**PEMBANGUNAN *SINGLE SIGN-ON* BERBASIS GO YANG CEPAT DAN RINGAN UNTUK AUTENTIKASI PENGUNA BERBASIS TOKEN**

**Laporan Tugas Akhir**

**Disusun sebagai syarat kelulusan tingkat sarjana**

**Oleh**

**Luqman Arifin Siswanto**

**NIM: 13513024**



**PROGRAM STUDI TEKNIK INFORMATIKA**

**SEKOLAH TEKNIK ELEKTRO & INFORMATIKA**

**INSTITUT TEKNOLOGI BANDUNG**

**2018**

**PEMBANGUNAN *SINGLE SIGN-ON* BERBASIS GO YANG CEPAT DAN RINGAN UNTUK AUTENTIKASI PENGUNA BERBASIS TOKEN**

**Laporan Tugas Akhir**

**Oleh**

**Luqman Arifin Siswanto**

**NIM: 13513024**

**Program Studi Teknik Informatika**

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung

Bandung, 3 Agustus 2018

Mengetahui,

Pembimbing,

Adi Mulyanto, ST., MT.

NIP. 19631126 198803 1 002

DAFTAR ISI

[DAFTAR ISI iii](#_Toc521360534)

[DAFTAR GAMBAR vi](#_Toc521360535)

[DAFTAR TABEL vii](#_Toc521360536)

[BAB I PENDAHULUAN 1](#_Toc521360537)

[I.1 Latar Belakang 1](#_Toc521360538)

[I.2 Rumusan Masalah 3](#_Toc521360539)

[I.3 Tujuan 4](#_Toc521360540)

[I.4 Batasan Masalah 4](#_Toc521360541)

[I.5 Metodologi 4](#_Toc521360542)

[I.6 Sistematika Pembahasan 5](#_Toc521360543)

[BAB II STUDI LITERATUR 7](#_Toc521360544)

[II.1 Autentikasi dan Autorisasi 7](#_Toc521360545)

[II.2 Sistem Autentikasi Identitas 8](#_Toc521360546)

[II.2.1 *Password* 8](#_Toc521360547)

[II.2.2 *Token* 9](#_Toc521360548)

[II.2.3 *Biometrics* 11](#_Toc521360549)

[II.2.4 Tanda Tangan Digital 11](#_Toc521360550)

[II.2.5 Sertifikat Digital 11](#_Toc521360551)

[II.3 *Multi-Factor Authentication* 12](#_Toc521360552)

[II.4 *Single Sign-On* 12](#_Toc521360553)

[II.5 *Web Single Sign*-*On* 16](#_Toc521360554)

[II.5.1 *Auth0* 16](#_Toc521360555)

[II.5.2 WSO2 *Identity Server* 19](#_Toc521360556)

[II.5.3 *Central Authentication Service (CAS)* 23](#_Toc521360557)

[II.5.4 *Java Open Single Sign-On (JOSSO)* 25](#_Toc521360558)

[II.6 Pekerjaan Terkait 26](#_Toc521360559)

[II.6.1 *CAS++* 26](#_Toc521360560)

[II.6.2 Kristanto, 2011 27](#_Toc521360561)

[BAB III ANALISIS PERMASALAHAN DAN RANCANGAN SOLUSI 29](#_Toc521360562)

[III.1 Analisis Permasalahan 29](#_Toc521360563)

[III.1.1 Auth0 29](#_Toc521360564)

[III.1.2 WSO2 *Identity Server* 30](#_Toc521360565)

[III.1.3 *Central Authentication Server* 31](#_Toc521360566)

[III.1.4 Perbandingan *Web Single Sign-On* 32](#_Toc521360567)

[III.2 Analisis Solusi 33](#_Toc521360568)

[III.2.1 Karakteristik *Web Single Sign-On* 33](#_Toc521360569)

[III.2.2 Kebutuhan Sistem 36](#_Toc521360570)

[III.2.3 Kebutuhan Fungsional *Single Sign-On* 38](#_Toc521360571)

[III.2.4 Kebutuhan Non-Fungsional *Single Sign-On* 39](#_Toc521360572)

[III.2.5 Diagram *Use Case* 40](#_Toc521360573)

[III.3 Rancangan Solusi 41](#_Toc521360574)

[III.3.1 Gambaran Umum Solusi 41](#_Toc521360575)

[III.3.2 Desain *Web* *Single Sign-On* 42](#_Toc521360576)

[III.3.3 Desain Aplikasi *Service Provider* 44](#_Toc521360577)

[BAB IV IMPLEMENTASI DAN EVALUASI 46](#_Toc521360578)

[IV.1 Lingkungan Implementasi 46](#_Toc521360579)

[IV.2 Batasan Implementasi 46](#_Toc521360580)

[IV.3 Implementasi 46](#_Toc521360581)

[IV.3.1 *Web Single Sign-On* 46](#_Toc521360582)

[IV.3.2 Aplikasi *Service Provider* 46](#_Toc521360583)

[IV.4 Evaluasi 46](#_Toc521360584)

[IV.4.1 Skenario Uji *Web Single Sign-On* 47](#_Toc521360585)

[IV.4.2 Kemudahan Integrasi 47](#_Toc521360586)

[IV.4.3 Keamanan 47](#_Toc521360587)

[IV.4.4 Ketergantungan terhadap Teknologi Tertentu 47](#_Toc521360588)

[IV.4.5 Kemampuan Autentikasi 47](#_Toc521360589)

[IV.4.6 Kemampuan Autorisasi 47](#_Toc521360590)

[IV.4.7 Kemampuan Manajemen Akun 47](#_Toc521360591)

[IV.4.8 Integrasi Sosial Media 47](#_Toc521360592)

[IV.4.9 Dukungan Dokumentasi 47](#_Toc521360593)

[DAFTAR PUSTAKA 48](#_Toc521360594)

DAFTAR GAMBAR

[Gambar ‎II.1 Sistem yang Mekanisme Autentikasinya tanpa SSO 14](#_Toc521360595)

[Gambar ‎II.2 Sistem dengan SSO 15](#_Toc521360596)

[Gambar ‎II.3 Cara Kerja Auth0 18](#_Toc521360597)

[Gambar ‎II.4 Arsitektur WSO2 *Identity Server* (WSO2, 2015) 20](#_Toc521360598)

[Gambar ‎II.5 Mekanisme WSO2 *Identity Server* 21](#_Toc521360599)

[Gambar ‎II.6 Mekanisme Kerja CAS 23](#_Toc521360600)

[Gambar ‎III.1 Sistem *Single Sign-On* 37](#_Toc521360601)

[Gambar ‎III.2 *Use Case Single Sign-On* 40](#_Toc521360602)

[Gambar ‎III.4 Arsitektur Minisso 43](#_Toc521360603)

[Gambar ‎III.5 Aplikasi *Service Provider* 45](#_Toc521360604)

DAFTAR TABEL

[Tabel ‎III.1 Perbandingan *Web Single Sign-On* 32](#_Toc521360605)

[Tabel ‎III.2 Karakteristik *Single Sign-On* 34](#_Toc521360606)

[Tabel ‎III.3 Kebutuhan Sistem 38](#_Toc521360607)

[Tabel ‎III.4 Kebutuhan Fungsional *Single Sign-On* 38](#_Toc521360608)

[Tabel ‎III.5 Kebutuhan Non-Fungsional *Single Sign-On* 39](#_Toc521360609)

# PENDAHULUAN

## Latar Belakang

Tren pengembangan perangkat lunak berevolusi dari waktu ke waktu. Di era 1980-an, orang cenderung mengembangkan aplikasi di *desktop*, pengembangan aplikasi berbasis *web* belum populer pada saat itu. Sementara itu, di masa kini, hampir semua aplikasi yang digunakan sudah berbasis *web* dan terkoneksi ke jaringan internet, walaupun tidak dipungkiri aplikasi *desktop* saat ini masih tetap digunakan.

Dengan bergesernya *trend* pengembangan aplikasi menuju ke arah berbasis internet, kini banyak juga yang perusahaan yang mengembangkan SaaS (*Software as a Service*) (Goth, 2008). Produk yang ditawarkan oleh perusahaan dapat diakses secara *real-time* dan langsung melalui internet. Banyak bidang yang menawarkan produknya melalui internet, seperti misalnya *e-commerce*, *banking*, *travel agent*, *e-government*, penyedia jasa infrastruktur, dan lain lain.

Banyak institusi yang menyediakan banyak *service* aplikasi sekaligus. Setiap aplikasi tentu membutuhkan *credential* untuk autentikasi dan autorisasi. Tidak efisien apabila tiap aplikasi dalam satu vendor yang sama memiliki mekanisme autentikasi sendiri-sendiri (Volchkov, 2001). Ini mengakibatkan redundansi *credential* yang sebenarnya tidak diperlukan.

Institusi biasanya memiliki lebih dari 70 aplikasi yang membutuhkan sistem supaya user dapat log-in dan menyimpan credential (nama, email, password) (Novell, 2011). Fakta yang terjadi pada perusahaan ini membuktikan bahwa ada kebutuhan besar terhadap solusi single sign-on supaya mekanisme autentikasi dan autorisasi menjadi efektif.

Setiap aplikasi dalam sebuah sistem yang terintegrasi membutuhkan mekanisme autentikasi supaya menjamin hanya user yang terautentikasi-lah yang mampu mengakses informasi pribadi dan servis dari aplikasi (Goth, 2008). Apabila setiap satu aplikasi menyimpan informasi *credential* berupa email dan password, redundansi akan terjadi. Dalam satu *enterprise*, rata-rata user akan menggunakan antara 5-10 aplikasi sekaligus (Novell, 2011). Sebagai contoh, user kemungkinan besar akan menggunakan banyak servis Google secara bersamaan, seperti Google Maps, Youtube, dan Google Mail. Tanpa *single sign-on*, user harus mengelola tiap password untuk tiap aplikasi.

Di sisi *enterprise*, Google harus menyimpan *credential* masing-masing user untuk tiap aplikasi. Ini tentunya tidak efisien. Bagaimana bisa aplikasi dalam satu vendor, memiliki mekanisme autentikasi yang berbeda. Bagaimana jika user cukup login sekali saja untuk satu vendor (Google), kemudian user bisa mengakses seluruh servis yang disediakan Google? (Goth, 2008).

*Single sign-on* adalah solusi dari permasalahan autentikasi multi-servis. Ide utama *single sign-on* adalah pemusatan autentikasi beberapa servis menjadi *single-entry point* untuk autentikasi (Volchkov, 2001). Dengan *single sign-on*, permasalahan autentikasi akan disentralisasi menjadi satu mekanisme autentikasi. Mekanisme *single sign-on* ini akan mengatur dan memberikan autorisasi kepada *credential* supaya bisa mengakses bagian tertentu pada servis.

Single sign-on adalah mekanisme di mana user cukup mengautentikasi dirinya satu kali saja kemudian user diberi akses ke banyak web servis, tanpa memasukkan banyak *password* (Volchkov, 2001). User diberi akses oleh *server single sign-on* berupa *token* atau *cookies* yang dapat digunakan untuk mengakses beberapa aplikasi *service provider*.

Secara umum, implementasi *single sign-on* melibatkan *server single sign-on* sebagai penyedia identitas yang mengatur autentikasi dan autorisasi dan aplikasi *service provider* sebagai penyedia servis yang bertugas mengkonsumsi autentikasi dari *server single sign-on*. Apabila bicara ke level detil implementasi, ada banyak mekanisme berbeda yang dilakukan oleh SSO yang sudah ada seperti yang dilakukan oleh SAML, Auth0, OAuth, OpenID, dan LastPass.

