

SKENARIO IMPLEMENTASI SISTEM INFORMASI IDENTITAS DIGITAL DENGAN MENGGUNAKAN WSO2 IS DI STMIK “AMIKBANDUNG”

Andi Rahayu¹, Hermawaty², Muh Abdul Mujib³ Rizal DZ⁴

^{1,2,3}Jurnal JOINT, STMIK AMIKBANDUNG

¹andira.1442909@gmail.com, ²emma@stmik-amikbandung.ac.id, ³Mujib@stmik-amikbandung.ac.id,

⁴Rizal@stmik-amikbandung.ac.id

Intisari— Semakin berkembangnya teknologi menjadikan banyaknya aplikasi yang digunakan dalam berbagai aktifitas. Sebagian besar pengguna menggunakan berbagai macam *credential* (*username* dan *password*) yang berbeda untuk *login* ke berbagai layanan aplikasi yang tersedia. Berdasarkan permasalahan, maka diusulkan sistem *Single Sign On* (SSO). untuk autentifikasi terhadap pengguna, dimana pengguna bisa mengakses beberapa aplikasi tanpa harus *login* di masing-masing aplikasi. Dalam penerapan SSO digunakanlah WSO2 IS sebagai *Identity Provider* dimana aplikasi *server* ini memfasilitasi keamanan saat menghubungkan dan mengelola banyak identitas di berbagai aplikasi. Dalam pengembangannya dibuat juga aplikasi yang bertindak sebagai *Service Provider* (pihak yang memerlukan otentikasi) dengan berbagai macam protokol seperti SAML dan OPENID. Hasil dari penerapan SSO menggunakan WSO2 IS dan aplikasi dengan protokol SAML dan OPENID berhasil membuat sistem untuk mengizinkan pengguna dapat mengakses seluruh sumber daya dalam jaringan hanya dengan menggunakan satu *credential* saja.

Kata kunci— *Credential*, *Single Sign On*, WSO2 IS, SAML, OPENID.

Abstract— The continued development of technology makes the number of applications used in various activities. Most users use different kinds of credentials (username and password) to log into the various available application services. Based on the problem, the *Single Sign On* (SSO) system is proposed for user authentication, where users can access several applications without having to log in to each application. In the application of SSO, WSO2 IS is used as an Identity Provider where this server application facilitates security when connecting and managing multiple identities in various applications. In its development, an application that acts as a Service Provider (the part that requires authentication) is also made with various protocols such as SAML and OPENID. The results of implementing SSO using WSO2 IS and applications with SAML and OPENID protocols succeeded in making the system allow users to access all resources in the network using only one credential..

Keywords— *Credential*, *Single Sign On*, WSO2 IS, SAML, OPENID..

I. PENDAHULUAN

Dewasa ini teknologi berbasis *cloud computing* menjamur dimana-mana. Berbagai layanan ditawarkan mulai dari layanan komersial sampai layanan kesehatan dan pendidikan. Layanan *cloud computing* mulai menggantikan layanan tradisional. Memberikan dampak signifikan terhadap pola hidup dan perubahan zaman.

Dengan maraknya layanan berbasis *cloud computing* munculah sistem dan aplikasi dengan fungsi yang berbeda-beda. Setiap sistem aplikasi memiliki sistem autentikasi data yang terpisah dengan yang lain sehingga bisa membuat beban *server* menjadi lebih berat karena server harus melayani setiap request autentikasi user yang ingin mengakses semua layanan yang tersedia. Untuk dapat mengakses berbagai semua layanan yang tersedia, pengguna juga harus melewati sebuah proses autentikasi yang berbeda-beda. Sehingga muncul kesulitan ketika pengguna harus mengingat ID dan *password* di setiap aplikasi.

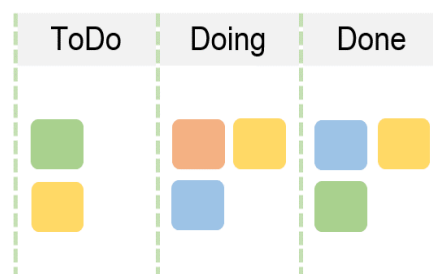
Salah satu metode yang penting demi mengurangi beban server dan pengguna maka diterapkan metode *Single Sign On* (SSO). SSO adalah sebuah teknologi yang membantu pengguna untuk dapat mengakses dan menggunakan suatu layanan yang terdapat pada semua aplikasi yang ada. SSO memberikan efisiensi dan keamanan bagi pengguna dalam mengelola serta mengakses berbagai layanan aplikasi. SSO meng autentikasi user untuk dapat mengakses semua aplikasi yang telah di-*authorized* untuk dapat diakses. Hal ini menghilangkan permintaan autentikasi lagi ketika *user* ingin

mengganti aplikasi yang lain selama *session* berlaku. Dengan sistem ini user tidak akan kesulitan untuk mengakses banyak aplikasi dalam satu waktu dengan satu akun saja.

