bibliografia	13

Elenco delle figure

1.1	Logo Zextras	1
-----	------------------------	---

Elenco delle tabelle

Capitolo 1

L'azienda

1.1 Profilo aziendale

Zextras s.r.l. nasce a Torri di Quartesolo(VI) nel 2011 come estensione di **Studio Storti s.r.l.** che opera, dal 1997, nel campo delle soluzioni [open source](#). Sin dall'inizio, l'obiettivo principale di questa società era quello di estendere [Zimbra Open Source Edition](#), uno dei più diffusi strumenti collaborativi per aziende e pubbliche amministrazioni, aggiungendo nuove funzionalità.

Nel corso degli anni è nata e cresciuta **Zextras Suite**, una raccolta di estensioni che permettono di arricchire [Zimbra](#) con nuove funzionalità utili nel suo utilizzo in ambito professionale. Le soluzioni proposte da **Zextras** con i suoi prodotti vengono da subito apprezzate da **Synacor**, l'azienda che sviluppa e mantiene [Zimbra](#), la quale decide di includere parte del codice sviluppato dall'azienda nella sua versione [open source](#). Attualmente i prodotti sviluppati dall'azienda vengono utilizzati da più di 100 milioni di utenti in tutto il mondo.



Figura 1.1: Logo Zextras

1.2 Dominio applicativo

1.2.1 Zimbra Open Source Edition

Zextras, come già accennato, è nata con l'obiettivo di creare nuovi contenuti per [Zimbra](#) facendone quindi il suo *core business*. **Zimbra** è un software collaborativo di gruppo adatto a coordinare e supportare l'attività lavorativa sia di aziende sia di pubbliche amministrazioni. I principali servizi offerti da questo software sono i seguenti:

- posta elettronica;
- gestione calendari condivisi e organizzazione eventi;
- interfaccia amministratore;

- supporto dei servizi su dispositivi mobili.

Per estendere l'applicativo con ulteriori funzionalità sviluppate anche da terze parti, è possibile installare un [plug-in](#) che in ambiente [Zimbra](#) viene chiamato **Zimlet**.

Esistono due versioni di [Zimbra](#):

- **Zimbra Open Source Edition**: è la versione su cui lavora **Zextras** e offre i servizi eleganti in precedenza;
- **Zimbra Network Edition**: è una versione a pagamento che offre alcune funzionalità [closed source](#) tra cui un protocollo per la sincronizzazione di calendario e contatti e maggiori funzionalità per gli amministratori.

1.2.2 Zextras Suite

Zextras Suite è un'insieme di funzionalità che permettono di aggiungere delle funzionalità a [Zimbra Open Source Edition](#) in modo indipendente da quest'ultimo. Ciò permette una configurazione altamente modulare e personalizzabile in base alle necessità dell'utilizzatore.

Questa suite offre i seguenti prodotti:

- **Powerstore**: sistema di ottimizzazione dei dati che permette il risparmio di memoria sui server **Zimbra**;
- **Backup**: motore di [backup](#) in [real-time](#);
- **Admin**: strumenti dedicati agli amministratori per la gestione e il monitoraggio dei servizi attivi sull'istanza di [Zimbra](#);
- **Mobile**: gestione e sincronizzazione di posta elettronica, contatti, eventi e calendario su dispositivi mobili tramite protocolli *Exchange* e *EAS 16.0 (ActiveSync)*;
- **Chat**: piattaforma di messaggistica istantanea nativamente integrata in [Zimbra](#), che permette lo scambio di messaggi e di effettuare videochiamate;
- **Drive**: piattaforma per la condivisione di file e l'utilizzo di fogli di lavoro in modo condiviso.

1.3 Struttura interna

L'azienda è suddivisa in diversi settori specializzati, ciò permette di avere un organico fornito di tutte le competenze necessarie per raggiungere gli obiettivi aziendali. Di seguito un elenco che illustra i diversi settori:

- **Commercio**: ...;
- **Amministrazione di sistema**: ...
- **Team di sviluppo**:
 - **Front-end**: ...;
 - **Back-end**: ...;
 - **UI/UX Design**: ...;
 - **Mobile**:

1.4 Processi aziendali

1.4.1 Fornitura

1.4.2 Comunicazione

Strumenti utilizzati

1.4.3 Metodologia di sviluppo

1.4.4 Gestione di progetto

Strumenti utilizzati

1.4.5 Configurazione

Controllo di versione

Strumenti utilizzati

Bitbucket e Git

1.4.6 Documentazione

Strumenti utilizzati

1.4.7 Verifica

Strumenti utilizzati

Jenkins, ecc...

Descrizione della metodologia adottata in particolare nel contesto aziendale

Capitolo 2

Obiettivi dello stage

2.1 Presentazione del progetto

Descrizione del progetto proposto dall'azienda

2.1.1 Analisi stato dell'arte protocolli di autenticazione

Descrizione dell'attività di analisi e di studio dei protocolli di autenticazione che ho dovuto condurre come prima attività durante lo stage.