Dalam praktek di lapangan, tidak seluruh *web single sign-on* dengan mudah diintegrasi dengan aplikasi *service provider*. Beberapa masalah muncul dalam proses pengembangan *single sign-on* dengan aplikasi *service provider*. Masalah yang muncul adalah dokumentasi tidak lengkap, contoh aplikasi yang disediakan tidak berjalan semestinya, server *single sign-on* yang membutuhkan memori besar untuk dijalankan. Sebagai contoh, *single sign-on* milik Apereo, *Central Authentication Service* membutuhkan server dengan RAM minimal 8 GB untuk dijalankan (Apereo, 2015). Sementara, WSO2 tidak dengan mudah diintegrasi karena dukungan dokumentasi yang kurang lengkap dan contoh aplikasi *service provider* pengguna *single sign-on* yang tidak berjalan semestinya. Sementara itu, Auth0 sebagai produk single sign-on lain memiliki banyak keunggulan seperti kemudahan pengembangan, dukungan dokumentasi lengkap, dan dukungan SDK lengkap terhadap banyak bahasa dan *framework*. Namun penggunaan Auth0 untuk lingkup gratis harus menggunakan media penyimpanan basis data *cloud* yang disediakan Auth0 (Pace, 2015). Ini tentunya kurang nyaman bagi developer ketika aplikasi menyimpan data sensitif user. Auth0 menyediakan server *self-hosted* yang memungkinkan developer menyimpan data *user* pada media penyimpanan yang dapat dimodifikasi sendiri, tetapi layanan ini berbayar.

Berdasarkan kelemahan dan kelebihan masing-masing *single sign-on* yang sudah dianalisis kemudian, maka dalam tugas akhir ini diusulkan *web single sign-on* yang baru. *Web single sign-on* yang dibangun merupakan akumulasi poin positif dari *web single sign-on* yang sudah ada, dengan penyempurnaan pada kelemahan dari masing-masing *single sign-on* yang dianalisis.

## Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, didapat perumusan masalah yang akan diselesaikan dalam tugas akhir, yakni sebagai berikut:

1. Bagaimana cara membangun *web single sign-on* sebagai penyempurnaan terhadap *single sign-on* yang pernah ada sebelumnya.
2. Bagaimana karakteristik *web* *single sign-on* yang akan dibangun.
3. Bagaimana mengevaluasi *web single sign-on* yang dibangun dibandingkan *web single sign-on* lain.

## Tujuan

Tujuan dari tugas akhir ini adalah sebagai berikut.

1. Menentukan teknik yang tepat untuk membangun web single sign-on sebagai penyempurnaan terhadap single sign-on yang sudah ada.
2. Menentukan karakteristik *web* *single sign-on* yang akan dibangun.
3. Mencari parameter evaluasi *web single sign-on* supaya bisa dibandingkan dengan *web single sign-on* lain.

## Batasan Masalah

Batasan-batasan dalam pelaksanaan tugas akhir ini perlu didefinisikan agar hasil dari tugas akhir bersifat spesifik dan jelas. Batasan-batasan yang diambil dalam pelaksanaan tugas akhir ini adalah sebagai berikut.

1. Fokus pengerjaan dalam tugas akhir ini adalah *web single sign-on*. Aplikasi *service provider* bukan merupakan fokus dalam tugas akhir.
2. Pengiriman data antar komponen dilakukan melalui protokol HTTP, protokol lain seperti OAuth, SAML, OpenID tidak didukung.

## Metodologi

Metodologi yang digunakan dalam pengerjaan tugas akhir ini meliputi:

1. Analisis masalah. Pada tahap ini, dilakukan analisis terhadap permasalahan berkaitan dengan topik yang diangkat pada tugas akhir ini. Analisis masalah ini meliputi kajian terhadap bermacam model dan desain *single sign-on* yang pernah didesain orang sebelumnya.
2. Pembangunan aplikasi *single sign-on*. Setelah masalah dianalisis dan dilakukan *requirement engineering*, dibangunlah aplikasi *single sign-on* yang sesuai dengan kebutuhan yang diberikan. Aplikasi ini harus mampu memenuhi kebutuhan fungsional yang telah didefinisikan pada tahap analisis masalah sebelumnya. Aplikasi *single sign-on* ini bertindak sebagai sentra pusat autentikasi bagi *service* lain..
3. Pembangunan aplikasi *service provider*. Walaupun pembangunan aplikasi *service provider* bukan merupakan fokus utama dalam pengerjaan tugas akhir ini karena topik sebenarnya adalah *single sign-on*, aplikasi yang bertindak sebagai *service provider* harus tetap dibangun walau dengan fungsionalitas yang bersinggungan langsung dengan *single sign-on* saja. Ini tetap harus dilakukan untuk tujuan pengujian fungsionalitas *single sign-on* nantinya.
4. Evaluasi dan penarikan kesimpulan. Pada tahap ini dilakukan evaluasi terhadap *single sign-on* yang telah dibangun. Setelah itu, dilakukan juga penarikan kesimpulan yang didasari oleh hasil evaluasi pengujian aplikasi single sign-on.

## Sistematika Pembahasan

Penulisan tugas akhir ini dibagi menjadi 5 bab, yaitu bab I Pendahuluan, bab II Studi Literatur, bab III Analisis Permasalahan dan Rancangan Solusi, bab IV Implementasi dan Pengujian, dan bab V Kesimpulan dan Saran. Bab I Pendahuluan memberikan gambaran mengenai tugas akhir ini. Bab I terdiri dari latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi, dan sistematika pembahasan.

Bab II Studi Literatur memaparkan hasil studi literatur terkait autentikasi dan autorisasi, *single sign-on*, beserta kakas dalam pengembangan *single sign-on*.

Bab III Analisis Permasalahan dan Desain Solusi berisi hasil analisis dari permasalahan yang ada pada tugas akhir ini serta usulan solusi yang diajukan untuk memecahkan permasalahan tersebut.

Bab IV Implementasi dan Pengujian membahas implementasi serta hasil pengujian. Pengujian yang dilakukan terkait perbandingan antara kakas yang digunakan satu sama lain atas berbagai parameter.

Bab V Kesimpulan dan Saran menjelaskan mengenai kesimpulan dari tugas akhir ini dan saran untuk mengembangkan lebih lanjut mengenai tugas akhir ini agar menghasilkan hasil yang lebih baik.

# STUDI LITERATUR

## Autentikasi dan Autorisasi

Autentikasi adalah proses bagaimana sistem dapat mengetahui dengan siapa sistem tersebut berkomunikasi (Tanenbaum, 2007). Menurut Neuman (1994), autentikasi adalah verifikasi dari identitas seseorang yang memberikan data beserta data yang diberikan.

Autorisasi adalah teknik yang menentukan proses apa saja yang boleh dilakukan (Tanenbaum, 2007). Definisi lain dari Neuman (1994), autorisasi adalah proses yang menentukan apakah sebuah pihak diperbolehkan untuk melakukan operasi tertentu.

Menurut Halonen (2000), autentikasi dan autorisasi seharusnya memiliki karakteristik sebagai berikut:

1. Kebenaran (*Correctness*)

Hasil dari setiap autentikasi dan autorisasi harus akurat.

1. Kemungkinan untuk anonim dan privasi (*Possibility to anonymity and privacy*)

Autentikasi terhadap identitas hanya dilakukan apabila benar-benar diperlukan. Apabila tidak perlu membuka identitas, maka identitas tersebut tidak perlu dibuka. Jika memungkinkan, autorisasi sebaiknya tidak dilakukan tanpa membuka identitas.

1. Kecepatan (*Speed*)

Proses autentikasi seharusnya dilakukan dengan cepat.

1. Ketahanan terhadap serangan (*Attack resistance*)

Metode autentikasi seharusnya dapat bertahan terhadap berbagai jenis serangan, misalnya serangan *Man-in-the-Middle* (MITM).

1. Murah (*Inexpensiveness*)

Proses autentikasi dan autentikasi seharusnya tidak memerlukan ongkos yang mahal, baik ongkos pengembangan dan pemeliharaan.

1. Kemudahan penggunaan (*User friendliness*)

Metode autentikasi sedapat mungkin mudah digunakan dan dimengerti oleh penggunanya. Pada kondisi ideal, pengguna tidak perlu mengeluarkan banyak usaha ketika melakukan proses autentikasi.

1. Universal (*Universality*)

Metode autentikasi sebaiknya bersifat sama pada semua layanan.

## Sistem Autentikasi Identitas

Autentikasi adalah hal paling mendasar dari keamanan *service* karena autentikasi yang terpercaya dibutuhkan untuk memberi kontrol akses, menentukan siapa yang berhak menerima atau mengubah informasi, dan melawan penyanggahan (*non-repudiation*) (Ford, 1997).

Menurut Ford (1998), ada lima metode yang dapat digunakan dalam proses autentikasi, yaitu sebagai berikut.

1. Sesuatu yang diketahui pengaku (*something the claimant knows*),
2. Sesuatu yang dimiliki pengaku (*something the claimant owns*),
3. Sesuatu tentang siapa pengaku (*something the claimant is*),
4. Pengaku pada tempat atau waktu tertentu (*claimant is at a particular place at particular time*),
5. Autentikasi yang diberikan oleh pihak ketiga yang terpercaya (*authentication is established by a trusted third party*).

### *Password*

*Password* merupakan metode yang paling mudah dan umum digunakan dalam proses autentikasi (Ford, 1998). *Password* pada umumnya diasosiasikan dengan *username*, sehingga metode ini dapat digunakan oleh sistem yang memiliki banyak pengguna. Tetapi, *password* merupakan metode yang paling tidak aman untuk autentikasi dan hal ini merupakan salah satu kerentanan utama dari metode *password*. Namun, kelemahan ini dapat diatasi dengan menggunakan *tool password generator* sehingga kita tidak perlu mengingat *password* yang panjang dan cukup menggunakan *tool password generator* yang diamankan dengan satu *master password* saja.

Kriteria keamanan pada metode *password* terletak hanya pada panjangnya *string password*. Beberapa teknik penyerangan yang dapat dilakukan pada metode *password* adalah *external disclosure*, *guessing*, *communications eavesdropping*, *replay attacks*, dan *host compromise* (Ford, 1998). Oleh karena itu, dewasa ini metode autentikasi *password* sering kali digunakan bersama dengan metode autentikasi lainnya sehingga memiliki tingkat keamanan yang lebih tinggi, atau yang sering disebut *Multi-Factor Authentication* (MFA).

### *Token*

*Token* adalah metode yang digunakan untuk meningkatkan keamanan dari sistem autentikasi (Ford, 1998). Salah satu penerapan metode autentikasi *token* adalah *physical tokens* yang sering digunakan oleh bank. Tujuannya adalah untuk memberikan pengamanan tambahan pada transaksi yang dilakukan. Jika seandainya PIN nasabah bank diketahui oleh pencuri atau pihak yang tidak berhak, maka pencuri tidak dapat melakukan transaksi jika tidak memiliki *token*. Metode pembangkitan *token* juga memerlukan suatu alat fisik dan memperhitungkan variabel waktu sehingga *token* menjadi sulit ditebak oleh penyerang.