II. METODE PENELITIAN

A. Metode Pengembangan Sistem

Metode pengembangan yang akan di gunakan dalam penelitian ini adalah *Kanban*. *Kanban* merupakan suatu metode untuk memvisualisasikan proses pekerjaan yang dilakukan saat kita sedang mengembangkan suatu Software. Dengan menggunakan metode ini dapat melacak *Bottleneck* dalam pengembangan aplikasi.



Gambar 1 Metodologi Agile: KANBAN [7]

Pada saat ini, metodologi *Agile* lebih sering digunakan dalam *Software Development Life Cycle* (SDLC) dibandingkan dengan metodologi *Waterfall*. Metodologi

Agile memiliki beberapa keunggulan dibandingkan dengan metodologi *Waterfall* yaitu:

- Lebih banyak berinteraksi
- Ruang untuk perubahan.
- *Release* yang cepat.
- Transparan
- Fokus kepada *user*
- Fokus kepada *Business Value*.
- Meningkatkan kualitas

III. HASIL PENELITIAN

Penelitian yang terkait:

Menurut Firda Zulivia Abraham, Paulus Insap Santosa, dan Wing Wahyu Winarno, dalam jurnalnya *Digital signature as green information and communication technology (ICT)* bahwa dengan tanda tangan digital dapat mengurangi penggunaan kertas dimana dengan mengurangi kertas dan beralih ke dokumen elektronik sepenuhnya akan mewujudkan Green ICT, terutama di lingkungan pemerintah. Dengan Tanda Tangan Digital Akan mewujudkan kembali semangat awal pengembangan TIK, yaitu menjadikan teknologi yang ramah lingkungan. Sedangkan pada penelitian Thalys Noor Cahyadi, dengan topic penelitian: “Aspek hukum pemanfaatan digital signature dalam meningkatkan efisiensi, akses dan kualitas *fintech* syariah”, menarik kesimpulan bahwa berdasarkan Keputusan digital, tandatangan digital memiliki kekuatan dan akibat hukum yang sah selayaknya tanda tangan basah.

Single Sign On merupakan salah satu fitur utama di produk WSO2 Identity Server yang memungkinkan user untuk dapat mengakses berbagai aplikasi lain dengan menggunakan kredensial yang sama. Dalam paper ini akan dijelaskan bagaimana cara melakukan konfigurasi Single Sign On antara Service Provider dan Identity Provider dengan WSO2 Identity Server menggunakan protokol OpenID Connect (OIDC).

Hasil penelitian penulis adalah sebagai berikut:

Pada tahap ini menjelaskan tentang hasil penelitian pada sistem yang telah dibuat.

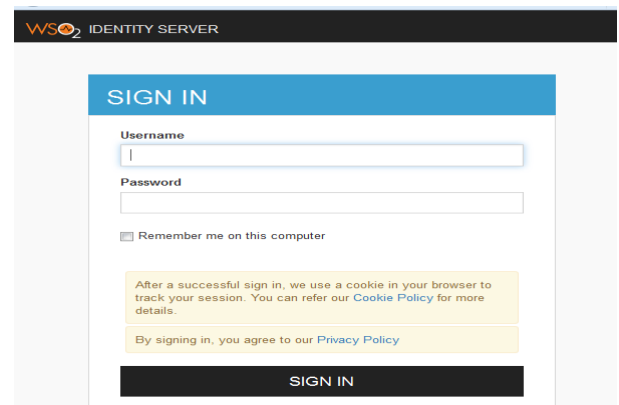
A. Implementasi Program Sampel Aplikasi yang mendukung SSO berbasis web berupa *info-amik.com*

Sistem aplikasi info merupakan suatu sampel aplikasi yang digunakan untuk mensimulasikan info mahasiswa seperti data pribadi mahasiswa beserta daftar nilai. Untuk masuk ke sistem info maka diharuskan login terlebih dahulu.



