



BUPATI SUKOHARJO
PROVINSI JAWA TENGAH

KEPUTUSAN BUPATI SUKOHARJO
NOMOR : 500.12.6/328 TAHUN 2024

TENTANG

STANDAR OPERASIONAL PROSEDUR PERMOHONAN INTEGRASI SISTEM
INFORMASI DAN DOKUMEN TEKNIS *SINGLE SIGN ON*

BUPATI SUKOHARJO,

- Menimbang : a. bahwa untuk melaksanakan ketentuan Pasal 45 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menyusun Standar Operasional Prosedur Permohonan Integrasi Sistem Informasi dan Dokumen Teknis *Single Sign On*;
- b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menyusun Standar Operasional Prosedur Permohonan Integrasi Sistem Informasi dan Dokumen Teknis *Single Sign On*;
- d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, dan huruf b, perlu menetapkan dalam Keputusan Bupati;
- Mengingat : 1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten dalam Lingkungan Propinsi Djawa Tengah sebagaimana telah diubah dengan Undang-Undang Nomor 9 Tahun 1965 tentang Pembentukan Daerah Tingkat II Batang dengan mengubah Undang-Undang No. 13 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten dalam Lingkungan Propinsi Jawa Tengah (Lembaran Negara Tahun 1965 Nomor 52, Tambahan Lembaran Negara Nomor 2757);
2. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

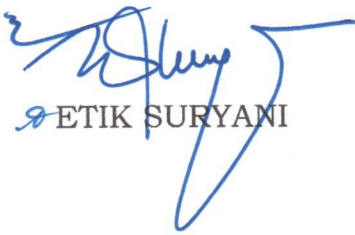
4. Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 159);
5. Peraturan Daerah Kabupaten Sukoharjo Nomor 2 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Daerah Kabupaten Sukoharjo Tahun 2022 Nomor 2, Tambahan Lembaran Daerah Kabupaten Sukoharjo Nomor 303);
6. Peraturan Bupati Sukoharjo Nomor 59 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik (Lembaran Daerah Kabupaten Sukoharjo Tahun 2022 Nomor 59);
7. Peraturan Bupati Sukoharjo Nomor 34 Tahun 2022 tentang Peta Rencana Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Sukoharjo Tahun 2022 Nomor 34) sebagaimana telah diubah dengan Peraturan Bupati Nomor 24 Tahun 2023 tentang Perubahan Atas Peraturan Bupati Nomor 34 Tahun 2022 tentang Peta Rencana Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Sukoharjo Tahun 2023 Nomor 24);

MEMUTUSKAN:

- Menetapkan :
KESATU : Standar Operasional Prosedur Permohonan Integrasi Sistem Informasi dan Dokumen Teknis *Single Sign On*, sebagaimana tercantum dalam Lampiran I dan Lampiran II Keputusan ini.
- KEDUA : Keputusan Bupati ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Sukoharjo
pada tanggal 10 Juni 2024

♣ BUPATI SUKOHARJO, ♣


♣ ETIK SURYANI

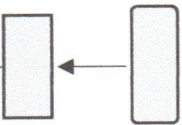
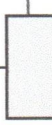
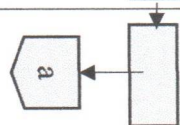
TEMBUSAN : Keputusan ini dikirim
kepada Yth.:

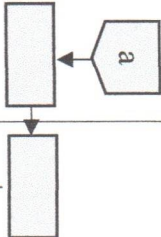
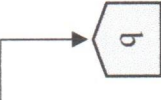
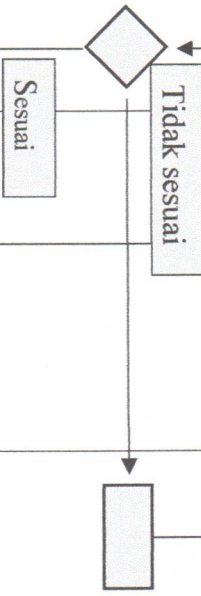
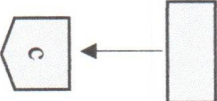
1. Ketua Dewan Perwakilan Rakyat Daerah Kabupaten Sukoharjo;
2. Sekretaris Daerah Kabupaten Sukoharjo di Sukoharjo;
3. Asisten Administrasi Umum Sekretaris Daerah Kabupaten Sukoharjo di Sukoharjo;
4. Kepala Badan/Dinas/Bagian di Lingkungan Pemerintah Kabupaten Sukoharjo;