Dewasa ini *virtual token* juga sering digunakan sebagai metode autentikasi. Cara pembuatan *virtual token* berbeda dengan cara pembuatan *physical token* yang memerlukan alat atau benda fisik untuk menghasilkan *token*. *Virtual token* merupakan *token* yang dapat dihasilkan secara *virtual* dengan bantuan perangkat lunak atau *software*. Sedangkan untuk representasi datanya, *physical token* dan *virtual token* mungkin saja memiliki representasi data yang sama, misalnya *string* atau angka. Contoh implementasi dari *virtual token* adalah *One-time Password*, atau yang sering disingkat OTP. OTP adalah *virtual token* yang memungkinkan *user* menerima *password* yang dibangkitkan secara acak oleh *provider* OTP dan berlaku hanya dalam jangka waktu tertentu (biasanya 30 detik). Contoh OTP yang secara luas digunakan oleh masyarakat adalah *Google Authenticator* dan *Authy*. Kedua aplikasi tersebut merupakan aplikasi yang berjalan pada *device* *Android* dapat diunduh di *Playstore* secara gratis.

Contoh penggunaan *virtual tokens* pada aplikasi berbasis web adalah *session* dan *cookie*. *Session* disimpan pada *server* dan digunakan untuk menyimpan *state* dari pengguna (Whitehead, 2006). *Session* dapat diumpamakan sebagai kumpulan dari *key* yang memiliki *value* tertentu. Masing-masing *session* memiliki *session* *ID* yang dihasilkan secara otomatis dan berbeda untuk setiap *session*. *Session ID* inilah yang dapat dianggap sebagai *token*.

*Cookie* merupakan kumpulan dari pasangan parameter dan nilainya. *Cookie* dibuat atau dihasilkan oleh *server*, dan diberikan kepada *web browser*. *Cookie* umumkan disimpan pada media penyimpanan lokal milik *device client* dan dapat diakses oleh *web browser*. *Cookie* dapat digunakan untuk memberikan tanda bahwa pengguna sudah melakkan atau mendapatkan sesuatu dari *server*. Dengan kata lain, *cookie* merupakan suatu mekanisme untuk menambahkan *state* pada *HTTP request* (Whitehead, 2006).

Pada umumnya, *session* dan *cookie* dapat dikombinasikan sebagai teknik manajemen *state* pada aplikasi web (Whitehead, 2006). State diperlukan pada aplikasi web untuk mengetahui apakah pengguna pernah mengunjungi web pada waktu sebelumnya atau apakah pengguna sudah melakukan tahapan yang benar untuk sebuah proses pada aplikasi berbasis web. *Server* menyimpan informasi *state* dari pengguna dengan menggunakan *session*. *Cookie* berisi informasi, misalnya *session ID*, yang digunakan untuk mencari *session* milik pengguna pada *server*. *Cookie* dihasilkan oleh *server* dan diberikan kepada *web browser* pada *HTTP response*, kemudian *cookie* dikirimkan kembali oleh *web browser* pada *server* pada *HTTP request* selanjutnya.

### *Biometrics*

Metode *biometrics* menekankan bahwa autentikasi akan mengidentifikasi dan memverifikasi seseorang berdasarkan dari ciri-ciri fisik atau perilaku yang dimilikinya. Metode autentikasi dengan *biometrics* memiliki kekurangan utama yaitu harga atau biaya untuk mengimplementasikannya sangat mahal dibandingkan dengan metode autentikasi lainnya (Ford, 1998). Contoh ciri-ciri fisik yang dapat digunakan pada metode *biometrics* adalah sidik jari (*fingerprint*), retina mata, tulisan tangan, bentuk wajah, dan bentuk gigi. Sedangkan, contoh ciri perilaku yang dapat digunakan adalah kebiasaan gerak seseorang dan suara dalam melafalkan kata-kata kalimat.

Salah satu metode *biometrics* yakni sidik jari memiliki akurasi yang sangat tinggi. Sidik jari manusia merupakan komponen yang identitas manusia yang unik. Dua *fingerprint* yang sama hanya ditemukan sekali dalam setiap 1048 tahun (Jain, 2005).

### Tanda Tangan Digital

Tanda tangan digital atau *digital signatures* adalah tanda tangan yang diberikan pada data digital (Munir, 2005). Tanda tangan berupa nilai yang berdasarkan dari isi dan pengirim pesan. Proses umum pemberian tanda tangan melibatkan kriptografi asimetri dan fungsi *hash*. Tanda tangan digital dapat digunakan oleh penerima pesan untuk memverifikasi bahwa pengirim pesan memiliki kunci privat yang sah dan isi pesan tidak diubah selama proses pengiriman (Ford, 1998). Penerima pesan dapat dianalogikan sebagai aplikasi dan pengirim pesan adalah pengguna, atau sebaliknya. Sebagai metode autentikasi, pengguna juga dapat mengirimkan tanda tangan digitalnya untuk diverifikasi.

### Sertifikat Digital

Sertifikat digital merupakan sertifikat yang dikeluarkan oleh *Certification Authorities* (CA) yang menyatakan hubungan antara kunci publik dan pemiliknya (Ford, 1998). Isi informasi dari sertifikat digital berupa nama organisasi pemilik kunci publik, kunci publik, dan waktu kadaluarsa sertifikat. Sertifikat digital dapat digunakan untuk mengautentikasi seorang pengguna atau sebuah *website* ataupun sebuah institusi. *Certification Authorities* memberikan cara untuk mengirimkan kunci publik beserta informasi pemiliknya pada dunia digital melalui sertifikat digital (Ford, 1998). Namun, pengenalan CA yang sah dan dipercaya untuk mengeluarkan sertifikat digital harus dapat dilakukan oleh pihak penerima pesan. Pengenalan CA yang sah menjadi masalah baru yang ditimbulkan dari penggunaan metode *Certification Authorities* untuk metode autentikasi.

## *Multi-Factor Authentication*

*Multi-Factor Authentication* (MFA) atau autentikasi banyak faktor adalah autentikasi yang menggunakan lebih dari satu faktor atau metode (*Federal Deposit Insurance Corporation*, 2004). Faktor untuk melakukan autentikasi adalah lima metode autentikasi yang sudah dijelaskan pada subbab 2.2. MFA dengan dua metode autentikasi seringkali disebut *two-factor authentication* (2FA).

Semakin banyak metode autentikasi yang digunakan, semakin baik keamanan sebuah sistem (*Federal Deposit Insurance Corporation*, 2004). Tetapi, untuk setiap kelebihan kadangkala terdapat kelemahan yang harus diterima sebagai konsekuensinya. Kelemahannya adalah lamanya waktu yang dibutuhkan untuk autentikasi yang berbanding lurus dengan banyaknya metode autentikasi yang digunakan.

## *Single Sign-On*

*Single sign-on* adalah proses autentikasi *user* yang memperbolehkan seorang pengguna dengan sebuah identitas yang terdaftar untuk mengakses berbagai aplikasi (Pashadilis, 2003). *Single sign-on* disingkat SSO. Menurut He (2007), *single sign-on* dalam definisi yang lebih sederhana adalah proses penggunaan identitas pengguna yang sama secara bersama-sama. *Single sign-on* adalah bagian dari sistem yang memungkinkan *user* mengakses beberapa layanan/aplikasi/*resource* melalui satu titik entri. *Single sign-on* merupakan properti akses kontrol dari beberapa sistem yang berhubungan tetapi independen (Volchkov, 2001). Dengan properti ini, *user* dapat melakukan *log in* menggunakan satu *ID* dan *password* untuk mendapatkan akses ke sistem yang terhubung atau sistem dengan banyak *username* dan *password* yang berbeda. *Single-sign on* biasanya menyimpan satu *set credential*, seperti nama, *e-mail*, dan *password* untuk mengakses beberapa aplikasi. *Single sign-on* mengautentikasi *user*, apakah *user* yang bersangkutan diberikan hak untuk mengakses *resource* yang ada. Pada *back-end*, *single sign-on* sangat membantu untuk mengelola aktivitas *user* sekaligus memonitor akun. Contoh sederhana dari *single sign-on* dapat dicapai lewat penyimpanan *cookie* di *browser* untuk domain tertentu, namun hanya dapat dicapai apabila situs memiliki domain DNS yang sama. Secara umum, *single sign-on* terdiri dari *Identity Provider* (IdP) yang berfungsi untuk mengelola *credential*/*session* milik *user*. Sementara itu *single-sign on* juga memiliki *Service Provider* (SP) yang merupakan konsumer dari autentikasi yang disediakan IdP.

Misalkan dalam sebuah sistem terdiri dari beberapa aplikasi dan sistem tersebut memiliki mekanisme autentikasi dalam *single sign-on*. Penguna harus melakukan *log in* pada setiap aplikasi dan aplikasi akan mengautentikasi pengguna tersebut. Pengguna juga harus mendaftarkan dirinya dan mengingat sejumlah identitas untuk diautentikasi pada sejumlah aplikasi. Hal ini juga dapat menyebabkan *human error* jika pengguna lupa terhadap identitasnya atau mekanisme autentikasi *error* pada sebuah aplikasi.

Pengelolaan pengguna menjadi pekerjaan yang merepotkan jika pengguna dan/atau aplikasi semakin bertambah banyak. Hal ini dapat diperburuk dengan pengelolaan pengguna yang harus dilakukan pada masing-masing aplikasi jika aplikasi-aplikasi tidak menggunakan *single sign-on*.

Pada sistem yang mekanisme autentikasinya tanpa *single sign-on*, aplikasi juga mengalami kerugian yaitu terdapat *overhead* proses autentikasi. *Overhead* pada autentikasi maksudnya adalah proses autentikasi dilakukan berkali-kali pada setiap aplikasi meskipun proses autentikasi tersebut cukup dilakukan sekali oleh sebuah aplikasi saja. Dengan menggunakan *single sign-on*, proses autentikasi cukup dilakukan sekali pada aplikasi yang menangani *single sign-on.*



Gambar ‎II.1 Sistem yang Mekanisme Autentikasinya tanpa SSO

.

Beberapa poin kerugian, yaitu kemungkinan terjadinya *human error*, kerumitan pada pengelolaan pengguna dan *overhead* pada proses autentikasi, dapat terjadi pada sistem yang tidak menggunakan *single sign-on*. Gambar II.x merupakan contoh sistem yang mekanisme autentikasinya tanpa *single sign-on*. Sistem pada gambar tersebut terdiri dari aplikasi A, B, dan C. Pengguna akan melakukan *log in* terlebih dahulu untuk menggunakan aplikasi yang diinginkannya. Setiap aplikasi memiliki mekanisme autentikasinya sendiri sehingga pengguna harus melakukan *log in* pada setiap aplikasi untuk menggunakannya.

Mekanisme autentikasi pada Gambar II.x kurang efektif dan efisien jika dibandingkan dengan mekanisme autentikasi pada Gambar II.x+1. Mekanisme autentikasi pada Gambar II.x+1 menggunakan *single sign-on* untuk mekanisme autentikasi seluruh aplikasi. Sehingga, pengguna cukup terautentikasi sekali saja untuk menggunakan aplikasi A atau B atau C. Autentikasi dapat dilakukan oleh salah satu aplikasi ataupun mengunakan aplikasi pihak ketiga yang dipercaya oleh masing-masing aplikasi A, B, dan C.



Gambar ‎II.2 Sistem dengan SSO

Berikut adalah kelebihan implementasi *single sign-on*:

1. Satu *password* untuk masuk ke dalam sistem.
2. *Login* otomatis, apabila *user* sudah memiliki *session* sebelumnya.
3. Lebih mudah untuk mengelola *user*.
4. Satu klik untuk mengambil (*revoke*) akses *user* untuk sebagian atau seluruh bagian sistem.

