bidang
TEKNIK

SINGLE SIGN ON (SSO) MENGGUNAKAN STANDAR SAML PADA SISTEM INFORMASI UNIKOM

TARYANA SURYANA, AHMAD AMARULLAH
Program Studi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer
Universitas Komputer Indonesia

Perusahaan besar yang memiliki sistem yang berbeda baik dari sisi Aplikasi maupun sistem operasi, yang mengharuskan setiap user untuk login ke setiap aplikasi yang berbeda secara berulang. Dengan adanya SSO ini, pengguna hanya cukup mengingat satu user dan satu password saja, namun berlaku secara universal diseluruh aplikasi perusahaan, sehingga dengan cara ini bisa lebih memudahkan aplikasi yang akan diintegrasikan tanpa harus membuat semacam user validasi tersendiri,

Keywords **:** *Single Sign On, Login*

PENDAHULUAN

1. Latar Belakang Masalah

Unikom memiliki banyak aplikasi yang saat ini digunakan untuk berbagai macam keperluan, setiap aplikasi memiliki username dan password yang berbeda untuk dapat masuk ke masing-masing aplikasi. Permasalahan yang sering terjadi adalah Pengguna Aplikasi lupa dengan username dan password tersebut. Untuk mengatasi permasalahan tersebut maka pada menelitian ini akan dibahas bagaimana membangun aplikasi SSO untuk diterapkan pada Sistem Informasi Unikom dengan Menggunakan Standar *Security Assertion Markup Language (SAML)*

2. Pembahasan

SSO merupakan kepanjangan dari Single Sign On adalah teknologi yang mengizinkan pengguna dalam jaringan ataupun system dapat mengakses sumber daya dalam jaringan atau sistem hanya dengan menggunakan satu akun pengguna saja.

SSO Memiliki 2 bagian yaitu *Single Sign On* (login satu aplikasi, maka aplikasi lain yang didefinisikan ikut dalam SSO otomatis akan bisa diakses) dan *Single Sign Out* (log out di satu aplikasi, maka semua aplikasi yang didefinisikan ikut dalam SSO akan ikut log-out secara otomatis.

Selain mendatangkan manfaat, SSO juga dapat mendatangkan bencana yaitu kelemahan dari teknologi SSO adalah rentan sekali terhadap penyerangan sistem, hanya dengan satu account saja diketahui, maka dimungkinkan untuk bisa masuk keseluruh data-data di organisasi maupun divisi yang berbeda

Dari cara pandang seperti ini, beberapa pengamat memperkirakan bahwa penggunaan SSO dapat menghemat biaya untuk memelihara password yang rumit yang dapat mencapai ratusan dolar setiap

pengguna tiap tahun. Tetapi, implementasi SSO dalam sebuah jaringan yang heterogen adalah rumit, sehingga banyak administrator jaringan kurang begitu giat dalam mengimplementasikannya

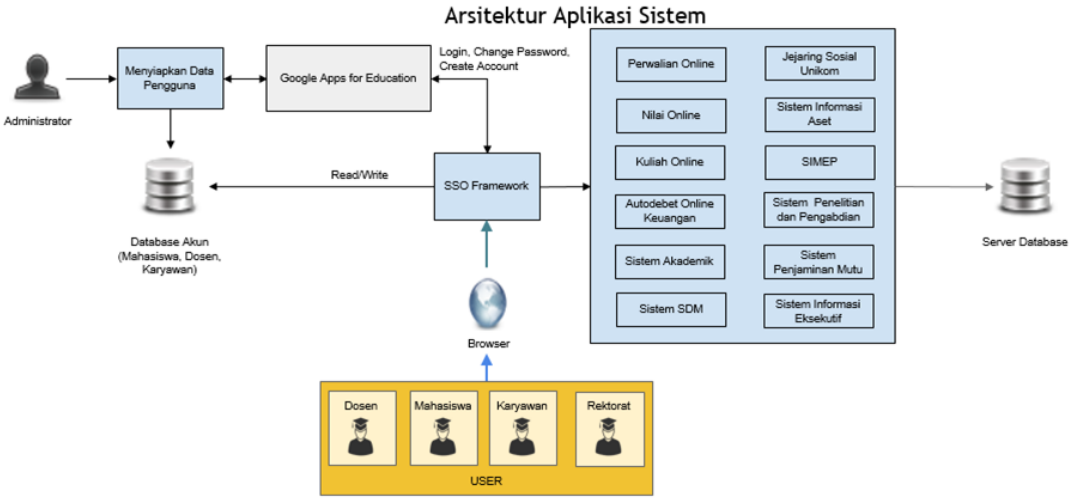
Unikom saat ini telah bekerja sama dengan *Google Apps For Education GAFE* untuk penggunaan aplikasi-aplikasi yang teintegrasi dalam layanan Google Apps, Untuk dapat masuk kedalam Google Apps tersebut diperlukan Username dan Password.