2.1.2 Progettazione di un sistema di autenticazione

Descrizione della soluzione proposta per l'implementazione del sistema di autenticazione

2.2 Vantaggi aziendali

Disamina sulle motivazioni dell'azienda ad ospitare uno stage di questo genere e quali vantaggi potesse trarne

2.3 Vincoli

Descrizione e motivazione delle tipologie di vincoli sotto i quali questo stage si è svolto

2.3.1 Vincoli metodologici

2.3.2 Vincoli temporali

2.3.3 Vincoli tecnologici

2.4 Aspettative aziendali

Descrizione degli output che l'azienda si aspettava da questo stage

2.5 Aspettative personali

Descrizione di ciò che io mi aspettavo al momento della scelta di questo stage

Capitolo 3

Resoconto dello stage

3.1 Descrizione del progetto

Descrizione dettagliata del progetto

3.2 Analisi

Descrizione dell'analisi dei requisiti e descrizione di alcuni dei requisiti

3.3 Pianificazione

Descrizione di come ho pianificato lo sviluppo del progetto rispettando i vincoli descritti in precedenza e le esigenze dell'azienda

3.4 Scelta del protocollo di autenticazione

Descrizione delle motivazioni che hanno portato alla scelta del protocollo SAML in seguito all'analisi svolta

3.4.1 Confronto SAML e OpenID

Breve confronto di due protocolli rispetto al problema da risolvere

3.4.2 SAML

Descrizione del protocollo SAML

3.5 Progettazione

Progettazione della soluzione proposta per l'implementazione del sistema di autenticazione

3.5.1 Configurazione applicazione Okta

3.5.2 Progettazione handler HTTP

3.5.3 Configurazione Zimbra

3.6 Sviluppo

Alcuni dettagli di rilievo per quanto riguarda la parte implementativa. In particolare ciò che ho dovuto attuare per superare alcuni ostacoli

3.6.1 Parsing SAML assertion

3.6.2 Adattamento libreria HTTP

3.7 Verifica e Validazione

Descrizione dell'attività di verifica svolta e della validazione

3.7.1 Verifica

3.7.2 Validazione

Capitolo 4

Valutazione retrospettiva

4.1 Soddisfacimento degli obiettivi

Illustrazione degli obiettivi raggiunti rispetto a quelli attesi

4.2 Conoscenze e abilità acquisite

Descrizione di tutte le conoscenze e competenze acquisite sul piano tecnico e sul mondo del lavoro

4.3 Valutazione personale

Valutazione personale sullo di stage in relazione all'esperienza accademica

Glossario

Backup Quando si parla di backup, si fa riferimento al processo di duplicazione di dati su più supporti (fisici o cloud) al fine di poterli recuperare in caso di perdita inattesa. [2](#), [11](#)

Closed Source Con il termine **closed source** si fa riferimento ad un software proprietario, quindi non disponibile pubblicamente. [2](#), [11](#)

CRUD Questo acronimo viene spesso usato in ambito di **database management** e indica:

- **Create**: creazione di un utente;
- **Read**: richiesta attributi di un utente;
- **Update**: aggiornamento attributi di un utente;
- **Delete**: non si parla di una cancellazione vera e propria di un utente ma di **deprovisioning**, ovvero una disabilitazione dell'account di quest'ultimo o di un cambio di permessi

. [11](#)

IdP Un identity provider è un sistema che crea, mantiene e gestisce le informazioni sull'identità di un utente. Si occupa di fornire il servizio di autenticazione ai [SP](#). [11](#), [12](#)

Okta Okta è una società di gestione di identità e di accessi, quindi un [IdP](#). [v](#), [11](#)

Open Source Con il termine **open source** si fa riferimento ad un software la cui licenza permette di utilizzarlo, modificarlo e redistribuirlo. [1](#), [11](#)

Plug-in Componente software che aggiunge funzionalità all'applicazione su cui viene installato. [2](#), [11](#)

Provisioning Con il termine **provisioning** si intende, generalmente, la gestione degli utenti. Questo termine include un insieme di funzionalità riassunte dall'acronimo [CRUD](#). [v](#), [11](#)

Real-time Software che opera sotto condizioni temporali ben definite. [2](#), [11](#)

SAML SAML è un protocollo basato su [XML](#) che permette lo scambio di messaggi per effettuare autenticazione e autorizzazione tra domini distinti. Tipicamente gli attori del protocollo sono un [IdP](#) che fornisce l'identità dell'utente da autenticare e un [SP](#) che fornisce il servizio a cui l'utente ha richiesto l'accesso. . [12](#)

SAML Assertion Una asserzione **SAML** è un documento in formato **XML** che contiene le informazioni sull'autenticazione e/o autorizzazione di un utente. Tale documento è solitamente generato dall'**IdP** e inviato al **SP**. [v](#), [12](#)

SP Un service provider è un sistema che fornisce un servizio a degli utenti. Lo si può identificare come un sito web che eroga un certo servizio. [11](#), [12](#)

XML Linguaggio di **Markup** che consente la definizione di **metadati**. [11](#), [12](#)

ZCS Zimbra Collaboration. [v](#), [1](#), [2](#)

Bibliografia