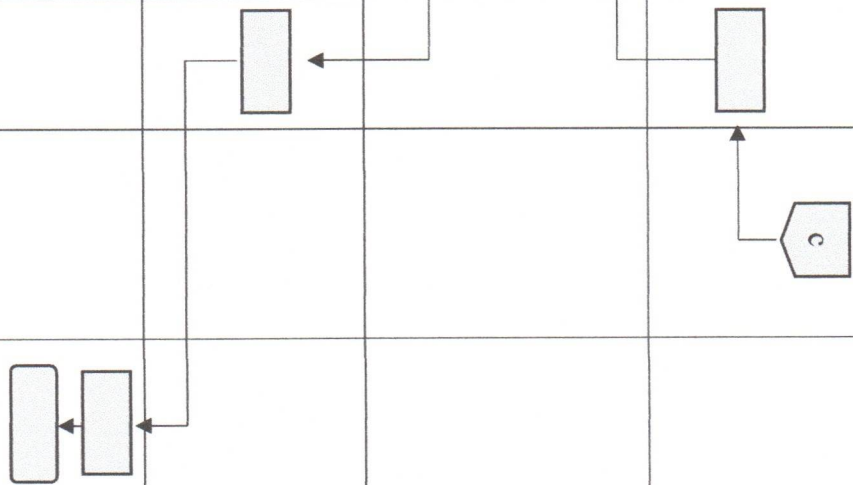
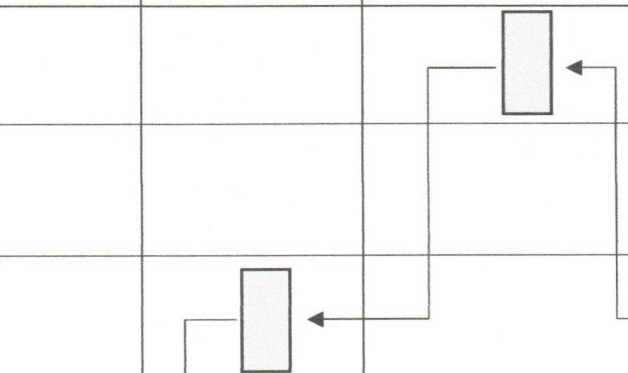
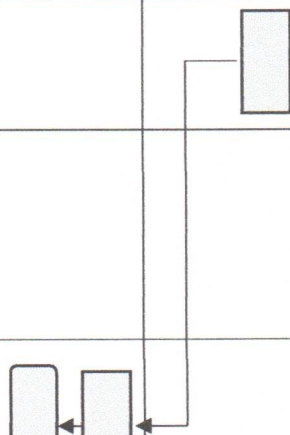
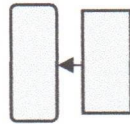
5. Camat di Lingkungan Pemerintah
Kabupaten Sukoharjo;

Lampiran I : Keputusan Bupati Sukoharjo
Nomor : 500.12.6 / 328 THAN 2024
Tanggal : 10 Juni 2024

STANDARD OPERATIONAL PROCEDURE PERMOHONAN INTEGRASI SISTEM APLIKASI

No	Kegiatan	Pelaksana					Mutu Baku			Keterangan	
		Kadis Kominfo	Kabid AI	Ketua Tim Integrasi	Tim DEV	Bidang Persandian dan Statistik	OPD Pemohon	Kelengkapan	Waktu		Output
1	OPD Pemohon menyusun dokumen kelengkapan terkait permohonan integrasi Sistem Aplikasi yang akan diintegrasikan							Diantaranya dapat berupa : 1. Dokumen Kebutuhan/ Kelengkapan integrasi sistem terkait	± 3 hari	Dokumen Kelengkapan Integrasi Sistem	
2	OPD Pemohon mengajukan permohonan integrasi Sistem Aplikasi secara tertulis kepada Kepala Dinas Komunikasi dan Informatika Kabupaten Sukoharjo dilengkapi dengan dokumen kelengkapan integrasi sistem							Diantaranya dapat berupa : 1. Surat Permohonan 2. Dokumen Kelengkapan integrasi sistem	±1-2 jam	Surat Permohonan dengan melampirkan Dokumen Kebutuhan/ Kelengkapan integrasi sistem Aplikasi	
3	Kabid Aplikasi Informatika dan Ketua Tim Integrasi menindaklanjuti disposisi							Disposisi	±1-2 jam	Disposisi	

4	Ketua Tim Integrasi menindaklanjuti dengan melakukan diskusi awal terkait proses integrasi sistem aplikasi dengan Tim Developer Aplikasi					Dokumen Kelengkapan Integrasi Sistem	± 1-2 hari	Dokumen hasil pembahasan proses integrasi	
5	Ketua Tim Integrasi menindaklanjuti dengan mengundang unit kerja pemohon untuk pembahasan integrasi sistem					Dokumen Kelengkapan Integrasi Sistem	± 1 hari	Surat Undangan	
6	Jika integrasi sistem sudah disetujui maka akan dilanjutkan ke proses berikutnya, jika tidak disetujui maka Unit Kerja Pemohon akan diinformasikan melalui Surat balasan					Diantaranya dapat berupa : 1. Dokumen integrasi aplikasi 2. API	± 1 hari	Dokumen hasil pembahasan proses integrasi	
7	Bidang Persandian dan Statistik akan melakukan <i>assessment</i> aplikasi yang akan diintegrasikan, Jika terdapat temuan yang perlu ditindaklanjuti oleh OPD Pemohon maka Diskominfo akan menginformasikan melalui Surat, Jika tidak terdapat temuan maka akan dilanjutkan ke tahap berikutnya					Diantaranya dapat berupa : 1. Dokumen integrasi aplikasi 2. API 3. Aplikasi yang akan diintegrasikan	± 2 hari	Dokumen <i>assessment</i>	

