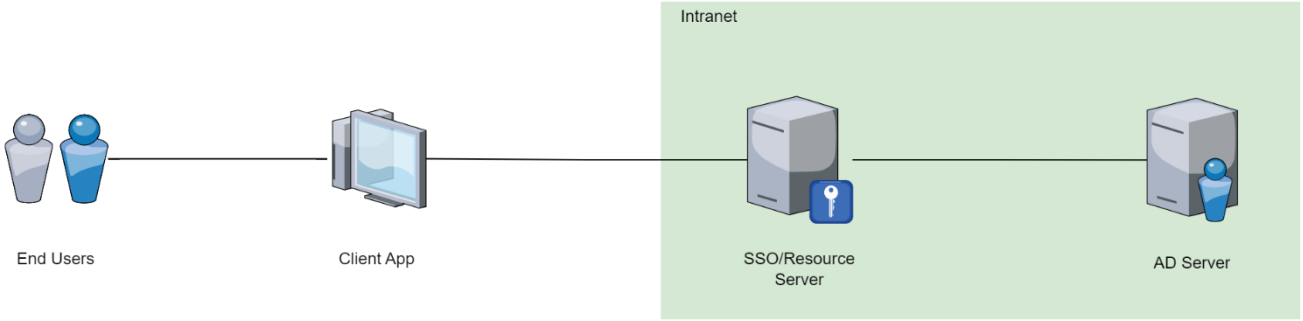
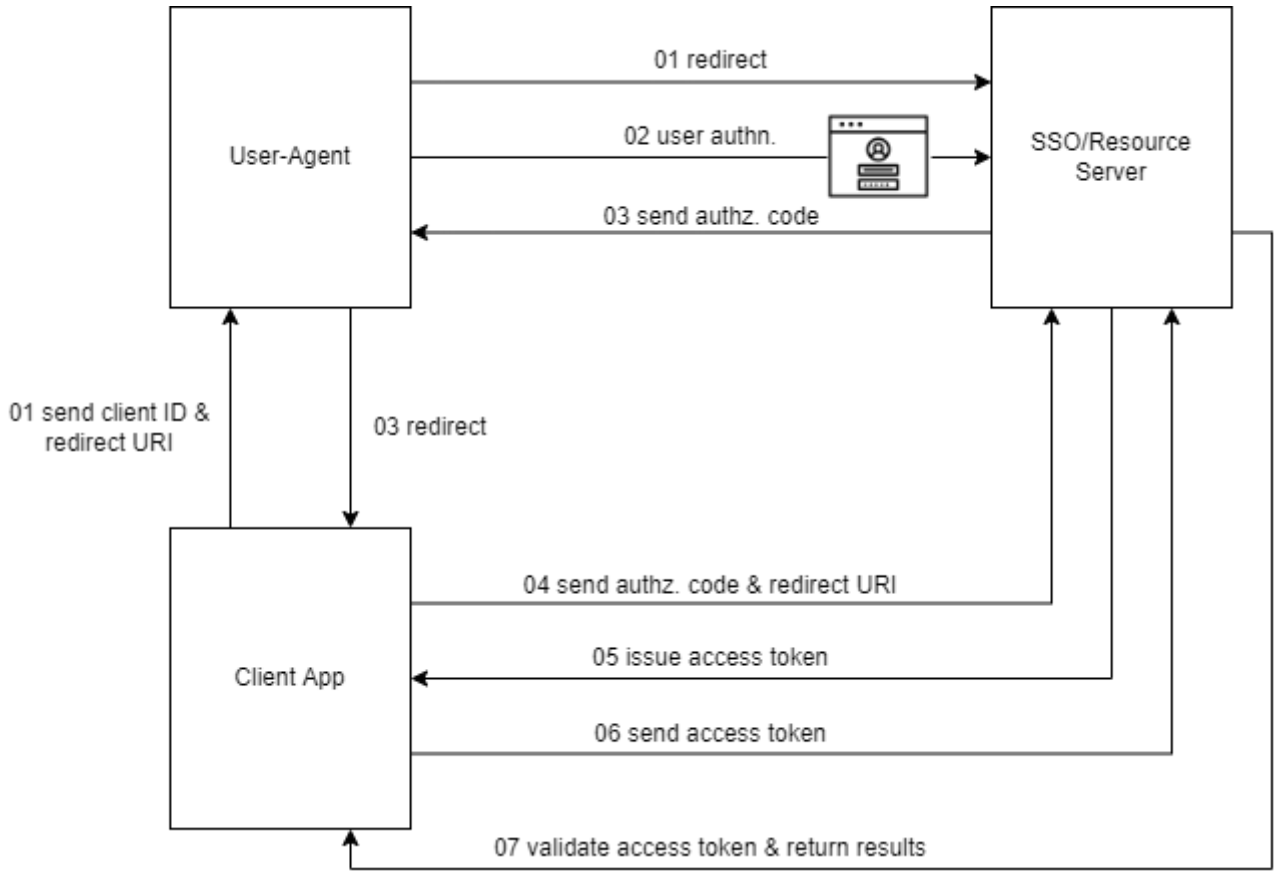
SSO Server Documentation

Table of Contents

I. System Architecture



II. Flowchart



III. Client Credentials Specification

1. Client Id

   Randomly generate GUID with no dash.

