IMPLEMENTASI PROTOKOL PENDUKUNG SINGLE SIGN-ON BERDASAR SISTEM IDENTITY DAN ACCESS MANAGEMENT KEYCLOAK

Skripsi

oleh
TIMOTHY DICKY HERLAMBANG
71150013

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2019

IMPLEMENTASI PROTOKOL PENDUKUNG SINGLE SIGN-ON BERDASAR SISTEM IDENTITY DAN ACCESS MANAGEMENT KEYCLOAK

Skripsi

Diajukan kepada Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

TIMOTHY DICKY HERLAMBANG
71150013

PROGRAM STUDI INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2019

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI PROTOKOL PENDUKUNG SINGLE SIGN-ON BERDASAR SISTEM IDENTITY DAN ACCESS MANAGEMENT KEYCLOAK

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 19 Desember 2019

TIMOTHY DICKY HERLAMBANG

71150013

HALAMAN PERSETUJUAN

Judul Skripsi	:	IMPLEMENTASI PROTOKOL PENDUKUNG SINGLE SIGN-ON BERDASAR SISTEM IDENTITY DAN ACCESS MANAGEMENT KEYCLOAK
Nama Mahasiswa	:	TIMOTHY DICKY HERLAMBANG
N I M	:	71150013
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Gasal
Tahun Akademik	:	2019/2020

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 19 Desember 2019

Dosen Pembimbing I	Dosen Pembimbing II
Budi Susanto, SKom.,M.T.	Willy Sudiarto Raharjo, S.Kom.,M.Cs.

HALAMAN PENGESAHAN

IMPLEMENTASI PROTOKOL PENDUKUNG SINGLE SIGN-ON BERDASAR SISTEM IDENTITY DAN ACCESS MANAGEMENT KEYCLOAK

Oleh: TIMOTHY DICKY HERLAMBANG / 71150013

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 13 Desember 2019

Yogyakarta, 19 Desember 2019
Mengesahkan,

Dewan Penguji:

1. Budi Susanto, SKom.,M.T.
2. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
3. R. Gunawan Santosa, Drs. M.Si.
4. Junius Karel, S.Si., M.T.

Dekan

(Restyandito,S.Kom.,MSIS.,Ph.D.)

Ketua Program Studi

(Gloria Virginia,Ph.D.)

PERNYATAAN PERSETUJUAN PUBLIKASI

TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS SECARA ONLINE UNIVERSITAS KRISTEN DUTA WACANA

Saya yang bertanda tangan di bawah ini:

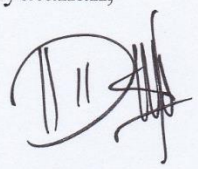
NIM	: 71150013
Nama	: Timothy Dicky Herlambang
Prodi/ Fakultas	: Informatika/ Teknologi Informasi
Judul Tugas Akhir	: Implementasi Protokol Pendukung *Single Sign-on* Berdasar Sistem *Identity* dan *Access Management* Keycloak

bersedia menyatakan Tugas Akhir kepada Universitas melalui Perpustakaan untuk keperluan akademis dan memberikan **Hak Bebas Royalti Non Eksklusif *(Non-exclusive Royalty-free Right)*** serta bersedia Tugas Akhirnya dipublikasikan secara online dan dapat diakses secara lengkap *(full access)*.

Dengan Hak Bebas Royalti Non Eksklusif ini Perpustakaan Universitas Kristen Duta Wacana berhak menyimpan, mengalihmedia/ formatkan, mengelola dalam bentuk database, merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/ pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenar-benarnya.