8	Tim Developer melakukan tindak lanjut berupa implementasi integrasi sistem yang telah disepakati					Diantaranya dapat berupa : 1. Dokumen hasil assesment 2. Dokumen integrasi sistem (API)	± 14 hari	Aplikasi/ Sistem yang telah terintegrasi	
9	Kepala Dinas Komunikasi dan Informatika Kabupaten Sukoharjo dan Kepala OPD melakukan penandatanganan perjanjian terkait data pada aplikasi					Diantaranya dapat berupa : 1. Dokumen hasil integrasi aplikasi 2. Aplikasi/Sistem yang telah terintegrasi	± 1-2 jam	Draft Berita Acara	
10	Integrasi telah selesai dilakukan dan dilanjutkan dengan System Internal Test (SIT)					Aplikasi	± 1 hari	Berita Acara SIT	
11	SIT telah selesai dilakukan dilanjutkan dengan UAT oleh OPDa Pemohon					Aplikasi	± 2 hari	Berita Acara UAT	

BUPATI SUKOHARJO,

ETIK SURYANI

Lampiran II : Keputusan Bupati Sukoharjo

Nomor : 500.12.6/328 TAJUN

Tanggal : 10 Juni 2024

DOKUMEN TEKNIS *SINGLE SIGN ON*

I. Informasi Umum

Dokumen ini digunakan sebagai panduan teknis penerapan *Single Sign On* User Login pada layanan sistem informasi dan jaringan Wireless di lingkungan Pemerintah Kabupaten Sukoharjo. Dokumen ini bertujuan untuk memberikan langkah-langkah detail dalam mengimplementasikan *Single Sign On*, serta integrasi *Single Sign On* dengan berbagai sistem dan jaringan yang ada di Pemerintah Kabupaten Sukoharjo.

II. Pendahuluan

Sistem *Single Sign On* Kabupaten Sukoharjo adalah sistem yang memungkinkan pengguna untuk mengakses berbagai aplikasi dengan menggunakan satu set kredensial (*username dan password*) yang sama. Protokol yang digunakan adalah menggunakan OAuth 2.0 sebagai autentikasi dan otorisasi. OAuth (kependekan dari "Open Authorization") adalah suatu protokol terbuka yang memungkinkan pengguna untuk berbagi sumber atau mendapatkan akses terbatas ke sumber daya pengguna di server. Proses ini dilakukan dengan memberikan token. Implementasi OAuth 2.0 sebagai klien untuk terkoneksi dengan *Single Sign On* Kabupaten Sukoharjo, memerlukan persyaratan teknis yang spesifik untuk memastikan integrasi yang sukses dan aman.

A. Integrasi *Single Sign On* dengan Protokol OAuth 2.0

1. Persyaratan Sistem

a. Kebutuhan Perangkat Lunak:

- Bahasa Pemrograman: Memilih bahasa pemrograman yang mendukung implementasi OAuth 2.0 seperti Python, Java, JavaScript (Node.js), PHP, atau bahasa lain yang disukai untuk mengembangkan klien OAuth 2.0.
- Framework atau Library OAuth 2.0: Memilih framework atau library OAuth 2.0 yang sesuai untuk mengimplementasikan alur otorisasi OAuth 2.0 secara efektif dengan *Single Sign On* Kabupaten Sukoharjo.

b. Kebutuhan Keamanan:

- HTTPS: Klien OAuth 2.0 harus mendukung komunikasi melalui protokol HTTPS untuk mengamankan pertukaran token OAuth antara klien dan server *Single Sign On* Kabupaten Sukoharjo.
- Penanganan Token: Memastikan bahwa token OAuth (access token, refresh token) disimpan dengan aman dan tidak terekspos secara tidak sengaja.
- Manajemen Kredensial: Klien OAuth 2.0 harus mampu menyimpan dan mengelola kredensial (seperti ID klien dan rahasia klien) dengan cara yang aman sesuai kebijakan *Single Sign On* Kabupaten Sukoharjo.

c. Kebutuhan Fungsional:

- Integrasi dengan API *Single Sign On* Kabupaten Sukoharjo: Klien harus dapat berinteraksi dengan API *Single Sign On* Kabupaten Sukoharjo untuk menginisiasi alur otorisasi OAuth 2.0, termasuk permintaan autentikasi dan pertukaran token.
- Manajemen Akses: Kemampuan untuk mengelola siklus hidup token OAuth 2.0, termasuk pembaruan token akses menggunakan token penyegaran (refresh token) yang sesuai dengan kebijakan *Single Sign On* Kabupaten Sukoharjo.