Dengan menggunakan Username dan Password yang didaftarkan di Server GAFE maka setiap user selain dapat menggunakan Aplikasi yang disediakan oleh Google, juga dapat mengakses Sistem Informasi yang ada Unikom.

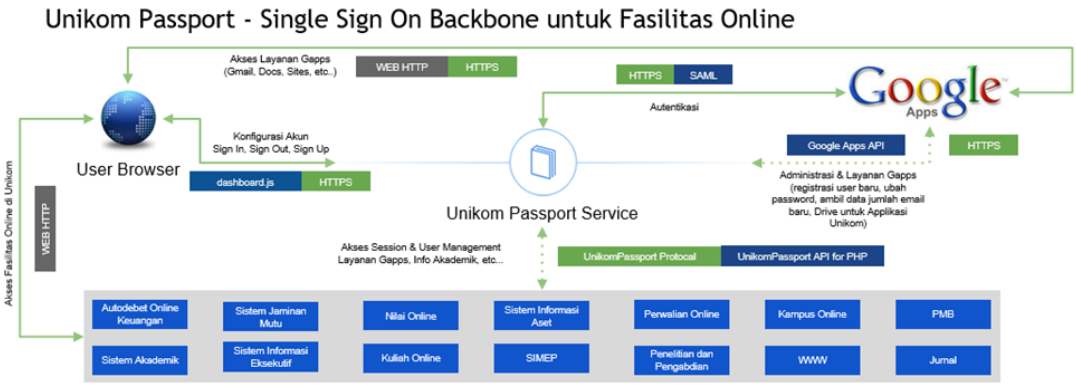
Google telah menyediakan API SSO *berbasis Security Assertion Markup Language* (SAML) yang dapat digunakan untuk diintegrasikan ke dalam *Lightweight Directory Access Protocol* (LDAP).

3. Rencana Pengembangan

Saat ini Unikom memiliki banyak sekali system ataupun aplikasi yang digunakan dalam menunjang proses belajar mengajar, baik yang berbasis web, ataupun yang masih berbasis desktop. Untuk aplikasi yang berbasis Web, dapat diakses dari mana saja melalui Internet baik untuk yang menggunakan Komputer maupun pengguna perangkat mobile seperti Smartphone, sedangkan untuk beberapa aplikasi yang masih berbasis desktop, system hanya bisa diakses dari terminal yang sudah di sediakan.



Gambar 1. Design Arsitektur Aplikasi



Gambar 2. Backbone SSO Aplikasi Online

4. Penjelasan Mengenai Unikom Passport

a. Client Transfer terenkripsi dengan SSL/ TLS pada **Protokol HTTPS**.
b. Data-data sensitif seperti Username dan Password harus dilakukan enkripsi lapis kedua (Second Layer Encryption) Mengunakan **ASecure Library** (dikembangkan oleh Unikom Center menggunakan **Algoritma RSA**) dengan Public dan Private Key yang berbeda untuk setiap session **minimal 1024bit. Key untuk pengiriman data di-generate pada Server (PHP), Key untuk penerimaan data di-generate pada Browser (Javascript).
c. Koneksi antara Client Apps (*Nilai online, Perwalian, Kuliah Online, dll*) dengan Unikom Passport dilakukan pada **Unikom Passport Protocol** dan selalu dalam keadaan terenkripsi dengan OpenSSL, dimana setiap Client memiliki Public Key yang berbeda-beda dan Akses Permission yang berbeda-beda sesuai dengan kebutuhan.
d. Client Apps yang berbasis Web harus menyertakan **Unikom Passport Dashboard** pada file HTML/PHP agar pengguna dapat melakukan Sign In dan melakukan kegiatan-kegiatan yang berhubungan dengan Akun.
e. Client Apps tidak perlu (tidak boleh) membuat formulir untuk melakukan Login/Pendaftaran dengan User Management Sendiri. Client Apps dapat secara langsung mengetahui status pengguna yang mengakses halaman Web dengan melakukan komunikasi pada **Unikom Passport Protocol** *(Atau menggunakan **Unikom Passport API for PHP**).*