Berikut adalah kekurangan implementasi *single sign-on*:

1. *Single point of failure*. Apabila server *single sign-on* *down*, maka seluruh aplikasi tidak memiliki mekanisme untuk autentikasi *user*. Dapat di-*handle* dengan mereplika *server* *single sign-on* menjadi beberapa replika supaya *availability* semakin besar.
2. *Single point of attack*. Penyerang dapat bertindak sebagai aplikasi yang sah untuk mencuri informasi yang dikirimkan SSO *server* kepada pengguna (Pashadilis, 2003). Sehingga, penyerang dapat mengetahui informasi berharga yang digunakan untuk komunikasi antara SSO *server* dan pengguna.
3. Apabila aplikasi sudah ada dan *single sign-on* akan diintegrasi, *cost* untuk mengintegrasikan *single sign-on* dengan aplikasi yang sudah ada cukup besar. Hal ini biasanya rumit, terutama untuk pengimplementasian SSO pada sebuah sistem lama. Pada kondisi ini, implementasi SSO lebih diarahkan kepada penambahan fitur untuk meningkatkan *user experience* dan efektivitas dan efisiensi dari aplikasi. Akibatnya, implementasi SSO harus memperhatikan fungsionalitas yang sudah ada dan biasa digunakan pada sistem lama.

## *Web Single Sign*-*On*

*Web single sign-on* adalah *single sign-on* yang digunakan pada aplikasi berbasis web (Jasig, 2009). *Web single sign-on* biasanya disingkat *web* SSO. Banyaknya jumlah layanan yang tersedia di Internet menyebabkan ketidaknyamanan terhadap pengguna layanan. Pengguna biasanya harus melakukan *log in* pada beberapa sistem layanan dan masing-masing sistem layanan memerlukan identitas untuk diautentikasi. Jika setiap sistem layanan yang memerlukan identitas yang spesifik dan berbeda, maka pengguna akan mendapatkan kesulitan yang lebih banyak. Salah satu kesultan dalah pengguna harus mengingat identitas yang digunakan pada setiap layanan.

*Web single sign-on* sangat mudah ditemukan dari *web* pada Internet. Dewasa ini, beberapa grup atau komunitas sudah mengembangkan *web single sign-on*. Beberapa produk *web single sign-on* bersifat *open-source*, tetapi ada juga produk yang bersifat komersil. Beberapa grup atau kounitas yang mengembangkan *web single sign-on* adalah:

1. *Auth0 Inc* dengan produknya *Auth0*.
2. WSO2 dengan produknya WSO2 *Identity Server*.
3. *Apereo* dengan produknya *Central Authentication Service*.
4. *Atricore Inc* dengan produknya *Java Open Single Sign-On*.

### *Auth0*

Auth0 adalah layanan *Platform as a Service* (PaaS) yang menyediakan *single sign-on* yang memudahkan *developer* untuk memungkinkan *developer* menambahkan SSO pada aplikasinya secara mudah tanpa memperdulikan bahasa, teknologi, dan protokol yang digunakan dalam autentikasi. Sebagai PaaS, Auth0 menyediakan *platform single sign-on* secara keseluruhan termasuk *dashboard*, media penyimpanan data *user*, dan halaman *login* untuk *single sign-on*. Auth0 dikembangkan oleh *Auth0 Inc* sebuah perusahan yang berpusat di Seattle, Amerika Serikat. Alamat *website* Auth0 adalah <https://auth0.com>. Sementara alamat *website* untuk manajemen *dashboard* Auth0 adalah <https://manage.auth0.com>.

Auth0 dapat digunakan tanpa memerdulikan bahasa apa yang digunakan aplikasi *service provider*. Sejauh ini, banyak *stack* teknologi yang didukung Auth0 baik *regular web application* (*server-side authentication*) seperti Go, Java, Ruby on Rails, dan seterusnya, *single-page application* (*client-side authentication*) seperti NodeJS, AngularJS, dan JQuery, maupun *mobile application* (iOS dan Android) (Pace, 2015). Masing-masing jenis *client server-side*, *client-side*, dan *mobile* memiliki alur autentikasi yang berbeda-beda. Auth0 mendukung lebih dari 65 SDK (*Software Development Kit*) yang dapat digunakan *developer* untuk mengintegrasikan aplikasinya dengan *single sign-on* Auth0. Auth0 juga mendukung protokol SAML, OpenID, dan integrasi dengan banyak penyedia *single sign-on* (*provider*) seperti Slack, Dropbox, Yahoo. Selain itu, dokumentasi Auth0 sangat mudah dimengerti dan diaplikasikan karena banyak tersedia *sample application* yang benar-benar dapat dijalankan. Dengan demikian, Auth0 berkembang dengan sangat pesat, saat ini memiliki 2000+ *enterprise* *customer*, 42 juta lebih *login* dalam satu hari. Cara kerja Auth0 dapat dilihat pada Gambar II.x di bawah.



Gambar ‎II.3 Cara Kerja Auth0

Cara kerja Auth0 adalah sebagai berikut.

* 1. *Admin*, atau *developer* mendaftarkan aplikasi *service provider* ke *dashboard* Auth0.
  2. *Dashboard* Auth0 akan menyimpan informasi kepada *server* mengenai *developer* dan aplikasi miliknya.
  3. *Developer* mengarahkan (*redirect*) aplikasi *service provider* ke *server* Auth0.
  4. *User* ingin mengakses *resource* di aplikasi *service provider* yang dilindungi oleh autentikasi.
  5. Aplikasi *service provider* mengetahui *user* belum terautentikasi, maka *service provider* mengarahkan *user* ke halaman *login* di *server* Auth0. *Server* Auth0 ini dapat berupa *cloud* Auth0 yang dapat ter-*deploy* sehingga dapat diakses siapapun, ataupun *server* yang berada pada jaringan privat. Untuk layanan gratis, Auth0 hanya menyediakan *server cloud* saja sehingga kita tidak bisa menggunakan *server* Auth0 pada jaringan privat kita sendiri. Ini artinya seluruh data *user* dan aplikasi *service provider* disimpan pada media penyimpanan milik Auth0.
  6. User melakukan autentikasi pada halaman *login server* Auth0 dengan memasukkan *credential*.
  7. Setelah autentikasi pada *server* Auth0 berhasil dilakukan, *server* mengembalikan *user* ke *service provider* beserta *token* yang dapat digunakan untuk identifikasi *user* ketika mengakses *resource* berikutnya.
  8. Ketika *user* membutuhkan *resource* yang membutuhkan autentikasi, aplikasi tidak perlu lagi melakukan *redirect* laman ke *server* Auth0 karena *token* sudah tersimpan pada aplikasi *service provider* untuk digunakan selanjutnya.

### WSO2 *Identity Server*

WSO2 *Identity Server* adalah *web single sign-on open-source* yang dibuat oleh WSO2. WSO *Identity Server* dibangun di atas WSO2 *Carbon*, sebuah framework manajemen identitas yang dibuat oleh WSO2. WSO2 mendukung banyak protokol SSO seperti OpenID Connect, OAuth, SAML SSO, maupun *social authenticator* yang popular seperti *Google*, *Facebook*, *Yahoo*, *Microsoft*, juga mendukung berbagai metode autentikasi lain seperti SMS OTP, Email OTP, Kerberos, dan lain-lain.

Berikut adalah arsitektur WSO2.



Gambar ‎II.4 Arsitektur WSO2 *Identity Server* (WSO2, 2015)

Aplikasi *service provider* yang menggunakan WSO2 *Identity Server* melakukan autentikasi pada sisi aplikasi *service provider*. *Credential* yang dimasukkan oleh *resource owner* (user) akan dikirimkan ke WSO2 *Identity Server* melalui *Inbound Authenticator*. *Inbound Authenticator* berfungsi untuk mengurusi permintaan *user* yang akan melakukan *log in*. Permintaan ini diterima oleh modul *Request Processor* kemudian akan diteruskan ke *Authentication Framework* yang berada pada gambar di tengah atas. Permintaan *user* atas *service provider* dipetakan ke struktur data lokal milik WSO2 (*claim mapping*) yang terstandardisasi menurut WSO2. Kemudian permintaan *login* akan dilanjutkan menurut tipenya. Apabila permintaan *login* tersebut adalah *login* dengan *username*/*password*, maka permintaan akan diteruskan ke *Local Authenticators*, sementara apabila permintaan *login* menggunakan model autentikasi lain seperti SAML, OpenID Connect, dst maka permintaan akan diteruskan *Federated Authenticators*. *Federated Authenticators* bertindak sebagai komunikator antara WSO2 *Identity Server* dengan aplikasi eksternal seperti *Google*, *Facebook*, *Yahoo*, atau penyedia layanan *identity server* lain.

Setelah *Local Authenticators* atau *Federated Authenticators* selesai melakukan validasi terhadap *user*, respon akan dikembalikan ke *Authentication Framework*. *Authentication Framework* akan melakukan pemetaan ulang dari *identity server* ke struktur data internal WSO2 (*claim mapping*), dan dari *claim mapping* ke *service provider*. Respons akan dikembalikan ke *Inbound Authenticator*. Modul *Response Generator* pada *Inbound Authenticator* akan mengembalikan respon *login* kepada *user*. Respon ini bisa berupa penolakan *login* atau penerimaan *login*.



Gambar ‎II.5 Mekanisme WSO2 *Identity Server*

Cara kerja WSO2 *Identity Server* adalah sebagai berikut:

* 1. *Admin*, atau *developer* mendaftarkan aplikasi *service provider* ke *dashboard* WSO2 *Identity Server*.
  2. *Dashboard* WSO2 akan menyimpan informasi kepada *server* mengenai *developer* dan aplikasi miliknya.
  3. *Developer* mengarahkan aplikasi *service provider* ke *single sign-on* ketika membutuhkan autentikasi *user*.
  4. *User* ingin mengakses *resource* di aplikasi *service provider* yang dilindungi oleh autentikasi.
  5. Aplikasi *service provider* mengirimkan *credential user* dan *credential* aplikasi untuk menukarkannya dengan *token* *user* yang bisa digunakan untuk *login* pada *session* berikutnya. *Credential user* diperlukan untuk membedakan suatu *user* dan *user* lain. *Credential* aplikasi diperlukan *server* WSO2 untuk memastikan aplikasi yang meminta *login user* tersebut adalah benar-benar aplikasi yang valid.
  6. Setelah autentikasi di *server* Auth0 berhasil dilakukan, *server* memberikan *token* kepada *service provider* yang dapat digunakan untuk identifikasi *user* ketika mengakses *resource* berikutnya.
  7. Ketika *user* membutuhkan *resource* yang membutuhkan autentikasi, aplikasi tidak perlu lagi *login* ke aplikasi, cukup ke laman ke *server* Auth0 karena *token* sudah tersimpan pada aplikasi *service provider* untuk digunakan selanjutnya.

Secara garis besar, cara kerja WSO2 *Identity Server* kurang lebih mirip dengan Auth0 yang telah dijelaskan pada subbab sebelumnya. WSO2 *Identity Server* menyediakan *dashboard* *developer/admin* sama seperti yang Auth0 miliki. Yang menjadi perbedaan adalah *server* WSO2 IS disediakan secara gratis karena *open-source* dan kita bisa melakukan *self-host* dengan mudah.

Perbedaan lain adalah aplikasi *service provider* tidak di-*redirect* ke *server* milik SSO untuk *login*. *Login* dilakukan pada sisi aplikasi tetapi validasi dilakukan pada sisi *server* WSO2.

### *Central Authentication Service (CAS)*

*Central Authentication Service* (CAS) merupakan *web single sign-on* yang dibuat oleh Apereo. Pada mulanya, CAS hanyalah sebuah protokol *single sign-on* yang dibuat oleh *Yale University*. Kemudian, *Central Authentication Service* diimplementasikan dengan *platform* Java dan mendukung *library* dari *client* untuk Java, PHP, Perl, dan lainnya sehingga CAS menjadi sebuah penyedia *web single sign-on*.