Yogyakarta, 20 Desember 2019

Yang menyatakan,



71150013 – Timothy Dicky Herlambang

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kepada Tuhan Yesus Kristus atas berkat dan rahmatnya penulis dapat menyelesaikan laporan skripsi yang berjudul "Implementasi Protokol Pendukung *Single Sign-on* Berdasar Sistem *Identity* dan *Access Management* Keycloak". Penulis menyadari bahwa selesainya skripsi ini tidak lepas dari restu dan dukungan dari berbagai pihak, sehingga pada kesempatan ini penulis ingin menyampaikan terima kasih kepada:

1. Ir. Henry Feriadi, M.Sc., Ph.D selaku Rektor Universitas Kristen Duta Wacana.
2. Restyandito, S.Kom., MSIS, Ph.D. selaku Dekan Fakultas Teknologi Informasi.
3. Gloria Virginia, S.Kom., MAI, Ph.D. selaku Ketua Program Studi Informatika.
4. Budi Susanto, S.Kom., M.T. selaku dosen pembimbing I untuk bimbingan dari berbagai aspek skripsi sehingga dapat membuat skripsi yang ditulis menjadi lebih baik.
5. Willy Sudiarto Raharjo, S.Kom., M.Cs. selaku dosen pembimbing II untuk bimbingan dari berbagai aspek skripsi sehingga dapat membuat skripsi yang ditulis menjadi lebih baik.
6. Pihak Gereja Kristen Indonesia yang memberikan restu dan masukan untuk dibangunnya sistem yang menjadi penelitian skripsi ini.
7. Dosen-dosen selama kuliah dari semester pertama hingga terakhir yang memberikan ilmu yang berharga dan mendukung kelancaran penyelesaian laporan skripsi ini.
8. Teman-teman dari Program Studi Informatika yang bersama-sama berjuang untuk dapat menempuh studi dari awal hingga akhir.
9. Keluarga besar penulis yang selalu memberi dukungan dan motivasi hingga skripsi dapat diselesaikan.
10. Teman-teman dekat penulis yang selalu memberi dukungan, hiburan, dan motivasi hingga skripsi dapat diselesaikan.
11. Kerabat kerja penulis yang selalu memberi inspirasi dan dukungan hingga skripsi ini dapat diselesaikan.

Penulis ingin mengucapkan terima kasih yang sebesar-besarnya untuk selesainya skripsi ini. Terima kasih juga ingin penulis sampaikan untuk orang-orang yang tidak dapat disebutkan satu per satu.

Yogyakarta, 20 Desember 2019

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

SSO	: *Single Sign-on*
SAML	: *Security Assertion Markup Language*
LDAP	: *Lightweight Directory Access Protocol*
SISWA GKI	: *Sistem Informasi Sinode Wilayah GKI*
RBAC	: *Role Base Access Control*
API	: *Application Programming Interface*
JWT	: *JSON Web Token*
IAM	: *Identity and Access Management*
JSON	: *JavaScript Object Notation*

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Dalam sistem yang besar dan kompleks, pengguna diharuskan melakukan autentikasi berulang kali dengan menggunakan berbagai akun untuk mendapatkan masing-masing layanan yang ditawarkan oleh sistem. Hal ini dapat menyulitkan pengguna dalam mengingat berbagai kombinasi ID dan kata sandi masing-masing layanan. Metode *Single Sign-on* (SSO) dinilai lebih memudahkan pengguna dalam menggunakan sistem, karena hanya dengan satu akun, pengguna dapat mengakses ke berbagai layanan yang disediakan oleh sistem. SSO belum banyak diterapkan karena dinilai rumit dalam mengimplementasikannya.

SSO dapat diterapkan dengan berbagai cara, dengan berbagai protokol (Kukic, 2012). Setiap protokol mempunyai cara masing-masing dalam melakukan autentikasi dan otorisasi terhadap pengguna. Oleh sebab itu, pengembang harus mengetahui protokol yang sesuai dengan sistem yang akan dikembangkannya. Hal tersebut yang menyebabkan penulis ingin mengetahui protokol manakah yang dapat diimplementasikan ke berbagai skenario dalam sistem.

Keycloak merupakan aplikasi yang menyediakan layanan untuk mengelola identitas dan manajemen akses yang menerapkan metode *Single Sign-on*. Keycloak dapat melakukan autentikasi serta otorisasi pengguna dengan menggunakan protokol OpenID Connect dan SAML. SSO yang ditawarkan Keycloak juga dapat digunakan untuk *Identity Brokering* pada *login* sosial media, dengan cara mendaftarkan setiap akunnya ke dalam *Account Management Console*. Keycloak juga menawarkan fitur *user federation* yang dapat menghubungkan *Lightweight Directory Access Protocol (LDAP), Active Directory servers* maupun *relational database* ke dalam satu proses autentikasi dan otorisasi Keycloak. Keycloak juga menawarkan *Client Adapters* yang mempermudah mengamankan berbagai aplikasi dan layanan pada sisi pengguna. Dengan menggunakan *Admin Console*, administrator dapat mengaktifkan atau menonaktifkan fitur-fitur Keycloak,

administrator juga dapat memberikan otorisasi maupun pengelolaan kepada penggunanya.