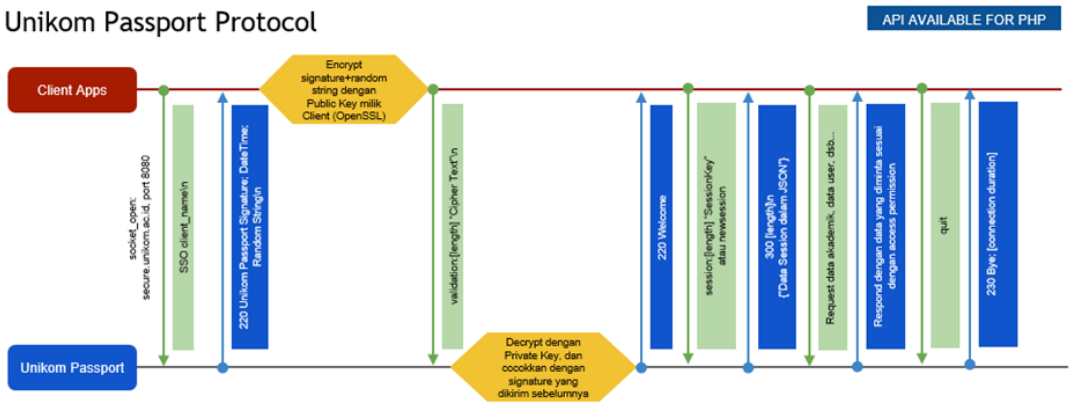
5. Modul Unikom Passports

Unikom Passport terdiri dari beberapa Modul utama yang memiliki fungsi yang berbeda:

a. **Unikom Passport Protocol** - Modul ini digunakan untuk menerima dan memproses Request dari Client Apps secara backend (Server to Server) baik itu berupa status Session, Data user yang sedang login, Query data user, Akses Notifikasi, Realtime Messaging, Encrypt & Decrypt, Query data Akademik, dsb. Aplikasi hanya dapat meminta Request pada perintah yang diizinkan pada Access Permission.
b. **Unikom Passport Dashboard** - Modul layanan tatap muka berupa Top Bar yang disisipkan pada setiap halaman web (Client Apps) yang berfungsi untuk memberikan user akses terhadap akun miliknya, termasuk form Sign In, pendaftaran, lupa password, notofikasi, dsb.

Dengan Dashboard ini, semua layanan online di Unikom memiliki fasilitas Akun yang seragam.

c. **Unikom Passport API for PHP** - PHP Class Based Client API untuk digunakan pada Client Apps yang ingin mengakses Unikom Passport Protocol tanpa harus berurusan dengan metode Transfer Data pada Protokol tersebut.
d. **Unikom Passport Secure Proxy** - Protokol HTTPS yang dapat digunakan bersama, Client Apps dapat memiliki URL https untuk urusan-urusan yang riskan, misalnya formulir PMB dapat diakses melalui https://secure.unikom.ac.id/pmb/onlinereg/
e. **Unikom Passport SAML Service** - Modul ini digunakan untuk melakukan Autentikasi antara Akun Google Apps.



Gambar 3. Protokol Unikom Passport

6. Spesifikasi Unikom Passport Protocol

Berikut akan dijelaskan mengenai beberapa Protocol yang disediakan didalam Unikom Passport

Unikom Passport Protocol - Spesifikasi (Communication Style)

- Port 8080 - Server secure.unikom.ac.id
- Setiap data untuk sebuah request harus dilakukan enkripsi dengan public key yang dimiliki Client Apps (gunakan openssl_public_encrypt)
- Setiap data yang dikirimkan Unikom Passport akan terenkripsi dengan private key, dan dapat di decrypt dengan menggunakan public key milik Client Apps (gunakan openssl_public_decrypt)
- Tipe koneksi: Stream request and respond.
- Setelah melakukan request harus menunggu respond dari Unikom Passport sebelum melakukan request lainnya.