2. Implementasi dan Pengujian

Untuk mengimplementasikan OAuth 2.0 sebagai klien dengan *Single Sign On* Kabupaten Sukoharjo menggunakan PHP, Anda perlu memilih library atau framework OAuth 2.0 yang mendukung bahasa pemrograman ini. Salah satu pilihan yang umum digunakan adalah '*league/oauth2-client*'. Berikut adalah langkah-langkah implementasi dan contoh source code dalam PHP:

Langkah 1: Instalasi Library OAuth 2.0

Pastikan Anda telah menginstal library *league/oauth2-client* dengan menggunakan Composer:

```
composer require league/oauth2-client
```

Langkah 2: Konfigurasi OAuth 2.0 Client

Konfigurasikan klien OAuth 2.0 untuk berinteraksi dengan SSO Kabupaten Sukoharjo. Anda perlu menentukan beberapa konfigurasi dasar seperti URL otorisasi, token, dan kredensial klien (client ID dan client secret).

```
<?php
require_once __DIR__ . '/vendor/autoload.php';

use League\OAuth2\Client\Provider\GenericProvider;

// Konfigurasi OAuth 2.0 Client
$provider = new GenericProvider([
    'clientId'                => 'your_client_id',
    'clientSecret'            => 'your_client_secret',
    'redirectUri'              => 'https://example.com/callback',
    'urlAuthorize'             =>
    'https://sso.sukoharjokab.go.id/application/o/authorize/',
    'urlAccessToken'          =>
    'https://sso.sukoharjokab.go.id/application/o/token/',
    'urlResourceOwnerDetails' =>
    'https://sso.sukoharjokab.go.id/application/o/userinfo/',
    'scope'                    => ['email openid profile'],
]);

// Contoh URL untuk mendapatkan otorisasi
$authorizationUrl = $provider->getAuthorizationUrl();

// Jika tidak ada access token, arahkan ke URL otorisasi
if (!isset($_GET['code'])) {
    $_SESSION['oauth2state'] = $provider->getState();
    header('Location: ' . $authorizationUrl);
    exit;
} elseif (empty($_GET['state']) || ($_GET['state'] !==
$_SESSION['oauth2state'])) {
    unset($_SESSION['oauth2state']);
    exit('Invalid state');
} else {
    // Mendapatkan access token menggunakan authorization code
    $accessToken = $provider->getAccessToken('authorization_code', [
        'code' => $_GET['code']
    ]);

    // Menampilkan informasi user yang diambil dari SSO
    $resourceOwner = $provider->getResourceOwner($accessToken);
    $user = $resourceOwner->toArray();

    // Tampilkan informasi user
    echo 'Welcome, ' . $user['name'] . '! Your email is ' . $user['email'];
}
?>
```

Langkah 3: Pengujian OAuth 2.0 Client

Untuk menguji klien OAuth 2.0 yang telah diimplementasikan, pastikan untuk melakukan pengujian fungsionalitas berikut:

- **Pengujian Koneksi:** Pastikan aplikasi dapat terhubung ke endpoint OAuth 2.0 *Single Sign On* Kabupaten Sukoharjo dan mengambil token dengan benar.
- **Pengujian Otorisasi:** Pastikan alur otorisasi berfungsi dengan baik, termasuk mendapatkan authorization code dan menukarnya dengan access token.
- **Pengujian Manajemen Akses:** Verifikasi bahwa access token dan refresh token (jika digunakan) dikelola dengan baik oleh klien OAuth 2.0.

3. Penjelasan Bagian-bagian Source Code

a. Pemanggilan Autoload dan Penggunaan Namespace:

```
require_once __DIR__ . '/vendor/autoload.php';  
  
use League\OAuth2\Client\Provider\GenericProvider;
```

- `require_once __DIR__ . '/vendor/autoload.php';`: Memuat Composer autoload untuk mengambil semua kelas dan dependensi yang diperlukan.
- `use ...`: Mendeklarasikan penggunaan namespace dari library OAuth 2.0 client yang akan digunakan (`league/oauth2-client`).

b. Konfigurasi OAuth 2.0 Client:

```
$provider = new GenericProvider([  
    'clientId'           => 'your_client_id',  
    'clientSecret'       => 'your_client_secret',  
    'redirectUri'        => 'https://example.com/callback',  
    'urlAuthorize'       =>  
    'https://sso.sukoharjokab.go.id/application/o/authorize/',  
    'urlAccessToken'     =>  
    'https://sso.sukoharjokab.go.id/application/o/token/',  
    'urlResourceOwnerDetails' =>  
    'https://sso.sukoharjokab.go.id/application/o/userinfo/',  
    'scope'              => ['email openid profile'],  
]);
```

- **GenericProvider:** Objek untuk konfigurasi OAuth 2.0 client menggunakan library `league/oauth2-client`.
- **clientId dan clientSecret:** ID klien dan rahasia klien yang diberikan

oleh *Single Sign On* Kabupaten Sukoharjo untuk mengidentifikasi aplikasi Anda.