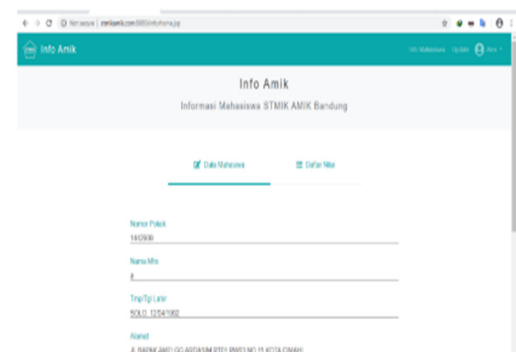
Gambar 1. Tampilan login aplikasi info

Setelah menekan tombol *login* maka sistem akan men-direct masuk ke sistem WSO2 IS, disini pengguna akan memasukkan *username* dan *password*.



Gambar 2. Tampilan credential aplikasi info

Jika *username* dan *password* yang dimasukan sudah benar maka, sistem akan men-direct kembali dengan membawa pesan ke sistem aplikasi info. Dan aplikasi info akan memverifikasi pesan tersebut dan memberikan akses masuk jika benar.



Gambar 3. Tampilan aplikasi info

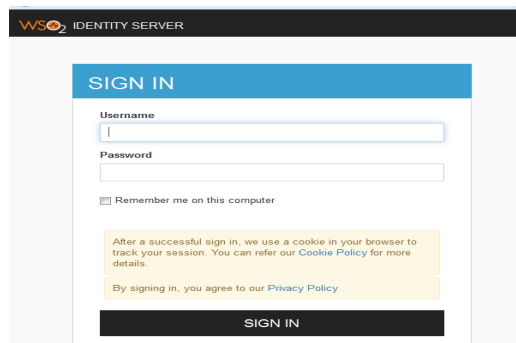
B. Implementasi Program Sampel Aplikasi yang mendukung SSO berbasis web berupa *lms-amik.com*

Sistem aplikasi lms merupakan suatu sampel aplikasi yang digunakan untuk mensimulasikan lms mahasiswa seperti *profile* mahasiswa, daftar matakuliah yang diikuti, kalender perkuliahan, dll. Untuk masuk ke sistem lms maka diharuskan *login* terlebih dahulu.



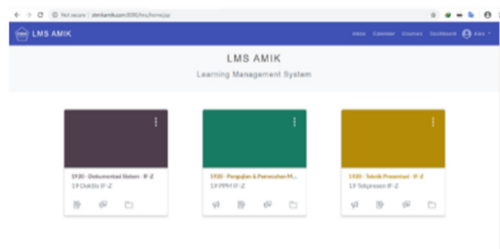
Gambar 4. Tampilan login aplikasi lms

Setelah menekan tombol *login* maka sistem akan *direct* masuk ke sistem WSO2 IS, disini pengguna akan memasukkan *username* dan *password*



Gambar 5. Tampilan credential aplikasi lms

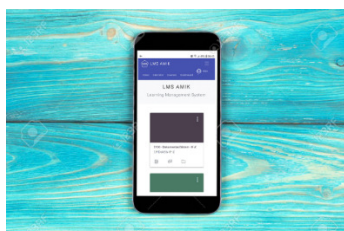
Jika *username* dan *password* yang dimasukan sudah benar maka, sistem akan *direct* kembali dengan membawa pesan ke sistem aplikasi lms. Dan aplikasi lms akan memverifikasi pesan tersebut dan memberikan akses masuk jika benar.



Gambar 6. Tampilan aplikasi lms

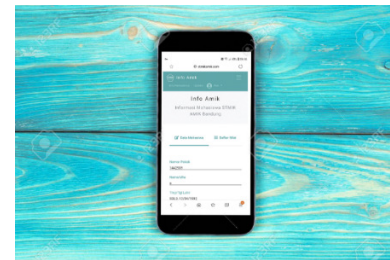
C. Implementasi Program Sampel Aplikasi yang mendukung SSO berbasis mobile

Sistem aplikasi info dan lms selain bisa digunakan dalam perangkat *desktop* juga dimungkinkan dalam berjalan dalam perangkat *mobile*.



Gambar 7. Tampilan aplikasi mobile lms

Dengan implementasi di perangkat *mobile* yang memiliki keterbatasan ukuran layar, aplikasi dimanajemen sehingga menampilkan sesuai prioritas



Gambar 8. Tampilan aplikasi mobile info

D. Implementasi Skenario Menggunakan Metode SAML

Dalam implementasi metode *SAML* terbagi kedalam 2 dua jenis utama penyedia *SAML*, *identity provider*, dan *service provider*.