- **Format pengiriman request tanpa data:**
  C: [command]\n
  S: [code] [message]\n
  atau
  S: 300\n
- **Format pengiriman request dengan data:**
  C: [command]:[data_length] [Encrypted Data]\n
  S: [code] [message]\n
  atau
  S: 300 [data_length]\n[Encrypted Data]\n

Unikom Passport Protocol - Spesifikasi (SESSION Steps)

- **Session ID Avaiable:**
  `C: session:[1024] [encrypted sessionid]\n`
  Session ID Unavaiable:
  `C: newsession\n`
- **Session Invalid:**
  `S: 501 Session ID Not Valid\n`
  Cannot Create Session:
  `S: 550 Internal Server Error\n`
- **Session Valid:**
  `S: 300 [dala_length]\n[session_data]\n`
- **`C: Client, S: Server`**

- **sessionid** akan dikirimkan server pada session_data.
- Bila Session Invalid, Client Apps dapat mencoba untuk meminta request **newsession**.
- Client harus menyimpan session_data yang dikirimkan Server untuk digunakan pada request selanjutnya.
- Dalam **UnikomPassport API** for PHP, API akan secara otomatis melakukan request session atau newsession dan akan secara otomatis menyimpan sessionid pada COOKIE. Client Apps hanya perlu memanggil method init():

```
$SSO->init();
```

Unikom Passport Protocol - Spesifikasi (Validation Steps)

- `C: SSO client_name\n`
- **Client Unvaiable:**
  `S: 504 Access Denied, No Client ID\n`
  Client Available:
  `S: 200 Unikom Passport; Version; Date; Random\n`
- `C: validate:[1024] [encrypted server signature]\n`
- **Not Valid:**
  `S: 504 Access Denied. Validation Error\n`
  Valid:
  `S: 200 Welcome\n`
  `C: Client, S: Server`

- **[encrypted server signature]:** Data berupa hasil sha1 dari Signature yang dikirimkan server (Unikom Passport; Version ...).
- [1024] Data Length dalam Bytes
- Data harus dalam format JSON. kemudian dilakukan enkripsi dengan menggunakan **openssl_public_encrypt**.
- Dalam **UnikomPassport API** for PHP, Client Apps, hanya perlu menambahkan kode berikut:

```
$SSO = new UnikomPassport(
   "client_name", $publicKey
);
```

Unikom Passport Protocol - Spesifikasi (SESSION Steps)

- **Session ID Avaiable:**
  `C: session:[1024] [encrypted sessionid]\n`
  Session ID Unavaiable:
  `C: newsession\n`
- **Session Invalid:**
  `S: 501 Session ID Not Valid\n`
  Cannot Create Session:
  `S: 550 Internal Server Error\n`
- **Session Valid:**
  `S: 300 [dala_length]\n[session_data]\n`
- **`C: Client, S: Server`**

- **sessionid** akan dikirimkan server pada session_data.
- Bila Session Invalid, Client Apps dapat mencoba untuk meminta request **newsession**.
- Client harus menyimpan session_data yang dikirimkan Server untuk digunakan pada request selanjutnya.
- Dalam **UnikomPassport API** for PHP, API akan secara otomatis melakukan request session atau newsession dan akan secara otomatis menyimpan sessionid pada COOKIE. Client Apps hanya perlu memanggil method init():

```
$SSO->init();
```

UnikomPassport API for PHP

- **PHP Class Based API**
- Proses validasi dan session dilakukan secara internal di dalam API.
- Transfer data telah disusun dan dilakukan secara internal di dalam API.
- Client hanya perlu memanggil command yang diinginkan.
- Enkripsi data pada protokol akan dilakukan secara internal di dalam API, Client hanya perlu memberikan PublicKey dan Client_Name pada API.
- API Akan otomatis membuat PHP Session. Jadi Client tidak perlu melakukan session_start();.

Contoh Inisialisasi:

```
include_once "UnikomPassportAPI.php";
$KEY = file_get_content("key.pem");
$compress=true;
$server_up="10.10.0.1";
$SSO = new UnikomPassport(
    "kuliahonline", $KEY, $compress, $server_up
);
if (!$SSO->init()){
    echo "GAGAL!!!".($SSO->printError()); exit();
}
if ($SSO->isLogin()){
    echo "Anda Login dengan: ".$SSO->myUsername();
}
```