- `redirectUri`: URL callback yang telah didaftarkan di *Single Sign On* Kabupaten Sukoharjo untuk menerima authorization code setelah otorisasi berhasil.
- `urlAuthorize`: Endpoint URL untuk memulai proses otorisasi OAuth 2.0 dengan *Single Sign On* Kabupaten Sukoharjo.
- `urlAccessToken`: Endpoint URL untuk memperoleh access token setelah mendapatkan authorization code.
- `urlResourceOwnerDetails`: Endpoint URL untuk memperoleh informasi pemilik sumber daya (biasanya informasi pengguna setelah autentikasi sukses).
- `scopes`: Scope atau ruang lingkup akses yang diperlukan oleh aplikasi, seperti openid dan profile, sesuai dengan kebutuhan aplikasi Anda.

c. Mendapatkan URL Autorisasi

```
$authorizationUrl = $provider->getAuthorizationUrl();
```

- `getAuthorizationUrl()`: Metode dari `GenericProvider` untuk menghasilkan URL untuk memulai proses otorisasi OAuth 2.0.

d. Redirect ke URL Autorisasi Jika Belum Mendapatkan Authorization Code

```
if (!isset($_GET['code'])) {  
    // Simpan state dalam session untuk verifikasi nanti  
    $_SESSION['oauth2state'] = $provider->getState();  
  
    header('Location: ' . $authorizationUrl);  
    exit;  
}
```

- `$_GET['code']`: Parameter yang akan menerima authorization code setelah pengguna berhasil mengotorisasi aplikasi.
- Jika tidak ada authorization code, maka pengguna akan diarahkan ke `$authorizationUrl` untuk memulai proses otorisasi dengan *Single Sign On* Kabupaten Sukoharjo.

e. Verifikasi State dan Mendapatkan Access Token

```
elseif (empty($_GET['state']) || ($_GET['state'] !==
$_SESSION['oauth2state'])) {
    unset($_SESSION['oauth2state']);
    exit('Invalid state');
} else {
    // Mendapatkan access token menggunakan authorization code
    $accessToken = $provider->getAccessToken('authorization_code', [
        'code' => $_GET['code']
    ]);

    // Menampilkan informasi user yang diambil dari SSO Kabupaten
    Sukoharjo
    $resourceOwner = $provider->getResourceOwner($accessToken);
    $user = $resourceOwner->toArray();

    // Tampilkan informasi user
    echo 'Welcome, ' . $user['name'] . '! Your email is ' . $user['email'];
}
```

- Verifikasi state: Memeriksa apakah state yang dikirim kembali sesuai dengan yang disimpan dalam session. Ini mencegah serangan CSRF.
- getAccessToken(): Metode untuk menukar authorization code dengan access token dari *Single Sign On* Kabupaten Sukoharjo.
- getResourceOwner(): Metode untuk memperoleh informasi pemilik sumber daya (misalnya informasi pengguna) dari endpoint urlResourceOwnerDetails.
- echo: Contoh sederhana untuk menampilkan informasi pengguna setelah autentikasi dan pengambilan data berhasil.

4. Informasi Data Pengguna

Array yang dihasilkan dari `$user = $resourceOwner->toArray()`; adalah representasi dari data pengguna yang diperoleh dari *Single Sign On* Kabupaten Sukoharjo setelah proses autentikasi OAuth 2.0 berhasil. Berikut adalah penjelasan untuk setiap elemen dalam array tersebut:

```
Array
(
    [email] => <username>@pns.sukoharjokab.go.id
    [email_verified] => 1
    [name] => <nama lengkap>
    [given_name] => <nama depan>
    [preferred_username] => <username>
    [nickname] => <username>
    [groups] => Array
        (

```



```
[0] => <grup pertama>
[1] => <grup kedua>
)

[nip] => <nip pegawai>
)
```

email: Alamat email pengguna. Dalam contoh ini, <username>@pns.sukoharjokab.go.id adalah alamat email yang terverifikasi.

email_verified: Menunjukkan apakah alamat email pengguna telah diverifikasi atau tidak. Dalam kasus ini, nilainya adalah 1, yang menandakan bahwa alamat email sudah diverifikasi.

name: Nama lengkap atau nama pengguna dari pengguna. Dalam contoh ini, <nama pegawai> adalah nama lengkap dari pengguna.

given_name: Nama depan dari pengguna. Jika informasi lengkap tentang nama pengguna tersedia, ini adalah nama depan dari pengguna.

preferred_username: Nama pengguna yang disukai atau digunakan untuk masuk ke sistem. Dalam contoh ini, <username> adalah nama pengguna yang disukai.

nickname: Nama panggilan atau alias pengguna. Dalam konteks ini, <username> adalah nickname atau nama panggilan pengguna.

groups: Sebuah array yang berisi daftar grup atau peran yang terkait dengan pengguna. Dalam contoh ini, pengguna memiliki dua grup yang terdaftar:

1. <grup pertama>
2. <grup kedua>

nip: Nomor Induk Pegawai (NIP) dari pegawai. Ini adalah identitas pegawai dalam konteks administratif di SSO Kabupaten Sukoharjo.