Ide dalam penelitian ini berawal dari Sistem Informasi Sinode Wilayah GKI (SISWA GKI) yang akan menggunakan banyak platform pada sistem tersebut, seperti web, desktop, dan *mobile*, sedangkan sistem tersebut harus menerapkan metode SSO untuk memudahkan pengguna dalam autentikasi dan otorisasi. Alasan manajerial mendasari SISWA GKI menerapkan metode SSO dengan menggunakan Keycloak. Keycloak sebagai penyedia identitas dan manajemen akses akan memudahkan petugas administrasi Sinode dalam mengelola pengguna SISWA GKI yang terdiri dari 89 Gereja dan akan aktif berganti setiap jangka waktu tertentu. Penelitian ini mencoba menggambarkan cara implementasi metode SSO untuk SISWA GKI dengan metode *prototyping*.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang ada, rumusan masalah yang dibahas pada penelitian ini adalah: Bagaimana membangun suatu sistem aplikasi yang memanfaatkan *Single Sign-on* untuk autentikasi dan otorisasi pengguna dengan menggunakan Keycloak sebagai sistem penyedia identitas dan manajemen akses?

1.3. Batasan Masalah

Adapun batasan masalah yang berkaitan dengan penelitian ini adalah sebagai berikut:

- Aplikasi yang dibangun adalah aplikasi *prototype* Sistem Informasi Sinode Wilayah GKI (SISWA GKI) dan berjalan *multiplatform*, yaitu web, desktop, dan *mobile*.
- Layanan yang dikembangkan merupakan dua layanan berbasis web servis untuk modul jemaat dan gereja.
- Protokol yang digunakan yaitu OpenID Connect.
- Penyedia layanan *Single Sign-on* yang digunakan yaitu Keycloak.
- Otorisasi yang digunakan berbasis Role Base Access Control (RBAC)

1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk membangun suatu sistem aplikasi *multiplatform* yang memanfaatkan *Single Sign-on* untuk autentikasi dan otorisasi pengguna dengan protokol OpenID Connect.

1.5. Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai gambaran atau panduan dalam mengimplementasikan metode *Single Sign-on* pada aplikasi berbasis web, desktop, dan *mobile* dengan menggunakan Keycloak.

1.6. Metodologi Penelitian

Metode penelitian yang digunakan dalam penelitian ini yaitu metode *prototyping*. Penelitian dilakukan dengan membuat *prototype* sistem informasi gereja sederhana, yang berjalan *multiplatform*. Arsitektur sistem ini berbasis *RESTful API*. Sistem yang dibangun secara garis besar terdiri dari tiga jenis aplikasi, yaitu Keycloak sebagai penyedia layanan autentikasi dan otorisasi, aplikasi *back-end* web servis, dan aplikasi *front-end* yang berjalan pada tiga platform. Keycloak bertugas untuk melakukan autentikasi kepada pengguna dan memberikan *token* otorisasi. Aplikasi *back-end* merupakan aplikasi web servis yang berhubungan langsung dengan basis data dan diamankan dengan Keycloak berbasis JSON Web Token (JWT), sehingga aplikasi lain yang menggunakan servis *back-end* ini harus menggunakan *token* dari Keycloak. Aplikasi *front-end* dibangun pada tiga platform yaitu *mobile*, web dan desktop. Aplikasi *front-end* berhubungan langsung dengan pengguna untuk melakukan CRUD jemaat dan gereja. Aplikasi *front-end* menggunakan servis *back-end* untuk menyimpan informasi jemaat sehingga aplikasi *front-end* juga berhubungan dengan Keycloak untuk melakukan autentikasi pengguna untuk mendapatkan *token* otorisasi. Ketiga jenis aplikasi tersebut dipasang langsung pada layanan *hosting* untuk mengetahui masalah-masalah yang mungkin terjadi pada saat implementasi.