1. *Identity provider* berupa WSO2 IS
2. *Service Provider* berupa Aplikasi info dan aplikasi lms

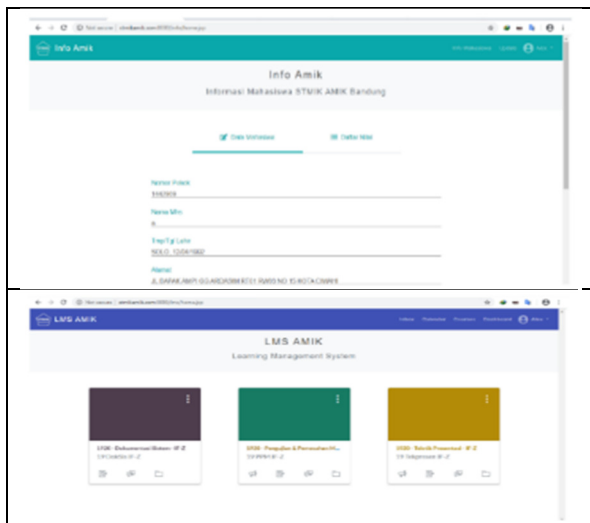
Dalam kondisi normal aplikasi harus login masing-masing setiap masuk ke setiap aplikasi. dengan SSO menggunakan metode *SAML* maka cukup satu kali memasukkan *credential*, maka di aplikasi kedua dan selanjutnya, aplikasi akan langsung *men-direct* ke halaman utama tanpa kembali memasukkan *credential* lagi.



Gambar 9. Tampilan login pada penerapan SAML

Aplikasi info dan lms bekerja dengan mengirimkan informasi tentang pengguna, *login*, dan atribut antara *Identity provider* dan *Service provider*. Setiap pengguna masuk sekali ke aplikasi dengan WSO2 IS, dan kemudian WSO2 IS dapat meneruskan atribut *SAML* ke aplikasi ketika pengguna mencoba mengakses layanan tersebut. aplikasi meminta otorisasi dan otentikasi dari WSO2 IS. Karena kedua sistem tersebut menggunakan bahasa yang sama *SAML*, pengguna hanya perlu masuk sekali. Setiap WSO2 IS dan Aplikasi harus menyetujui konfigurasi untuk *SAML*. Kedua ujung harus memiliki konfigurasi yang tepat agar otentikasi *SAML* berfungsi dengan baik.

SAML memungkinkan pengguna untuk mengakses beberapa aplikasi secara aman hanya dengan menggunakan satu set kredensial sekaligus. Pengguna harus *login* hanya pada satu titik dan semua aplikasi lain dapat diakses tanpa login ulang. Karena pengguna memerlukan satu set kredensial, mereka bebas menyimpan beberapa nama pengguna dan kata sandi untuk setiap aplikasi secara terpisah.



Gambar 10. Tampilan aplikasi pada penerapan SAML

E. Implementasi Program Menggunakan Metode OAuth/OpenID Connect

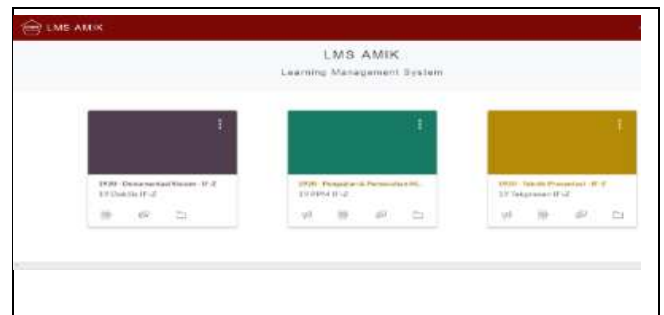
Dalam implementasi metode *OAuth/OpenID Connect* seperti *SAML* terbagi kedalam 2 dua jenis utama penyedia *identity provider*, dan *service provider*.



Gambar 11. Tampilan login pada penerapan OpenID Connect

Aplikasi info dan lms bekerja dengan mengirimkan informasi tentang pengguna, *login*, dan atribut antara *Identity provider* dan *Service provider*. Dalam *OpenID Connect* *Identity provider* memberikan *ID Token* dan/atau *Access Token*. *token* ter-enkripsi menggunakan skema *public/private key*. Setiap pengguna masuk sekali ke aplikasi dengan *WSO2 IS*, dan kemudian *WSO2 IS* dapat meneruskan atribut ke aplikasi ketika pengguna mencoba mengakses layanan tersebut. aplikasi meminta otorisasi dan otentikasi dari *WSO2 IS*. Karena kedua sistem tersebut menggunakan bahasa yang sama *OpenID*, . Kedua ujung harus memiliki konfigurasi *ID Token* dan/atau *Access Token* yang tepat agar otentikasi *OpenID Connect* berfungsi dengan baik.