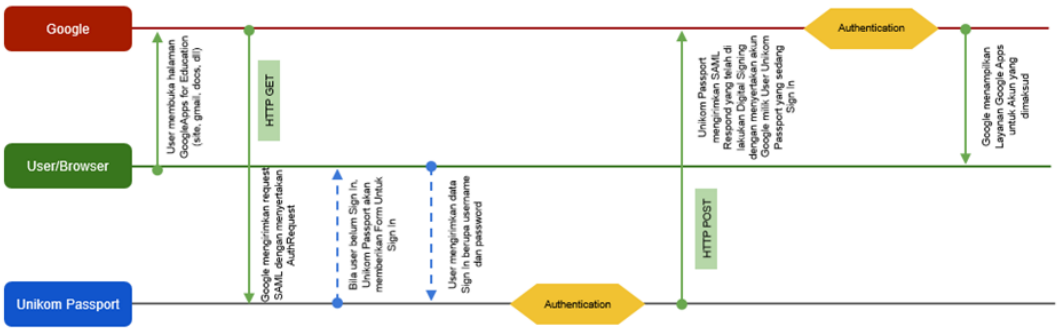
UnikomPassport API for PHP - Methods ($SSO->method())

- **isLogin()** - Apakah user telah melakukan Login?
- **myUsername()** - Username untuk user yang telah login.
- **myDisplayName()** - Nama Tampilan.
- **myType()** - Tipe user (mahasiswa, alumni, dosen, karyawan, public).
- **myGoogleUsername()** - Username/Email GoogleApps.
- **isHaveGoogle()** - Untuk tipe selain public bernilai true, bila GoogleApps telah diaktifkan untuk user tersebut.
- **myUid()** - User ID berupa Integer.
- **myAid()** - ID Akademik untuk user yang dimaksud. Bila tipe mahasiswa dan alumni akan berisi NIM, bila dosen dan karyawan akan berisi nomor absensi. Untuk public=false.
- **getUser("username")** - Meminta data user yang dimaksud
- **getUser("username1","username2",...)** - Meminta data user-user yang dimaksud.
- **encrypt("Data")** - Encrypt data yang dimaksud
- **decrypt("Cipher")** - Decrypt cipher yang dimaksud
- **myPhotoUrl()** - URL untuk foto user yang sedang login.
- *Method lainnya akan dipaparkan pada User Manual.*