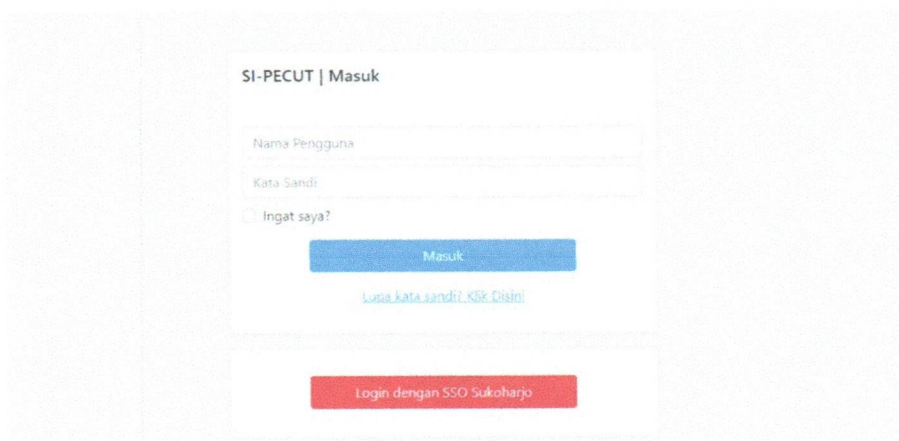
Array ini merupakan struktur data yang disediakan oleh *Single Sign On* Kabupaten Sukoharjo melalui endpoint `urlResourceOwnerDetails` setelah klien OAuth 2.0 berhasil menukar `authorization code` dengan `access token`. Data ini biasanya digunakan untuk mengidentifikasi pengguna dan mengatur akses ke sumber daya atau layanan yang terlindungi. Dalam aplikasi yang menggunakan OAuth 2.0, data ini dapat digunakan untuk menyesuaikan pengalaman pengguna atau memberikan akses yang sesuai dengan peran atau grup yang dimiliki pengguna.

5. Dokumentasi

- Halaman Login *Single Sign On* Pemerintah Kabupaten Sukoharjo



- Halaman Login Sistem Informasi



B. Integrasi *Single Sign On* dengan Jaringan Wireless (WiFi)

1. Pendahuluan

Integrasi *Single Sign On* dengan jaringan wireless (WiFi) bertujuan untuk menyediakan pengalaman pengguna yang aman dalam mengakses jaringan dengan tanpa perlu memasukkan kredensial berulang kali. Skema yang digunakan untuk integrasi *Single Sign On* dengan jaringan wireless berbeda dengan integrasi *Single Sign On* pada layanan sistem informasi, namun untuk data diambil dari sumber yang sama. Implementasi dilakukan dengan mengintegrasikan Wireless WPA2-Enterprise dengan RADIUS Server Pada Windows Active Directory.

Windows Active Directory (AD) adalah layanan direktori yang digunakan oleh sistem operasi Windows untuk menyimpan informasi tentang jaringan dan sumber daya, serta menyediakan mekanisme autentikasi dan otorisasi. AD menggunakan protokol LDAP (Lightweight Directory Access Protocol) untuk memungkinkan administrator mengelola izin pengguna dan mengakses sumber daya jaringan seperti file, printer, dan server. AD juga mendukung Group Policy untuk manajemen konfigurasi terpusat, dan merupakan bagian penting dari infrastruktur keamanan untuk banyak organisasi.

RADIUS Server adalah komponen jaringan yang bertanggung jawab untuk autentikasi, otorisasi, dan akuntansi (AAA) pengguna yang mengakses jaringan atau layanan. Network Policy Server (NPS) adalah implementasi RADIUS Server oleh Microsoft yang digunakan dalam Windows Server.

Berikut adalah cara kerja integrasi AD dengan WPA2 Enterprise:

- a) Server RADIUS: Konfigurasi server RADIUS, seperti Microsoft Network Policy Server (NPS), untuk berfungsi sebagai perantara antara pengguna dan AD.
- b) Autentikasi: Saat pengguna mencoba terhubung ke jaringan Wi-Fi, mereka akan diminta untuk memasukkan kredensial AD mereka.
- c) Verifikasi Kredensial: Server RADIUS akan memverifikasi kredensial tersebut dengan AD.
- d) Akses Jaringan: Jika kredensial valid, server RADIUS akan memberikan kunci enkripsi kepada klien untuk mengakses jaringan.

Dengan demikian, integrasi antara AD dan WPA2 Enterprise memungkinkan manajemen akses jaringan yang aman dan terpusat melalui autentikasi pengguna yang kuat.

WPA2-Enterprise dengan PEAP-MSCHAPv2 adalah metode autentikasi yang umum digunakan untuk jaringan Wi-Fi yang aman, Ini menggabungkan:

- a) WPA2-Enterprise: Standar keamanan yang menyediakan autentikasi pengguna individual melalui server RADIUS.
- b) PEAP (Protected Extensible Authentication Protocol): Protokol yang mengamankan komunikasi antara klien dan server RADIUS dengan membuat tunnel TLS yang terenkripsi.
- c) MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2): Protokol autentikasi yang digunakan dalam tunnel PEAP



untuk memverifikasi kredensial pengguna tanpa mengirimkan kata sandi secara langsung.