Jika *username* dan *password* yang dimasukkan sudah benar maka, sistem akan *men-direct* kembali dengan membawa pesan ke sistem aplikasi lms. Dan aplikasi lms akan memverifikasi pesan tersebut dan memberikan akses masuk jika benar.



Gambar 12. Tampilan aplikasi pada penerapan OpenID Connect

IV. Pengujian

Pada tahap ini menjelaskan tentang hasil pengujian pada sistem yang telah dibuat.

Tabel 1. Pengujian Login pada aplikasi info SAML

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login. Memasukan Username : admin. Password : admin. Klik tombol Login.	Aplikasi mengirim data ke WSO2 IS. Berdasarkan data WSO2 IS memunculkan halaman Form Login. Setelah sukses maka akan memunculkan halaman utama.	Dapat masuk ke halaman Login serta Dapat masuk ke halaman utama aplikasi info	[x] diterima [] ditolak
Kasus dan Hasil Uji (Data Salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login. Memasukan Username : admin. Password : admin123. Klik tombol Login.	Tidak dapat login dan memunculkan pesan error	Memberikan pesan error	[x] diterima [] ditolak

Tabel 2. Pengujian Login pada aplikasi lms SAML

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login. Memasukan Username : admin. Password : admin. Klik tombol Login.	Aplikasi mengirim data ke WSO2 IS. Berdasarkan data WSO2 IS memunculkan halaman Form Login.	Dapat masuk ke halaman Login serta Dapat masuk ke halaman utama aplikasi lms	[x] diterima [] ditolak

	Setelah sukses maka akan memunculkan halaman utama.		
Kasus dan Hasil Uji (Data Salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login. Memasukan Username : admin. Password : admin123. Klik tombol Login.	Tidak dapat login dan memunculkan pesan error	Memberikan pesan error	[x] diterima [] ditolak

Tabel 3. Pengujian Single Sign On pada SAML

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login pada aplikasi info. Memasukan Username : admin. Password : admin. Klik tombol Login. Klik tombol login pada aplikasi lms	Aplikasi info mengirim data ke WSO2 IS. Berdasarkan data WSO2 IS memunculkan halaman Form Login. Setelah sukses maka akan memunculkan halaman utama aplikasi info. Masuk ke halaman aplikasi lms tanpa harus Login kembali	Dapat masuk ke halaman Login serta Dapat masuk ke halaman utama aplikasi info Dapat masuk ke halaman utama aplikasi lms tanpa harus Login Kembali	[x] diterima [] ditolak
Kasus dan Hasil Uji (Data Salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Mengakses langsung halaman utama tanpa Login di salah satu aplikasi	Tidak dapat menampilkan halaman utama	Halaman utama tidak dapat diakses.	[x] diterima [] ditolak

Tabel 4. Pengujian Single Sign Out pada SAML

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol Logout pada	Aplikasi info mengirim data ke WSO2 IS.	Masuk ke halaman Login lms dan info	[x] diterima [] ditolak

aplikasi info.	Berdasarkan data WSO2 IS memunculkan halaman Login. Aplikasi lms memunculkan halaman Login juga		
----------------	---	--	--

Tabel 5. Pengujian Login pada aplikasi info OPENID

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login. Memasukan Username : admin. Password : admin. Klik tombol Login.	Aplikasi mengirim data ke WSO2 IS. Berdasarkan data WSO2 IS memunculkan halaman Form Login. Setelah sukses maka akan memunculkan halaman utama.	Dapat masuk ke halaman Login serta Dapat masuk ke halaman utama aplikasi info	[x] diterima [] ditolak
Kasus dan Hasil Uji (Data Salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login. Memasukan Username : admin. Password : admin123. Klik tombol Login.	Tidak dapat login dan memunculkan pesan error	Memberikan pesan error	[x] diterima [] ditolak

Tabel 6.. Pengujian Login pada aplikasi lms OPENID

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login. Memasukan Username : admin. Password : admin. Klik tombol Login.	Aplikasi mengirim data ke WSO2 IS. Berdasarkan data WSO2 IS memunculkan halaman Form Login. Setelah sukses maka akan memunculkan halaman utama.	Dapat masuk ke halaman Login serta Dapat masuk ke halaman utama aplikasi lms	[x] diterima [] ditolak
Kasus dan Hasil Uji (Data Salah)			

Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login. Memasukan Username : admin. Password : admin123. Klik tombol Login.	Tidak dapat login dan memunculkan pesan error	Memberikan pesan error	[x] diterima [] ditolak

Tabel 7. Pengujian Single Sign On pada OPENID

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login pada aplikasi info. Memasukan Username : admin. Password : admin. Klik tombol Login.	Aplikasi info mengirim data ke WSO2 IS. Berdasarkan data WSO2 IS memunculkan halaman Form Login. Setelah sukses maka akan memunculkan halaman utama aplikasi info. Masuk ke halaman aplikasi lms tanpa harus Login kembali	Dapat masuk ke halaman Login serta Dapat masuk ke halaman utama aplikasi info Dapat masuk ke halaman utama aplikasi lms tanpa harus Login Kembali	[x] diterima [] ditolak
Kasus dan Hasil Uji (Data Salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Mengakses langsung halaman utama tanpa Login di salah satu aplikasi	Tidak dapat menampilkan halaman utama	Halaman utama tidak dapat diakses.	[x] diterima [] ditolak

Tabel 8. Pengujian Single Sign Out pada OPENID

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol Logout pada aplikasi info.	Aplikasi info mengirim data ke WSO2 IS. Berdasarkan data WSO2 IS memunculkan halaman Login. Aplikasi lms memunculkan halaman Login juga	Masuk ke halaman Login lms dan info	[x] diterima [] ditolak

Tabel 9. Pengujian Single Sign On pada Mobile

Kasus dan Hasil Uji (Data Normal)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Klik tombol login pada aplikasi info. Memasukan Username : admin. Password : admin. Klik tombol Login. Klik tombol login pada aplikasi lms	Aplikasi info mengirim data ke WSO2 IS. Berdasarkan data WSO2 IS memunculkan halaman Form Login. Setelah sukses maka akan memunculkan halaman utama aplikasi info. Masuk ke halaman aplikasi lms tanpa harus Login kembali	Dapat masuk ke halaman Login serta Dapat masuk ke halaman utama aplikasi info Dapat masuk ke halaman utama aplikasi lms tanpa harus Login Kembali	[x] diterima [] ditolak

Kasus dan Hasil Uji (Data Salah)			
Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Mengakses langsung halaman utama tanpa Login di salah satu aplikasi	Tidak dapat menampilkan halaman utama	Halaman utama tidak dapat diakses.	[x] diterima [] ditolak

V. Kesimpulan

Berdasarkan implementasi dan hasil uji coba dapat diambil beberapa kesimpulan, yaitu:

1. Sistem mengizinkan pengguna agar dapat mengakses seluruh sumber daya dalam jaringan hanya dengan menggunakan satu credential saja.
2. Sistem dapat melakukan pemrosesan data pengguna (penambahan, pengurangan, perubahan) cukup hanya melakukan sekali pemrosesan.
3. Sistem dapat diakses melalui aplikasi Desktop dan Mobile.
4. Sistem melakukan efisiensi dalam penggunaan database karena menyimpan banyak data realtif dalam 1 database.

REFERENSI

- [1] "Authenticationworld.com," 23 05 2014. [Online]. Available: <https://archive.is/20140523114521/http://www.authenticationworld.com/Single-Sign-On-Authentication/SSOandLDAP.html>.
- [2] A. a. C.J.Mitchel, "Impostor: A Single Sign-On System for," 2004.

- [3] WSO2, "WSO2 Identity Server," [Online]. Available: <https://wso2.com/identity-and-access-management/>.
- [4] J. Hughes, "Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0," 2005. [Online].
- [5] A. Parecki, in *OAuth 2.0 Simplified: A Guide to Building OAuth 2.0 Servers*, 2018.
- [6] G. Blokdyk, "SAML and OpenID Connect A Complete Guide," 2018.
- [7] <https://sis.binus.ac.id/2018/03/09/knowning-agile-development-methodologies-kanban/>

Lampiran

Kode	Penjelasan
SAML	Standar XML yang memungkinkan domain web aman untuk bertukar data otorisasi dan autentikasi pengguna
OPENID	login pengguna biasanya merupakan alamat HTTP sumber daya yang bertanggung jawab untuk otentikasi.
SSO	Single Sign On