Data yang diperlukan dalam penelitian ini adalah data pengguna yang bersifat fiksi. Data pengguna tersebut memiliki *role user* atau *admin*. *Role user* hanya

diperbolehkan melakukan fungsi *GET* ke servis *back-end,* sedangkan *role admin* diperbolehkan melakukan fungsi POST, PUT, dan DELETE.

Pada tahap testing penelitian ini menguji pertukaran *token* yang terjadi antara aplikasi *front-end* dan *back-end* sesuai *role* dari pengguna, bagaimana metode *Single Sign-on* berjalan, bagaimana aplikasi *front-end* menanggapi respons *back-end* ketika otorisasi ditolak, dan bagaimana aplikasi *front-end* menyimpan *token* agar *user* tidak harus selalu melakukan *login* setiap kali aplikasi di buka.

1.7. Sistematika Penulisan

Bab 1 Pendahuluan. Dalam bab ini dijelaskan gambaran umum mengenai penelitian ini. Gambaran umum tersebut meliputi latar belakang permasalahan, perumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan.

Bab 2 Tinjauan Pustaka dan Landasan Teori. Isi dari bab ini merupakan ulasan penelitian-penelitian yang sudah dilakukan sebelumnya yang terkait dengan tugas akhir ini. Selain itu juga dijelaskan landasan teori yang mendasari penelitian ini.

Bab 3 Metodologi Penelitian. Bab ini membahas tentang metode/cara yang digunakan untuk melakukan penelitian. Hal yang ditulis meliputi bahan yang digunakan, termasuk alat yang digunakan, perancangan penelitian, dan perancangan pengujian penelitian

Bab 4 Hasil dan Pembahasan. Bab ini membahas tentang analisis dan pemaparan hasil dari penelitian yang dilakukan. Hasil yang didapat dibahas lebih lanjut secara mendetail pada bab ini. Kemudian hasil pengujian juga dipaparkan dan juga dianalisis untuk mendapat suatu informasi baru dari penelitian ini

Bab 5 Kesimpulan dan Saran. Bab ini berupa kesimpulan dari hasil penerapan sistem yang dilakukan pada penelitian ini serta disertai saran yang diberikan untuk penelitian berikutnya maupun penggunaan hasil penelitian yang sudah dilakukan.

BAB 5
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Membangun sistem aplikasi yang memanfaatkan metode *Single Single-on* dengan menggunakan Keycloak sebagai penyedia identitas dan akses pengguna dapat diterapkan menggunakan *library* Keycloak Springboot Starter pada platform web, *library* Keycloak Installed Adapter pada platform desktop, dan AppAuth pada platform *mobile*. Secara umum setiap *library* dapat diterapkan dan dapat menjawab semua kebutuhan dasar proses autentikasi dan otorisasi dengan metode *Single Sign-on*. *Library* Keycloak Springboot Starter pada platform web berhasil memenuhi semua kebutuhan dasar yang diperlukan, namun *library* Keycloak Installed Adapter pada platform desktop dan AppAuth pada platform *mobile* perlu dilakukan penambahan fungsi untuk menjawab beberapa kebutuhan dasar yang diperlukan. Fungsi yang perlu ditambahkan sebagian besar berhubungan dengan pengelolaan *token* pengguna dan pengelolaan HTTP respons yang akan diterima. Fungsi-fungsi tersebut telah berhasil diterapkan dan diuji dengan *tes case* yang telah dibentuk. Penelitian ini juga menemukan masalah yang mendasar pada proses *logout*. Proses *logout* pada platform desktop dan *mobile* gagal dalam menghapus sesi Keycloak, atau yang disebut juga dengan proses *invalidate token.* Kekurangan dalam setiap *library* sudah dibahas dan berhasil diselesaikan melalui penelitian ini.