Cara kerja protokol autentikasi CAS hampir mirip dengan cara kerja protokol Kerberos. Kemiripan protokol autentikasi dikarenakan CAS menggunakan Kerberos sebagai model dalam pembuatan mekanisme autentikasi. Cara kerja protokol CAS dapat dilihat pada Gambar II.x.



Gambar ‎II.6 Mekanisme Kerja CAS

Cara kerja protokol CAS adalah sebagai berikut (Jasig, 2009)

1. Pengguna mengakses sebuah aplikasi *web* atau *service provider*.
2. Pengguna tersebut akan di-*redirect* ke CAS *login* URL melalui koneksi HTTPS. Nama aplikasi *web* atau *service provider* diberikan sebagai parameter dari *request*.
3. Pengguna memasukkan ID, yang dapat berupa *username*, dan *password*. Kemudian, CAS *server* melakukan autentikasi terhadap pengguna. Jika autentikasi gagal, aplikasi web tidak akan bisa diakses dan pengguna akan diminta untuk mengisikan ID dan *password* yang benar.
4. Jika autentikasi berhasil, CAS *server* mengarahkan pengguna ke aplikasi *web* yang diinginkan dan menambahkan *ticket* pada parameter URL. CAS *server* membuat sebuah *cookie* yang disebut *ticket granting cookie* (TGC). *Ticket granting cookie* akan digunakan untuk menandakan bahwa pengguna berhasil diautentikasi. Untuk selanjutnya, *ticket granting cookie* dapat digunakan untuk melakukan autentikasi secara otomatis.
5. Aplikasi *web* atau *service provider* akan melakukan validasi keabsahan dari *ticket* dan kepemilikan *ticket* oleh pengguna yang sah. CAS *Server Validate* yang disediakan oleh CAS *server* dapat digunakan untuk memvalidasi *ticket*.
6. Aplikasi *web* dan CAS *server* akan berkomunikasi melalui HTTPS dan *ticket* dan nama aplikasi akan dijadikan sebagai parameter. CAS *server* melakukan pengecekan bahwa *ticket* tersebut sah. Jika validasi berhasil, CAS *server* akan memberikan ID pengguna pada aplikasi.

*Central Authentication Service* terdiri dari dua komponen yaitu CAS *server* dan CAS *client*. CAS *server* menangani *web single sign-on* untuk aplikasi *web*. CAS *server* merupakan sebuah aplikasi *web* dengan *platform* Java.

CAS *client* akan membantu aplikasi *web* untuk menangani modul *web* *single sign-on* dari CAS *server*. CAS *client* akan dijadikan sebagai modul dari aplikasi *web* yang ingin mengunakan *web single sign-on*. CAS *client* harus disesuaikan dengan *platform* atau *framework* dari aplikasi *web*. CAS *client* juga dapat dikonfigurasi atau diimplementasi ulang jika memang diperlukan untuk memberikan dukungan *web single sign-on* pada aplikasi *web*.

Keunggulan dari CAS adalah CAS menyediakan banyak metode autentikasi yang dapat digunakan dengan aplikasi atau komponen lain. Contoh komponen yang digunakan CAS adalah *active directory*, LDAP, DBMS, X.509, SPNEGO, Legacy, dan lain-lain (Jasig, 2009). Metode autentikasi tersebut dapat dikonfigurasi pada CAS *server*.

### *Java Open Single Sign-On (JOSSO)*

JOSSO adalah sebuah infrastruktur *open-source single sign-on* berbasiskan Java EE and Spring yang menyediakan solusi untuk autentikasi dan autorisasi pengguna secara terpusat tanpa melihat *platform* (Atricore, 2010). Alamat URL *website* JOSSO adalah sebagai berikut: <http://josso.org>. JOSSO merupakan sebuah perangkat lunak yang dibuat oleh Atricore Inc.

JOSSO dapat digunakan pada *web server* dengan *platform* yang berbeda-beda, misalnya Jboss, Tomcat, Weblogic, Apache, PHP, dan Microsoft IIS. Meskipun begitu, SSO *gateway* hanya dapat di-*install* pada *web server* yang men-*support* Java, sedangkan SSO *agent* dapat di-*install* pada seluruh *web server*.

Komponen utama JOSSO berjumlah tiga, yaitu SSO *gateway*, SSO *agent*, dan aplikasi *service provider*. Sedangkan, entitas luar yang berinteraksi dengan JOSSO adalah penguna dengan *web browser*-nya, *identity storage resource*, dan *application stage storage resource*.

Penjelasan tiga komponen utama JOSSO adalah sebagai berikut.

1. SSO *gateway* / SSO *server* (*Identity Provider*/IdP)

SSO *gateway* merupakan SSO *server* atau dikenal sebagai *Identity Provider*. SSO *gateway* memiliki fungsi untuk mengelola SSO dari aplikasi *web* yang dapat menggunakan SSO. Pengguna yang dapat menggunakan SSO dapat dikelola melalui SSO *gateway*.

1. SSO *agent*

SSO *agent* bertugas melakukan penanganan *web single sign-on* terhadap aplikasi rekanan sesuai dengan lingkungan eksekusinya. Lingkungan eksekusi dalam prakteknya adalah *web server* dari aplikasi *service provider*. SSO *agent* menggunakan *identity services* yang disediakan oleh SSO *gateway*.

1. Aplikasi *service provider* (SP)

Aplikasi *service provider* atau *partner application* merupakan aplikasi yang menggunakan *web* SSO. Aplikasi *service provider* memiliki ketergantungan atau dependensi terhadap SSO *agent* dan SSO *gateway* untuk menyediakan *web single sign-on* kepada pengguna.

JOSSO mengandalkan komponen *identity provider*, *identity manager*, dan *session manager* untuk menangani *single sign-on* yang dilakukan oleh setiap aplikasi *service provider*. *Session manager* merupakan komponen yang mengelola *session* aplikasi, *identity manager* merupakan komponen yang mengelola *session* dari *user* yang sudah *login*, dan *identiy provider* merupakan komponen yang menyediakan daftar pengguna yang dapat menggunakan SSO.

Pada April 2011, versi JOSSO yang terbaru adalah 2.0.2, JOSSO2, mulai versi 2.0.0, merupakan generasi baru dari JOSSO. JOSSO generasi pertama (JOSSO1) dikembangkan hingga versi 1.8.4. Arsitektur JOSSO1 tidak berbeda dengan arsitektur JOSSO2. Namun, JOSSO2 men-*support* SAML2 untuk memberikan *interoperability* dengan sistem SSO pihak ketiga dan aplikasi *Software-as-a-Service* (SaaS). JOSSO2 juga memberikan pengelolaan SSO dengan menggunakan RIA (*Rich Internet Application*).

## Pekerjaan Terkait

### *CAS++*

CAS++ merupakan sistem *open-source single sign-on* yang dikembangkan oleh Ardagna dan krunya. CAS++ merupakan pengembangan dari *Central Authentication Services* (Ardagna, 2006). Pengembangan yang dilakukan pada CAS++ adalah:

1. Menggunakan identity certificates dan intertigrasi dengan security layer pada Jboss. Identity certificates disebut juga sebagai digital certificates atau public key certificates.
2. Mekanisme autentikasi menggunakan Public Key Infrastrukture (PKI).
3. Keamanan pada CAS++ ditingkatkan dengan menggunakan:
   * 1. SSL untuk memberikan jalur komunikasi yang aman terhadap aplikasi web yang berpartisipasi.
     2. X.509 digital certificates digunakan untuk pertukaran credentials.
4. Menyediakan user management secara terpusat sehingga masing-masing aplikasi web tidak perlu melakukan atau menyediakan user management. Identitas pengguna akan disimpan secara terpusat pada SSO server.
5. Memiliki layanan yang dapat digunakan untuk aplikasi web berbeda platform.
6. Proses autentikasi menggunakan username dan password dan diperkuat dengan metode biometrics dan smart card. Metode biometrics yang digunakan adalah sidik jari atau fingerprint yang dibaca dengan fingerprint readers.

Dengan pengembangan yang dilakukan pada CAS++, CAS++ memiliki kelebihan terhadap aspek keamanan (Ardagna, 2006). Keamanan pada CAS++ ditingkatkan dengan menggunakan SSL, X.509 dan metode autentikasi yang menggunakan metode biometrics dan smart card. CAS++ menjadi lebih mudah untuk diguankan oleh appliaski web berbeda platform karena menggunakan protokol standar seperti HTTP, SSL, X.509 untuk melakukan pertukaran informasi antara CAS++ server dengan aplikasi web.

### Kristanto, 2011

Kristanto mencoba mengimplementasi web single sign-on pada web pada lingkungan informatika ITB. Masalah timbul ketika aplikasi-aplikasi yang digunakan pada lingkungan informatika ITB seperti *milestone*, *moodle*, *oddyseus* memiliki mekanisme *login*-nya masing-masing.

Kristanto menganalisis karakteristik masing-masing aplikasi, terutama struktur data yang digunakan dalam autentikasi *user* beserta protokol yang digunakan dalam web SSO. Kristanto kemudian mengintegrasikan JOSSO pada aplikasi lingkungan informatika ITB. Media penyimpanan untuk data *user* menggunakan LDAP.

Berikut adalah komponen yang digunakan Kristanto dalam pengembangan SSO pada lingkungan web informatika ITB:

1. SSO *Server* yang merupakan bawaan JOSSO. SSO *server* ini tidak diimplementasi ulang, hanya perlu dikonfigurasi.
2. SSO *Agent* adalah komponen yang menghubungkan aplikasi *service* *provider* dengan SSO *server*. SSO *Agent* mendefinisikan bagaimana aplikasi *login*, *logout*, dan *endpoint* milik SSO *server*. Untuk membuktikan bahwa *single sign-on* tidak peduli pada bahasa client, SSO *Agent* diperlukan sebanyak dua buah, masing-masing menggunakan bahasa Java dan PHP.
3. Aplikasi *service provider*. Terdapat dua buah yakni Java dan PHP dan diletakkan pada *web server* yang berbeda. Aplikasi *service provider* ini melakukan autentikasi melalui SSO *Agent* yang sudah diimplementasi sebelumnya.

Kesimpulan yang didapat adalah *web single sign-on* pada lingkungan informatika ITB dapat dilakukan dengan mengubah sedikit basis data dan beberapa atribut kelas pada aplikasi.

# ANALISIS PERMASALAHAN DAN RANCANGAN SOLUSI

## Analisis Permasalahan

Pada bab ini, akan dipaparkan analisis berdasarkan studi literatur pada bab sebelumnya. Permasalahan yang dipaparan merupakan acuan dari topik Tugas Akhir ini. Setelah analisis permasalahan tersebut, akan dijelaskan rancangan solusi yang akan dibangun.

### Auth0

Dalam tahap studi literatur, di antara *tool web single sign-on* yang dipelajari, Auth0 menyediakan fungsional dan *Software Development Kit* (SDK) yang paling lengkap. Proses integrasi aplikasi dengan *single sign-on* milik Auth0 sangat mudah, hampir tidak ada halangan. Selain itu, Auth0 memiliki dokumentasi *Application Programming Interface* (API) yang jelas dan benar-benar berjalan. Dokumentasi API sangat penting dalam pengembangan perangkat lunak. Penyebabnya adalah karena dalam praktiknya, dokumentasi API merupakan kontrak yang sudah disediakan oleh penyedia API, yang mana *developer* harus mengikuti kontrak yang ada. Selain itu, Auth0 memiliki *dashboard admin* yang bisa digunakan untuk *monitoring user*, *monitoring* aplikasi *service provider*, *monitoring identity provider* eksternal yang terintegrasi dengan SSO Auth0. *Dashboard admin* ini memudahkan *developer* dalam *monitoring* banyak hal. Penggunaan Auth0 sebagai *single sign-on* gratis dibatasi hanya fitur sederhana, untuk penggunaan lebih, Auth0 memungut biaya.