Dengan menggunakan PEAP-MSCHAPv2, informasi kredensial pengguna dilindungi selama proses autentikasi, meningkatkan keamanan jaringan Wi-Fi kantor.

2. Persyaratan Sistem

a. Kebutuhan Perangkat Lunak

- Sistem Operasi: Sistem operasi yang digunakan untuk server adalah windows server 2019 desktop experience
- Active Directory: Windows Active Directory (AD) adalah layanan direktori yang digunakan oleh sistem operasi Windows untuk menyimpan informasi tentang jaringan dan sumber daya, serta menyediakan mekanisme autentikasi dan otorisasi.
- Server RADIUS: Server RADIUS ini yang akan memverifikasi kredensial saat pengguna terhubung ke jaringan.
- Sertifikat Digital: Setiap klien (pengguna) memerlukan sertifikat digital yang valid untuk otentikasi. Pada sistem ini kami menggunakan Active Directory Certificate Services.

b. Kebutuhan Perangkat Keras

- Server : Server ini digunakan untuk menjalankan Windows Server, RADIUS Server, Active Directory. Server dapat berupa server fisik maupun virtual machine.
- Router : perangkat inilah yang akan mengatur jaringan pada WPA2-Enterprise, seperti Routing, penerapan VLAN, Pemberian IP pada Client (DHCP).
- Access Point : Gunakan Access Point yang sudah mendukung WPA2-Enterprise. Akan lebih baik jika menggunakan Access Point yang memiliki Controller.

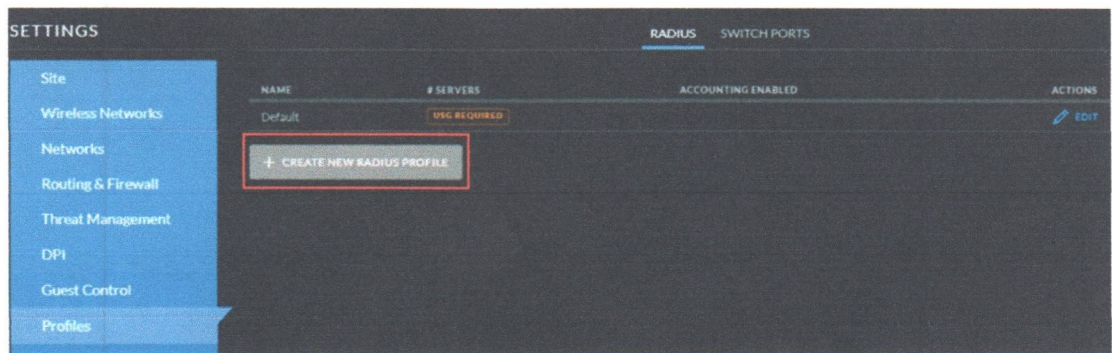
3. Implementasi dan Pengujian

Untuk implementasi WPA2-Enterprise di Kabupaten Sukoharjo, Anda bisa mengikuti langkah-langkah dibawah ini.

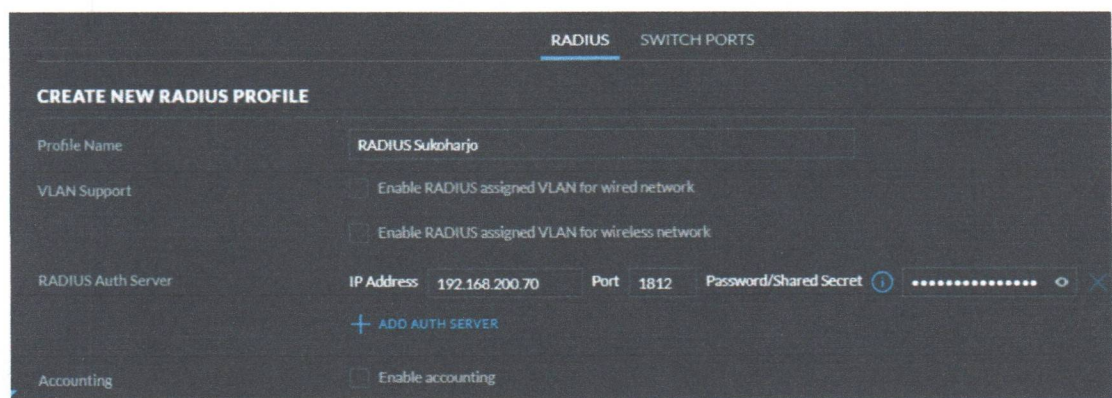
- 1) Buat profile RADIUS Server terlebih dahulu dengan ketentuan sebagai berikut:

- RADIUS Auth Server: 192.168.200.70

- Port: 1812

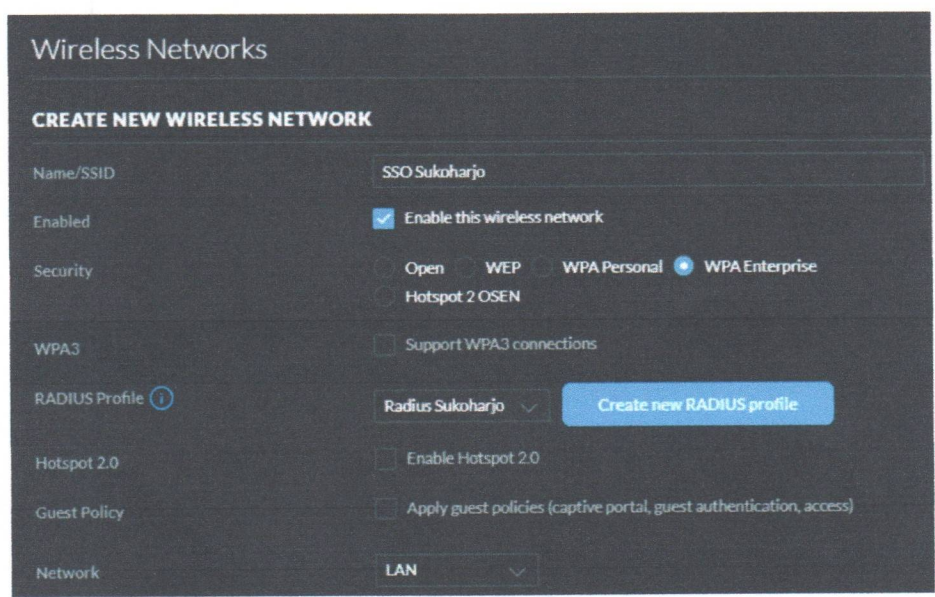


- Shared Secret: sukoharjoradius



2) Membuat SSID Baru dengan ketentuan sebagai berikut:

- SSID: SSO Sukoharjo
- Security: WPA Enterprise
- RADIUS Profile: Radius Sukoharjo
- Network: LAN

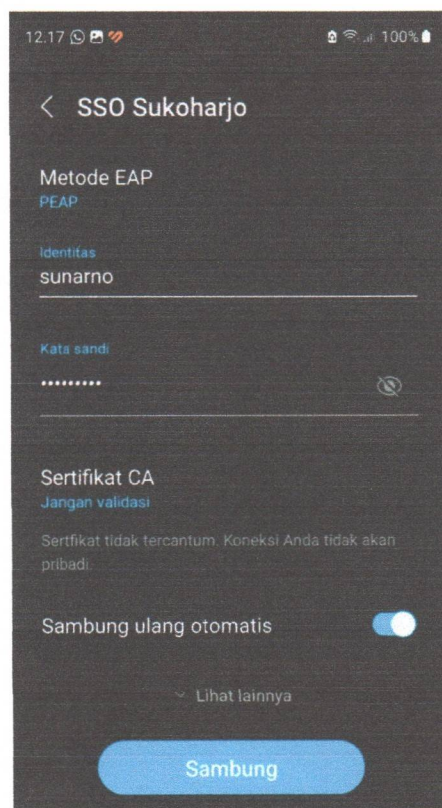


3) Pengujian dengan menggunakan perangkat handphone:

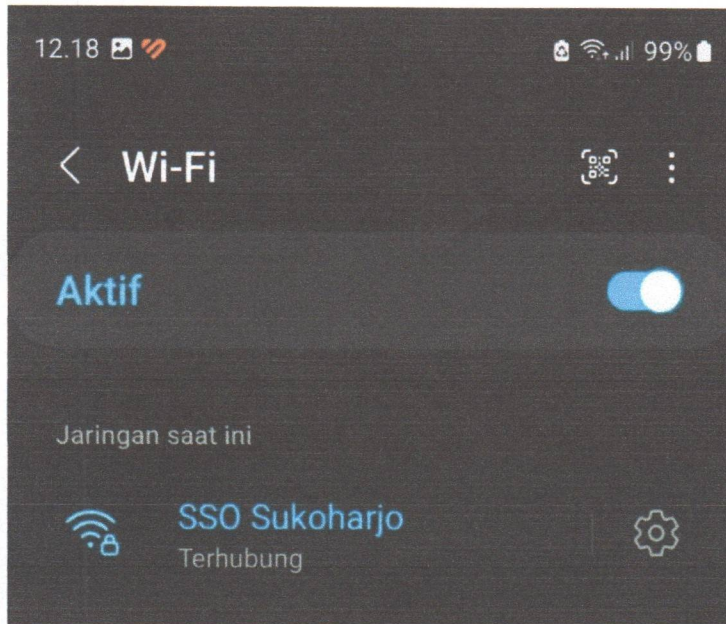
- Pada menu wifi, akan muncul SSID SSO Sukoharjo. Pilih SSID tersebut untuk menghubungkan ke jaringan.



- Selanjutnya, setting konfigurasi sebagai berikut:
 - Metode EAP: PEAP
 - Identitas: username pada account @pns.sukoharjokab.go.id
 - Kata sandi: password account @pns.sukoharjokab.go.id
 - Sertifikat CA: Jangan Validasi



- Wifi dapat tersambung ke SSO Sukoharjo



BUPATI SUKOHARJO, P
Etik Suryani
ETIK SURYANI

Etik