Penelitian ini juga membuktikan proses otorisasi dapat berjalan antar aplikasi dengan layanan web servis. Hal ini terbukti dari pertukaran *token* yang terjadi pada sistem dapat berjalan dengan lancar. Aplikasi *front-end* dapat menerima *token* hasil dari proses *login* dengan Keycloak, dan menggunakan *token* tersebut untuk melakukan permintaan servis *back-end. Token* yang diterima aplikasi *back-end* melalui header Authorization berhasil divalidasi kembali oleh Keycloak sehingga aplikasi *back-end* mendapatkan informasi otorisasi dari pengguna dan dapat memberikan respons yang tepat.

Kebutuhan fungsional mendasar untuk proses autentikasi dan otorisasi seperti *login*, *logout*, *handle* respons 401 dan 403 serta pengelolaan *token* sudah di

implementasikan dan diuji melalui pengujian mandiri dan mendapatkan hasil yang sesuai dengan yang diharapkan.

5.2. Saran

Sistem yang dibangun pada penelitian ini masih berupa *prototype*, sehingga masih banyak aspek yang dapat dikembangkan. Penelitian ini hanya menggambarkan cara implementasi metode *Single Sign-on* pada platform web, desktop, dan *mobile* dengan menggunakan Keycloak. Penelitian ini tidak mengimplementasikan metode SSO ke Sistem Informasi Sinode Wilayah GKI (SISWA GKI) yang sesungguhnya karena waktu penelitian ini bersamaan dengan waktu pengembangan SISWA GKI. Penelitian selanjutnya dapat melakukan implementasi metode SSO ke sistem yang nyata baik SISWA GKI maupun sistem lain yang memerlukan metode SSO untuk autentikasi maupun otorisasi pengguna, baik menggunakan Keycloak maupun penyedia identitas dan akses manajemen lainnya. Penelitian selanjutnya juga dapat berupa pengujian keamanan pada sistem yang menerapkan SSO dengan Keycloak, serta perbandingan keamanannya dengan penyedia identitas dan akses managemen lain.

DAFTAR PUSTAKA

Beltran, V. (2016). Charcterization of Web Single Sign-on Protocols. *IEEE Communication Magazine*, 24-30.

Dhamdhere, M., & Karande, S. (2017). Identity And Access Management: Concept, Challenge, Solutions. *International Journal of Latest Trends in Engineering and Technology*, 300-308.

Identity Management Institute. (2018, September 20). *Identity and Access Management Protocols*. Diambil kembali dari Identity Management Institute: https://www.identitymanagementinstitute.org/identity-and-access-management-protocols/

Kukic, A. (2012). *The Definitive Guide to Single Sign On (SSO).* Buenos Aires: Auth0.

Kutera, R., & Gryncewicz, W. (2016). Single sign on as an effective way of managing user identity in distributed web systems. The ActGo-Gate project case study . *Informatyka Ekonomiczna*, 25-43.

Pudyatmoko, A. A. (2015). *Studi Literatur: Analisis Kebutuhan dalam Membangun Sistem Web Single Sign-On, Studi Kasus Akses Situs Internal Kampus untuk Mahasiswa Informatika UKDW.* Diambil kembali dari Sistem Informasi Tugas Akhir Universitas Kristen Duta Wacana: http://sinta.ukdw.ac.id

RedHat. (2018, September 20). *About Keycloak.* Diambil kembali dari Keycloak: https://www.keycloak.org/about.html

Siriwardena, P. (2014). *Advanced API Security: Securing APIs with OAuth 2.0, OpenID Connect, JWS, and JWE.* Apress.

Somorovsky, J., Mayer, A., Schwenk, J., Kampmann1, M., & Jensen, M. (2012). On Breaking SAML: Be Whoever You Want to Be. *USENIX Security Symposium*, 397-412.

Spasovski, M. (2013). *OAuth 2.0 Identity and Access Management Patterns.* Birmingham - Mumbai: Packt Publishing Ltd.

Subhash, K. B., & Kahate, S. A. (2016). Different Framework for Single Sign On (SSO). *International Journal of Computer Science and Mobile Computing*, 53-56.

Techopedia. (2018, September 20). *Single Sign-On (SSO)*. Diambil kembali dari Technopedia: https://www.techopedia.com/definition/4106/single-sign-on-sso

Tsyrklevich, E., & Tsyrklevich, V. (2007). Single Sign-On for the Internet: A Security Story. *BlackHat*, 340.