Kelemahan Auth0 adalah Auth0 merupakan perangkat lunak *proprietary* milik Auth0 Inc. Produknya Auth0 tidak *open-source*, artinya tidak bisa dikembangkan lebih lanjut oleh orang umum. Pengembangan Auth0 hanya dapat dilakukan oleh pegawai Auth0 In. Selain itu, dalam penggunaan gratis, *developer* harus me-*redirect* aplikasi *service provider* ke halaman *login* yang di-*deploy* pada *cloud server* milik Auth0. Hal ini berarti seluruh data *user*, data aplikasi *service provider* tersimpan di basis data milik Auth0. Praktik ini tidak aman, terutama apabila data *user* yang disimpan merupakan data sensitif. Ini menyebabkan aplikasi *service provider* milik *developer* akan bergantung secara penuh terhadap ketersediaan *cloud server* milik Auth0. Apabila *cloud server* milik Auth0 *down*, maka aplikasi *service provider* tidak akan dapat melakukan segala hal yang berkaitan dengan manajemen *user* seperti autentikasi atau meminta data dari *user*. Untuk mengatasi permasalahan ini, Auth0 Inc menyediakan Auth0 agar dapat di-*deploy* secara *self-host* di *server* sendiri. Namun kelebihan ini hanya dapat dimanfaatkan bagi *developer* yang menggunakan Auth0 secara berbayar.

### WSO2 *Identity Server*

WSO2 *Identity Server* adalah produk SSO milik WSO2. WSO2 *Identity Server* dapat digunakan secara gratis karena *open-source*. Masyarakat umum secara luas dapat ikut berpartisipasi dalam mengembangkan WSO2 *Identity Server* melalui *pull request* di GitHub. WSO2 juga memungkinkan SSO di-*deploy* pada *server* privat (*self-hosted*). Dengan demikian, basis data dan media penyimpanan data tentang aplikasi *service provider* juga dapat dikontrol secara langsung oleh *developer* sehingga dapat dijamin sendiri keamanan dan *maintenance*/*uptime* *server*-nya. Seperti Auth0, WSO2 *Identity Server* juga memiliki *dashboard* yang digunakan untuk melakukan konfigurasi aplikasi *service provider*. Selain itu, WSO *Identity Server* juga mendukung banyak protokol SSO seperti SAML, OAuth, dan HTTP. WSO *Identity Server* juga menyediakan banyak integrasi dengan *identity provider* lain, seperti Facebook, Google, dan Yahoo.

Kelemahan utama dari WSO2 *Identity Server* adalah dokumentasi yang kurang rapi dan *learning curve* yang cukup tajam. *Sample application* yang sangat dasar untuk SSO dengan protokol SAML dan OAuth milik WSO2 *Identity Server* bahkan tidak bisa dijalankan. Dengan demikian, *developer* yang baru menggunakan teknologi *single sign-on* akan mengalami kesulitan dalam melakukan integrasi terhadap aplikasinya. Dengan tingkat kompleksitas aplikasi yang tinggi seperti ini, dukungan teknis *customer service* hanya dapat diperoleh apabila *developer* men-*subscribe* WSO2 *Identity Server* secara berbayar. WSO2 *Identity Server* (SSO *server*) membutuhkan *resource* memori yang tinggi ketika dijalankan, yakni sekitar 800 MB dan 500 MB *heap size*. Kebutuhan memori yang besar terjadi karena WSO2 *Identity Server* diimplementasi menggunakan bahasa pemrograman Java. WSO2 *Identity Server* menyediakan *cloud server* yang hanya bisa diakses secara berbayar. Selain itu, untuk *monitoring user*, WSO2 *Identity Server* tidak menyediakan *dashboard* secara terpusat dan harus dilakukan dari sisi aplikasi *service provider*. *Dashboard* yang disediakan WSO2 *Identity Server* hanya berfungsi sebagai *monitoring* aplikasi *service provider*, tetapi tidak untuk *monitoring user*.

### *Central Authentication Server*

*Central Authentication Server* (CAS) pada mulanya adalah sebuah protokol untuk *single sign-on*. CAS sekarang telah dikembangkan lebih lanjut menjadi *tool single sign-on* dan aplikasi *client*-nya banyak diimplementasikan menggunakan beberapa bahasa pemrograman. CAS merupakan *project open-source* milik Apereo. Dengan demikian, CAS *server* memungkinkan untuk di-*deploy* secara *self-hosted*. CAS mendukung beberapa protokol seperti CAS, SAML, OAuth, dan OpenID. CAS memiliki dokumentasi yang lengkap pada laman <https://apereo.github.io/cas/4.2.x/index.html>. CAS memiliki *standalone dashboard* (berbeda dari *server*) yang dapat digunakan untuk memonitor aplikasi *service provider*.

Walaupun memiliki dokumentasi yang lengkap, tetapi Apereo, organisasi pemilik *project* CAS, tidak menyediakan *sample application* yang bisa digunakan sebagai petunjuk dalam mengintegrasikan aplikasi dengan *Central Authentication Server*. Kelemahan CAS berikutnya adalah CAS membutuhkan memori besar untuk dijalankan. CAS *server* membutuhkan memori minimal 8 GB dan prosesor minimal 3,00 GHz (Apereo, 2015). Selain itu walaupun CAS memiliki *dashboard* untuk *monitoring* aplikasi *service provider*, CAS tidak memiliki *dashboard* untuk manajemen *user* sehingga *developer* harus membuat aplikasi *client* sendiri. Kelemahan lainnya dari CAS adalah pertukaran informasi antar komponen CAS dilakukan tidak menggunakan SSL yang menyebabkan kerentanan terhadap serangan *Man-in-the-Middle*. Selain itu, bahasa pemrograman *client* yang didukung oleh CAS hanya bahasa pemrograman kuno, seperti Java, .NET, PHP, dan Perl. Bahasa modern seperti Python, Go, Ruby tidak didukung karena CAS merupakan teknologi lama. CAS juga tidak mendukung *single sign-on* untuk *single page application* (SPA) yang menggunakan berbagai *framework* JavaScript seperti React, Redux, dan VueJS yang akhir-akhir ini sedang *trend*.

### Perbandingan *Web Single Sign-On*

Setelah melakukan analisis pada beberapa produk *single sign-on* pada subbab di atas, diperoleh beberapa poin yang dapat dibandingkan antara *web single sign-on* dengan yang lain. Berikut adalah ringkasan tabel perbandingan *web single sign-on* yang telah dianalisis.

Tabel ‎III.1 Perbandingan *Web Single Sign-On*

| No | Tipe | Auth0 | WSO2 IS | CAS |
| --- | --- | --- | --- | --- |
| 1. | Kemudahan integrasi | Mudah | Sulit | Mudah |
| 2. | Dokumentasi | Bagus | Buruk | Bagus |
| 3. | *Sample application* | Ada | Ada, tidak bisa dijalankan | Tidak ada |
| 4. | Dukungan SDK *client* | Lengkap | Lengkap | Kurang lengkap, tidak terkini |
| 5. | Dukungan protokol lain (SAML, OAuth, dll) | Ada | Ada | Ada |
| 6. | *Dashboard* untuk *service* | Ada | Ada | Tidak |
| 7. | *Dashboard provisioning user* | Ada | Tidak | Tidak |
| 8. | Hak cipta | *Proprietary* | *Open-source* | *Open-source* |
| 9. | Tipe *server* | *Cloud* | *Self-hosted* | *Self-hosted* |
| 10. | Mekanisme SSO | *Redirect* | *Redirect* | API |
| 11. | SSL | Bisa | Bisa | Tidak |
| 12. | Kebutuhan memori *server* | - | 800 MB + 500 MB *heap* | Minimum RAM sistem 8 GB |

## Analisis Solusi

Berdasarkan analisis permasalahan pada subbab sebelumnya, kali ini akan dibahas mengenai analisis solusi yang ditawarkan dalam tugas akhir ini. Secara garis besar, akan dibuat sebuah *single sign-on* baru yang memiliki fungsionalitas gabungan dari *web single sign-on* di atas dan mengurangi/menghapus kelemahan dari *web single sign-on* yang sudah ada.

### Karakteristik *Web Single Sign-On*

Dengan demikian, dalam tugas akhir ini ditawarkan *single sign-on* baru dengan karakteristik sebagai berikut.

Tabel ‎III.2 Karakteristik *Single Sign-On*

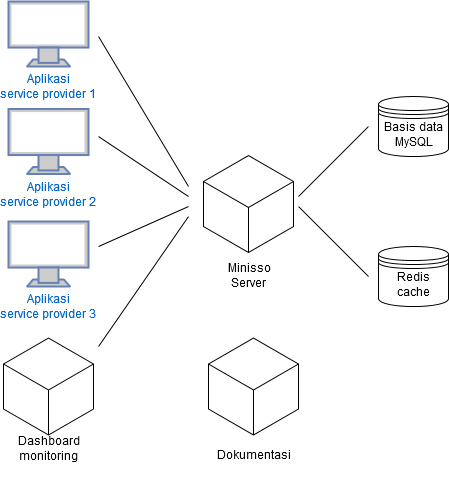
| No | Tipe | Solusi *single sign-on* |
| --- | --- | --- |
| 1. | Kemudahan integrasi | Mudah |
| 2. | Dokumentasi | Bagus |
| 3. | *Sample application* | Ada |
| 4. | Dukungan SDK *client* | Go, HTTP API |
| 5. | Dukungan protokol lain (SAML, OAuth, dll) | Tidak |
| 6. | *Dashboard* untuk *service* | Ada |
| 7. | *Dashboard provisioning user* | Ada |
| 8. | Hak cipta | *Open-source* |
| 9. | Tipe *server* | *Self-hosted* |
| 10. | Mekanisme SSO | API |
| 11. | SSL | Bisa |
| 12. | Kebutuhan memori *server* | Sedikit |

Sebagai pengembangan dari *web single sign-on* yang sudah ada sebelumnya, pada tugas akhir ini akan dibangun *web single sign-on* baru dengan karakteristik seperti di atas. Secara general, karakteristik *web single sign-on* yang dibangun merupakan perbaikan dari kelemahan *web single sign-on* yang telah dianalisis pada bab III.1. Berikut adalah penjelasan dari setiap poin karakteristik dari *single sign-on* yang akan dibangun.