2. Client Secret

   Randomly generate 32 bytes then convert to string with Base64.

IV. API Specification

1. Authorize

Name	Authorize				
Description	Client redirect user-agent to SSO Server and show the sign-in page				
Request					
Method	GET				
Path	/oauth/authorize				
Parameters	Name	Required	In	Type	Description
	response_type	v	Query	string	OAuth flow type, must be “code”
	client_id	v	Query	string	Client identifier
	redirect_uri	v	Query	string	The URI that client has registered, the server will redirect the user-agent to this URL after authenticated
	state	v	Query	string	To maintain the state of the user-agent
	scope		Query	string	Requested permission(s) to the resources *currently not implemented
Example	GET {server address}/oauth/authorize?response_type=code&client_id=s6BhdRkqt3&redirect_uri=https%3A%2F%2Flocalhost%3A44377%2Foauth%2Fcallback&state=CfDJ8DqrCKkseT1LhY-15jdeucTVZwQGztP1zO2Y5hOTdP3gHFeSljp3rxBz3bN-U3k6_FJYrcwAKOY920LwqLqz9Qz0YHkKEn4YrsSVOrdwMouywYezDNiiJRL7h4Q2l8cWbxRdbIMIwilzkrIJpojzKuPXec1P8y5y3GJflKA9no8rkig2y17ulhVZt0-WKdYA1HLWXpNIEqMBopAdLXM5yxM HTTP/1.1				
Response					
Format	HTML				
Example	Code	200			
	Body	Log-in page HTML			

2. Token

Name	Token
Description	Client exchange authorization code for access token and redirect user-agent to client
Request	
Method	POST

Path	/oauth/token				
Parameters	Name	Required	In	Type	Description
	Authorization	v	Header	string	HTTP Basic authorization encoded with client id & secret
	grant_type	v	Form	string	Describe how to get access token: “authorization_code” or ”refresh_token”
	code		Form	string	Authorization code, required if the grand_type is “authorization_code”
	redirect_uri	v	Form	string	Should be the same as in authorization request
	client_id	v	Form	string	Client identifier
	refresh_token		Form	string	Token to refresh access token, required if the grand_type is “refresh_token” *currently not implemented

Request Example	POST {server address}/oauth/token HTTP/1.1
	Authorization: Basic czZCaGRSa3F0Mzo3RmpmcDBaQnIxS3REUmJuZlZkbUl3
	{
	"grant_type":"authorization code",
	"code": "2a322bbf891e419b9f08b17d3ccec694",
	"redirect_uri":"https://localhost:44377/oauth/callback",
	"client_id": "s6BhdRkqt3"
	}				

Response					
Scheme	Name	Required	Type	Description	
	access_token	v	String	Token to access protected resource	
	token_type	v	String	“Bearer”	
	raw_claim		String		
	refresh_token		String	Token to refresh access token	
Format	JSON				
Example	Code	200			
	Body	{ "access_token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJVc2VySWQiOiJhbGxhbi5jaGVuZyIsImVtYWlsIjoiYWxsYW4uY2hlbmdAZWRlbnJlZC5jb20iLCJuYmYiOjE2NjAyODQ5NjgsImV4cCI6MTY2Mjk2MzM2OCwiaXNzIjoiaHR0cHM6Ly9sb2NhbGhvc3Q6NDQzMzIvIi			

		wiYXVkIjoiaHR0cHM6Ly9sb2NhbGhvc3Q6NDQzMzIvIn0.0EGkzqA EAcLtTGAlK-VWfqHXduIgmSjQ4oGSyLzpW5I", "token_type":"Bearer", "raw_claim":"raw claim", "refresh_token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJVc2 VySWQiOiJwb3l1YW4ua2FuZyIsImVtYWlsIjoicG95dWFuLmthbmd AZWRlbnJlZC5jb20iLCJuYmYiOjE2NjA4MTU0MTYsImV4cCI6MTY2 MDkwMTgxNiwiaXNzIjoiaHR0cHM6Ly9sb2NhbGhvc3Q6NDQzMzI vIiwiYXVkIjoiaHR0cHM6Ly9sb2NhbGhvc3Q6NDQzMzIvIn0.5f5O3s GmWiZt0CsiamIBzB2CsgUrujElqBi0L6qr2wo" }

3. Validate Permission

Name	Validate Permission				
Description	Validate user's permission when accessing protected resource				
Request					
Method	POST				
Path	/api/user/permission				
Parameters	Name	Required	In	Type	Description
	ClientId	v	Header	string	Client identifier
	PermissionKey	v	Query	string	The permission identifier that should be validated

Example	POST {server address}/api/user/permission HTTP/1.1
	Authorization: Basic czZCaGRSa3F0Mzo3RmpmcDBaQnIxS3REUmJuZlZkbUl3
	{
	"ClientId":" s6BhdRkqt3",
	"PermissionKey": "User.Query"
	}				

Response					
Format	Empty text				
Example	Code	200, 401, 403, 500			