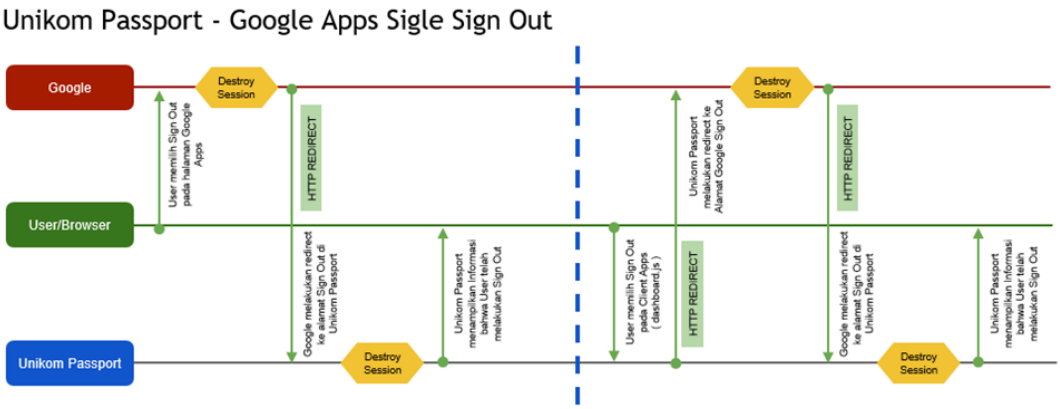
**** Method Name is subject to change*

7. Arsitektur Unikom Passport Sign In dan Sign Out

Unikom Passport - Google Apps SAML Authentication



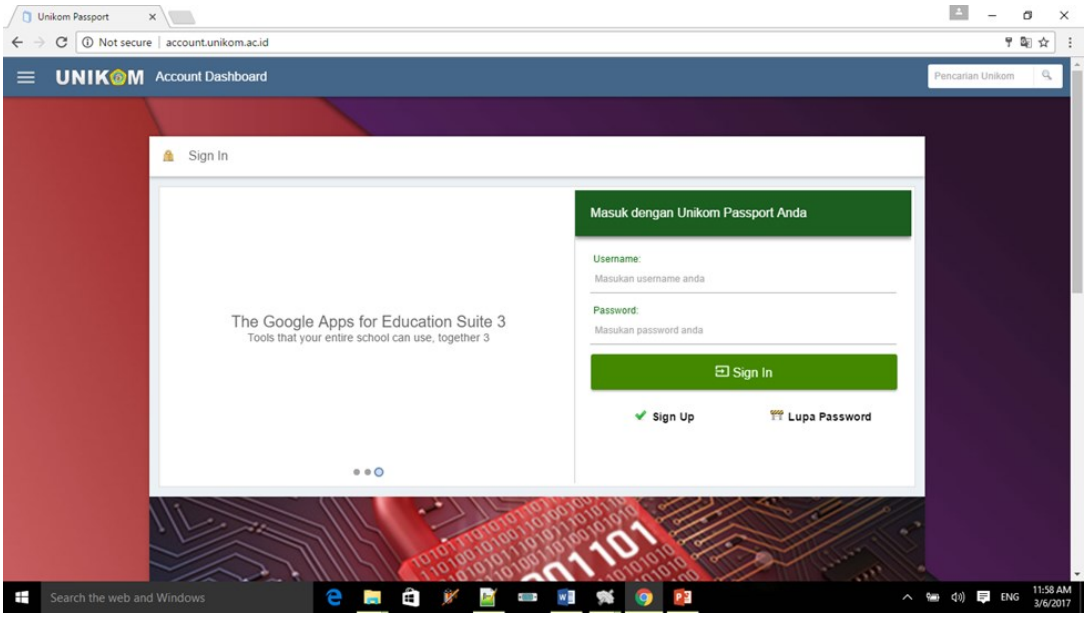
Gambar 4. Unikom Passport - Google Apps SAML Authentication



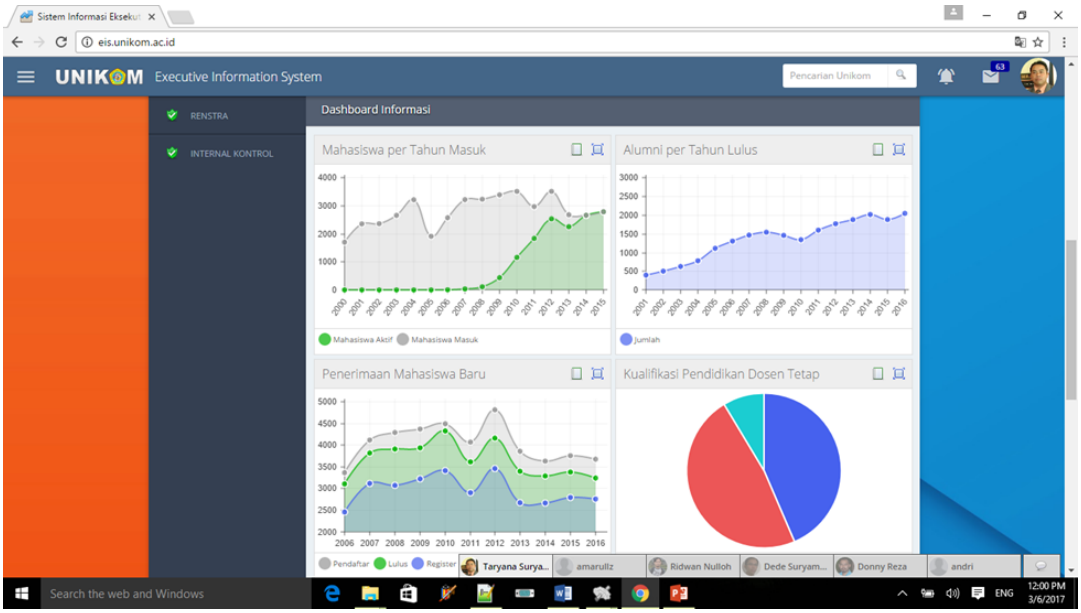
Gambar 5. Unikom Passport—Google Apps Sigle Sign Out

8. Implementasi Sistem

Sistem saat ini sedang dibangun dan terus dikembangkan untuk memenuhi segala kebutuhan informasi dari berbagai bidang terkait yang ada dilingkungan Civitas Akademika Universitas Komputer Indonesia.



Gambar 6. Halaman *Account Dashboard* Unikom



Gambar 7. Halaman Dashboard Executive Information System

DAFTAR PUSTAKA

https://support.google.com/a/answer/6087519?hl=en

https://developers.onelogin.com/saml

https://robinpowered.com/blog/how-to-set-up-saml-with-google-apps/