1. **Kemudahan integrasi**. *Single sign-on* akan menggunakan protokol HTTP dan JSON. Saat ini, umumnya *web application* menggunakan protokol HTTP untuk berkomunikasi antar *service*. Dengan pembangunan SSO menggunakan protokol *single sign-on*, harapannya adalah *service* dengan teknologi dan bahasa apapun dapat diintegrasi *web* SSO dengan mudah. Diimplementasinya SSO menggunakan protokol HTTP memberikan ruang cerah sehingga SSO yang berkarakter *language-agnostic* dapat dicapai.
2. **Dokumentasi.** Dokumentasi yang akan dibangun haruslah mudah dipahami sehingga *developer* dapat menggunakan *web* SSO ini dengan mudah.
3. **Adanya *sample application*.** Dokumentasi saja tidak cukup untuk sebuah perangkat lunak supaya dirilis secara *open-source*. Perangkat lunak harus memiliki *sample application* yang benar-benar berhasil dijalankan.
4. **Dukungan SDK *client***. Kelebihan dari *web* SSO yang sudah terkenal dan besar adalah mereka memiliki dukungan SDK yang lengkap. Dukungan yang lengkap bisa terjadi karena jumlah tim yang besar dan memiliki basis *developer* yang kuat. Untuk pengerjaan tugas akhir ini, karena keterbatasan sumber daya manusia, *client* hanya didukung untuk bahasa Go saja. Sementara, untuk bahasa lain, SSO yang akan dibangun hanya mendukung integrasi melalui HTTP API.
5. **Dukungan protokol lain (SAML dan OAuth).** Protokol lain seperti SAML dan OAuth tidak didukung dalam *web single sign-on* ini. Web *single sign-on* yang akan dibangun bertujuan untuk melakukan simplifikasi dari teknologi *single sign-on* yang sudah ada dan rumit, menjadi *service* sederhana yang mudah diintegrasikan.
6. ***Dashboard* untuk *service*.** *Single sign-on* harus memiliki *dashboard* yang dapat digunakan untuk mengelola *application service provider*. *Dashboard* ini hanya dapat diakses oleh *admin*.
7. ***Dashboard provisioning user*.** *Single sign-on* harus memiliki *dashboard* yang digunakan untuk pengelolaan *user*.
8. **Hak cipta *open-source*.** *Web single sign-on* akan di-*open-source* ke masyarakat luas supaya dapat dikembangkan dengan bebas.
9. **Tipe *server* *self-hosted***. *Server web single sign-on* dapat dijalankan pada mesin sendiri. Dengan demikian, aplikasi *service provider* yang menggunakan *single sign-on* tidak perlu bergantung pada infrastruktur *cloud server single sign-on.*
10. **Mekanisme SSO.** *Web**single sign-on* akan diimplementasi dalam bentuk API. *Web**single sign-on* dapat menerima *request* dari aplikasi *service provider* untuk *login*/*register* atau manajemen *user*.
11. **SSL.** Seluruhtransport informasi pada sistem SSO dilakukan mengunakan *layer* yang aman sehingga aman dari serangan *Man-in-the-Middle*.
12. **Kebutuhan memori rendah.** *Server*haruslah ringan dijalankan sehingga tidak perlu membutuhkan banyak *resource*. Ini dapat dicapai dengan menggunakan bahasa Go sebagai *server*. *Service* yang diimplementasi menggunakan Go memiliki karakteristik yakni ringan untuk dijalankan.

### Kebutuhan Sistem

Sistem yang dimaksud pada subbab ini adalah keseluruhan sistem yang terlibat dalam *single sign-on* termasuk *web single sign-on*, aplikasi *service provider*, *dashboard* untuk manajemen dan *monitoring*, dan dokumentasi. Berikut adalah gambaran secara garis besar antar komponen dalam sistem.



Gambar ‎III.1 Sistem *Single Sign-On*

Aplikasi *service provider* menggunakan Minisso *server* untuk proses autentikasi. Sementara itu, Minisso *server* menggunakan basis data persisten MySQL untuk penyimpanan data, dan Redis untuk *cache* sebagai media penyimpanan data sementara yang cepat. Dashboard monitoring akan menghubungi Minisso server untuk proses manajemen user dan manajemen service.

Berdasarkan analisis yang dilakukan sebelumnya, *web single sign-on* yang akan dibangun setidaknya memiliki spesifikasi kebutuhan sistem seperti yang dijabarkan pada tabel III.3.

Tabel ‎III.3 Kebutuhan Sistem

| Kode | Kebutuhan Sistem |
| --- | --- |
| KS1 | Sistem mampu menerima autentikasi *single sign-on* dari aplikasi *service* *provider* dengan akurat. |
| KS2 | *Developer* mampu mengintegrasikan *single sign-on* dengan mudah. |
| KS3 | *Learning curve* untuk memahami cara kerja *single sign-on* tidak tajam. |
| KS4 | Ada cara untuk memonitor aplikasi *service provider* dan *user*. |
| KS5 | *Single sign-on* haruslah gratis, mudah dimodifikasi, dan dikembangkan lebih lanjut. |
| KS6 | Setiap informasi yang ditukarkan di antara sistem dilakukan secara aman. |
| KS7 | Sistem *single sign-on* ringan dijalankan. |

### Kebutuhan Fungsional *Single Sign-On*

Kebutuhan fungsional yang dibahas pada subbab ini hanyalah mencakup kebutuhan fungsional dari *web single sign-on*. Berdasarkan kebutuhan sistem yang telah dilakukan sebelumnya, *web single sign-on* yang akan dibangun setidaknya memiliki spesifikasi kebutuhan fungsional seperti yang dijabarkan pada tabel III.4.

Tabel ‎III.4 Kebutuhan Fungsional *Single Sign-On*

| Kode | Kebutuhan Fungsional *Single Sign-On* |
| --- | --- |
| KF1 | Mampu menerima pendaftaran *user* baru. |
| KF2 | Mampu menerima *login user* dan mengembalikan *token*. |
| KF3 | Mampu memberikan detil informasi *user* ketika *token* terbukti *valid*. |
| KF4 | Mampu melakukan manajemen aplikasi *service provider* (*create*, *read*, *update*, *delete*) |
| KF5 | Mampu melakukan manajemen *user*. |
| KF6 | Mampu menerima *request* dari aplikasi *service provider* untuk proses autentikasi *user* untuk keperluan *single sign-on*. |

### Kebutuhan Non-Fungsional *Single Sign-On*

Berdasarkan kebutuhan sistem yang telah dilakukan sebelumnya, *web single sign-on* yang akan dibangun setidaknya memiliki spesifikasi kebutuhan non-fungsional seperti yang dijabarkan pada tabel III.5.

Tabel ‎III.5 Kebutuhan Non-Fungsional *Single Sign-On*

| Kode | Kebutuhan Non-Fungsional *Single Sign-On* |
| --- | --- |
| KNF1 | Terdapat dokumentasi yang runtut dan mudah dipahami. |
| KNF2 | Terdapat contoh aplikasi *service provider* yang menggunakan *single sign-on* dan langsung bisa digunakan. |
| KNF3 | *Single sign-on* haruslah *open-source* dan bisa dimodifikasi setiap orang. |
| KNF4 | Transport data dilakukan menggunakan SSL. |
| KNF5 | Kebutuhan memori untuk menjalankan *server single sign-on* rendah. |

### Diagram *Use Case*

Berdasarkan kebutuhan fungsional yang telah dipaparkan pada subbab sebelumnya, maka *use case diagram* dari *single sign-on* yang akan dibangun adalah seperti pada gambar III.1 berikut.



Gambar ‎III.2 *Use Case Single Sign-On*

Berikut adalah penjelasan dari masing-masing aktor yang terlibat dalam *use case single sign-on*.

1. Aplikasi *service provider*. Merupakan aplikasi *service provider* yang menggunakan *web single sign-on* sebagai autentikasi.
2. *Developer*. Adalah entitas yang memiliki akses terhadap *single sign-on*. Karena developer merupakan pemilik *single sign-on*, oleh karena itu *developer* berhak untuk akses manajemen *single sign-on* seperti *monitoring user* dan aplikasi *service provider*.
3. Basis data relasional. Basis data relasional ini digunakan untuk media penyimpanan data permanen seperti data *user*, aplikasi *service provider*, dan menyimpan *log history user*.
4. Redis cache. Redis adalah basis data no-SQL non-persisten yang berjalan di RAM, digunakan untuk menyimpan data sementara seperti token untuk keperluan manajemen user. Redis dipilih karena performansinya yang bagus.

## Rancangan Solusi

Pembahasan mengenai rancangan solusi dibagi menjadi 4 bagian. Bagian pertama dibahas mengenai gambaran umum solusi. Bagian kedua mengenai desain *web single sign-on*. Bagian ketiga mengenai desain dokumentasi *web single sign-on*. Bagian keempat mengenai desain aplikasi *service provider*.

### Gambaran Umum Solusi

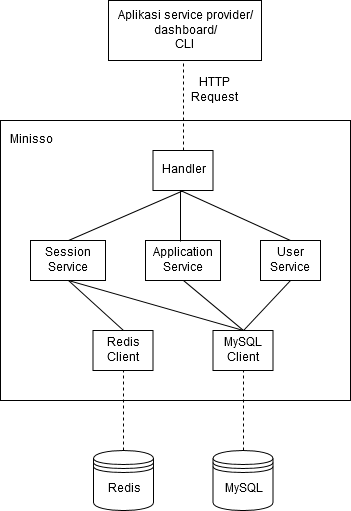
Berdasarkan analisis yang telah dilakukan, akan dibangun sebuah *web single sign-on* dengan karakteristik seperti yang sudah dipaparkan pada subbab III.2.1. Tipe *single sign-on* yang akan digunakan adalah REST API dan dilakukan menggunakan protokol HTTP menggunakan SSL untuk tingkat keamanan yang tinggi. Dengan demikian, secara umum berikut ini adalah cara kerja *web single sign-on* yang akan dibangun. Untuk memudahkan, *web single sign-on* yang akan dibangun selanjutnya akan dinamai **Minisso**.

Kode sumber server Minisso dibuka secara umum (*open-source*) pada laman <https://github.com/luqmanarifin/minisso>. Dengan demikian, seluruh akan bisa menggunakan *server* Minisso untuk mengintegrasikan aplikasinya secara mudah. Dengan di-*open-source*-nya Minisso, artinya *developer* juga bisa mengembangkan Minisso secara bebas. Kelanjutan pengembangan Minisso yang mungkin contohnya adalah pengembangan fungsional SSO, semisal integrasi dengan *identity provider* eksternal, seperti Google atau Yahoo, atau penambahan data atribut *user* sehingga bermanfaat untuk *monitoring user*.

Contoh kemungkinan pengembangan Minisso yang lain adalah pengembangan Minisso *client* dengan bahasa lain, semisal Java, JavaScript, atau Ruby. Minisso *server* hanya menyediakan API dengan protokol HTTP dengan tujuan supaya mudah diintegrasikan dengan sistem lain yang rata-rata sekarang ini berkomunikasi lewat protokol HTTP. Kelebihan lain menggunakan protokol HTTP adalah *server* tidak perlu mempedulikan bahasa yang digunakan oleh *client*. Minisso *client* akan bertindak sebagai penghubung (*plug*) antara aplikasi *service provider* dengan *server* Minisso. Tentunya bahasa dan teknologi yang digunakan dalam Minisso *client* seharusnya disesuaikan dengan aplikasi dan *framework* yang digunakan oleh aplikasi *service provider*.

### Desain *Web* *Single Sign-On*

Berikut adalah arsitektur Minisso *web* SSO. Dalam hal ini, dijelaskan modul-modul yang berperan dalam perangkat lunak *web* SSO.



Gambar ‎III.4 Arsitektur Minisso

Arsitektur Minisso melibatkan modul-modul sebagai berikut.

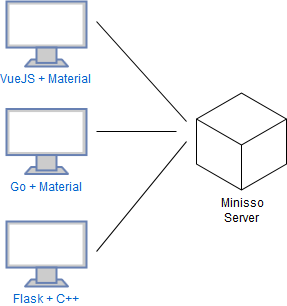
1. ***Handler***. *Handler* berfungsi untuk menerima HTTP *request* dari alamat Minisso. *Handler* juga bertanggungjawab untuk mentransformasi data dari JSON (tipe data yang dapat dioper dengan mudah di prokotol HTTP) ke tipe data Go sehingga dapat diproses oleh bahasa pemrograman.
2. ***User Service*.** *User service* bertugas memproses seluruh aktivitas yang berkaitan dengan manajemen *user*, termasuk tambah *user*, hapus *user*, ubah *user*, cari *user*.
3. ***Application Service*.** *Application service* bertugas memproses seluruh aktivitas yang berkaitan dengan manajemen aplikasi yang terdaftar pada Minisso, termasuk tambah, hapus, baca, dan ubah aplikasi.
4. ***Session Service***. *Session service* bertugas untuk memproses seluruh proses yang berkaitan dengan manajemen *session user* yang sudah *login*. Cakupan modul ini termasuk *token*, riwayat *login* berhasil/gagal, dan lainnya.
5. **MySQL *client***. MySQL *client* bertugas untuk memproses seluruh *query* pada *database* relasional MySQL.
6. **Redis *client***. Redis *client* bertugas untuk memproses seluruh *query* yang melibatkan Redis *cache*.

Desain Minisso menggunakan design pattern MVC, yakni *Model-View-Controller*.

1. *Model*: entitas yang berperan dalam komunikasi langsung kepada basis data atau media penyimpanan lainnya, semisal *cache*.
2. *View*: entitas yang bertanggung jawab dalam tampilan aplikasi yang dilihat langsung oleh *end-user*.
3. *Controller*: entitas yang berperan sebagai pengatur *business logic* aplikasi, juga sebagai penjembatan antara *view* dan *model*.

### Desain Aplikasi *Service Provider*

Dibutuhkan dua atau lebih aplikasi *service provider* untuk menguji Minisso apakah sudah berjalan sesuai yang diharapkan. Namun, dalam pengembangan tugas akhir ini, aplikasi *service provider* bukan merupakan fokus utama. Namun, aplikasi *service provider* tetap dibutuhkan untuk menguji kemampuan *web single sign-on* dalam melakukan integrasi autentikasi beberapa aplikasi. Rancangan desain aplikasi *service provider* adalah sebagai berikut.



Gambar ‎III.5 Aplikasi *Service Provider*

1. Aplikasi *service provider* baru menggunakan VueJS (JavaScript) dan *Material Design* (CSS).
2. Aplikasi *service provider* baru menggunakan Go dan *Material Design* (CSS).
3. Aplikasi *service provider* tentang mesin pencari citra milik Rifai (2018) diimplementasi menggunakan Flask (Python) dan C++.

# IMPLEMENTASI DAN EVALUASI

Pembahasan pada bab ini akan dibagi menjadi dua bagian. Bagian pertama akan dipaparkan tentang lingkungan, batasan, dan detail implementasi. Sedangkan bagian kedua dibahas mengenai teknis dan hasil pengujian terhadap *web single sign-on* yang telah dibangun.

## Implementasi

Bagian implementasi ini dibagi menjadi 3 bagian. Bagian pertama dibahas mengenai lingkungan implementasi. Bagian kedua dibahas mengenai batasan implementasi. Bagian ketiga dibahas mengenai detail implementasi *web single sign-on*.

### Lingkungan Implementasi

| Perihal | Spesifikasi |
| --- | --- |
| Sistem Operasi |  |
| CPU |  |
| RAM |  |
| Bahasa Pemrograman |  |
| Go Compiler |  |
| MySQL |  |
| Redis |  |

### Batasan Implementasi

### Detail Implementasi *Web Single Sign-On*

* Modul

## Evaluasi

Menurut Halonen (2000), autentikasi dan autorisasi seharusnya memiliki karakteristik sebagai berikut:

1. Kebenaran (*Correctness*)

Hasil dari setiap autentikasi dan autorisasi haruslah akurat.

1. Kemungkinan untuk anonim dan privasi (*Possibility to anonymity and privacy*)

Autentikasi terhadap identitas hanya diperlukan apabila benar-benar diperlukan. Apabila tidak perlu membuka identitas, maka tidak perlu identitas dibuka. Jika memungkinkan, autorisasi sebaiknya tidak dilakukan tanpa membuka identitas.

1. Kecepatan (*Speed*)

Proses autentikasi seharusnya dilakukan dengan cepat.

1. Ketahanan terhadap serangan (*Attack resistance*)

Metode autentikasi seharusnya dapat tahan terhadap jenis serangan, misalnya serangan mid-in-the-middle.

1. Murah (*Inexpensiveness*)

Proses autentikasi dan autentikasi seharusnya memerlukan ongkos tidak mahal, baik ongkos pengembangan dan pemeliharaan.

1. Kemudahan penggunaan (*User friendliness*)

Metode autentikasi sedapat mungkin mudah digunakan dan dimengerti. Pada kondisi ideal, pengguna tidak perlu mengeluarkan usaha ketika melakukan autentikasi.

1. Universal (*Universality*)

Metode autentikasi sebaiknya sedapat mungkin sama pada semua layanan.

### Skenario Uji *Web Single Sign-On*

### Kemudahan Integrasi

### Keamanan

### Ketergantungan terhadap Teknologi Tertentu

### Kemampuan Autentikasi

### Kemampuan Autorisasi

### Kemampuan Manajemen Akun

### Integrasi Sosial Media

### Dukungan Dokumentasi

DAFTAR PUSTAKA

Adabala, S., Matsunaga, A., Tsugawa, M., Figueiredo, R., & Fortes, J. A. B. *Single Sign-On in In-VIGO: Role-based Access via Delegation Mechanisms Using Short-lived User Identities*. ACIS Laboratory, University of Florida, Gainesville.

Ardagna, Claudio A., et al. (2006). *CAS++: an Open Source Single Sign-On Solution for Secure e-Services*. Crema: University Degli Study di Milano.

Apereo. (2015). Installation Requirements for CAS | Enterprise Single Sign-On for All. <https://apereo.github.io/cas/development/planning/Installation-Requirements.html#servlet-containers>. Diakses pada 25 Juli 2017.

Atricore. (2010). Simplified Identity an Access | About JOSSO. <http://www.josso.org/>. Diakses pada 18 Juli 2018.

Arianezhad, M., Kelley, T., Camp, L. J., & Stebila, D. *Comparative Eye Tracking of Experts and Novices in Web Single Sign-on*. School of Engineering Science, Simon Fraser University, Burnaby, B.C., Canada. Indiana University Bloomington, IN. Science and Engineering Faculty, Queensland University of Technology, Brisbane, Queensland, Australia.

Bauer, L., Bravo-Lillo, C., Fragkaki, E., & Melicher, W. *A Comparison of Users’ Perceptions of and Willingness to Use Google, Facebook, and Google+ Single-Sign-On Functionality*. Carniage Mellon University, Pittsburgh, PA.

Fleury, T., Basney, J., & Welch, V. *Single Sign-On for Java Web Start Applications Using MyProxy*. National Center for Supercomputing Applications.

Federal Deposit Insurance Corporation. Division of Supervision and Consumer Protection. (2004). *Putting and End to Account-Hijacking Identity Theft*. New York: FDIC.

Ford, M. D. (1998). *Identity Authentication and ‘E-Commerce‘*. The Journal of Information, Law, and Technology.

Ford, W., & Baum, M. S. (1997). Secure Electronic Commerce: Building the infrastructur for digital signature and encryption. New Jersey: Prentice Hall, Inc.

Goth, G. (2008). *Single Sign-on and Social Networks*. IEEE Computer Society, IEEE Distributed System Online, 1541-4922. vol. 8, no. 12.

Halonen, T. (2000). *Authentication and Authorization in Mobile Environment*. Finlandia: Helsinki University of Technology.

Harding, P., Johansson, L., & Klingenstein N. (2007). *Dynamic Security Assertion Markup Language Simplifying Single Sign-On*. IEEE Computer Society, IEEE Security & Privacy, 1540-7993/07.

He, Wenli. (2007). *Single Sign On*. University of Iowa.

Huhnlein, D. et al. *Options for Integrating eID and SAML*. ecsec GmbH, Ruhr-Universitat Bochum. Adolf Wurth GmbH & Co. KG.

Horst, T. W. V. D., & Seamons, K. E. (2007). *Simple Authentication for the Web*. Internet Security Research Lab, Brigham Young University, Provo, UT, USA.

Ishii, T., Inoie, A., & Okamoto, M. *Single Sign-on Using Portable IdP on USB Flash Drive*. Kanagawa Institute of Technology.

Jain, Anil. K. (2005). *On The Uniqueness of Fingerprints*. Dept. of Computer Science and Engineering, Michigan State University.

Jasig. (2009). *Central Authentication Service*. <https://wiki.jasig.org/display/CAS/Home>. Diakses pada 18 Juli 2018.

Kamil, R. (2016). *Smartcity Bandung 2016*. Presentation of Mayor of Bandung.

Kristanto, R. F. (2011). *Otentikasi dan Otorisasi Terpusat pada Aplikasi Web di Lingkungan Informatika ITB*. Program Studi Teknik Informatika, Institut Teknologi Bandung.

Munir M.T., Ir. Rinaldi. (2005). *Diktat Kuliah IF5054 Kriptografi*. Bandung: Institut Teknologi Bandung.

Neuman, B. Clifford, & Theodore Ts’o. (1994). Kerberos: An Authenticaton Service for Computer Networks. IEEE Communications Magazine, Vol 32, No 9, p. 33-38.

Novell. (2011). *Investigating Single Sign-on*. Novell Solution Provider. Waltham, MA.

OASIS. (2008). *Security Assertion Markup Language (SAML) V2.0 Technical Overview*.

Pace, Eugenio. (2015). *About Auth0 | The new way to solve Identity*. <https://auth0.com/about>. Diakses pada 24 Juli 2018.

Pashadilis, Andreas dan Chris J. Mitchell. (2003). *Single Sign-On using Trusted Platforms*. London: University of London.

Park, K., Lim, S. S., & Park, K. H. (2008). *Computationally Efficient PKI-Based Single Sign-On Protocol PKASSO for Mobile Devices*. IEEE Transactions on Computers, vol. 57, no. 6.

Rifai, Wiwit. (2018). *Pengembangan Mesin Pencari Citra dengan Penanganan Semantik Kemiripan yang Berbeda*. Bandung: Institut Teknologi Bandung.

Sun, S.-T., & Beznosov, K. *The Devil is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems*. Laboratory for Education and Research in Secure Systems Engineering, Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, Canada.

Sun, S.-T., Boshmaf, Y., Hawkey, K., & Beznosov, K. *A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On*. Laboratory for Education and Research in Secure System Engineering (LERSSE), Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, Canada.

Sun, S.-T. et al. (2010). *What Makes Users Refuse Web Single Sign-On? An Empirical Investigation of OpenID*. University of British Columbia, Vancouver, BC, Canada. Dalhousie University, Halifax, NS, Canada.

Sun, S.-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., and Beznosov, K. 2013. *Investigating users’perspectives of Web single sign-on: Conceptual gaps and acceptance model*. ACM Trans. Internet Technol. 13, 1, Article 2 (November 2013), 35 pages.

Tanenbaum, & Steen V., (2007). Distributed System: Principles and Paradigms 2nd Edition. Pearson Education. Vrije Universiteit, Amsterdam, The Netherlands.

Volchkov, A. (2001). *Revisiting Single Sign-On. A Pragmatic Approach in a New Context*. IEEE Computer Society Magazine IT Pro, 1520-9202/01.

Whitehead, Prof. Jim. (2006). *PHP Session Management*. CMPS.

WSO2 Inc, (2015). *WSO2 Identity Server Documentation | Architecture*. <https://docs.wso2.com/display/IS530/Architecture>. Diakses pada 25 Juli 2018.

Yang, R. Li, G., Lau, W. C., Zhang, K., & Hu, P. *Model-based Security Testing: an Empirical Study on OAuth 2.0 Implementations*. The Chinese University of Hong Kong.