SPECIFICHE TECNICHE PER AUTENTICAZIONE TRAMITE OAUTH2

	Data	Nominativo	Funzione
Redazione	20/10/2022	Riccardo Righi	Area Sistemi di conservazione
Verifica	10/01/2023	Cristiano Casagni	Responsabile Area Sistemi di conservazione
Approvazione	10/01/2023	Stefania Papili	Responsabile del Servizio

Codice documento	Autenticazione_OAUTH2
Versione	1.0
Livello di riservatezza	**TLP:WHITE**
Lista di distribuzione	

Indice

Storia delle modifiche apportate al documento

VERSIONE	*Variazioni*	*Data*
1.0	Prima emissione	10/01/2023

Documenti di riferimento

Titolo e nome file	Indirizzo pubblicazione
Manuale di Conservazione	Documentazione — ParER — Polo archivistico dell'Emilia-Romagna (regione.emilia-romagna.it)
Specifiche tecniche dei servizi di versamento, aggiornamento, recupero e annullamento	Documentazione — ParER — Polo archivistico dell'Emilia-Romagna (regione.emilia-romagna.it)

Introduzione

Il presente documento descrive la modalità di autenticazione ai servizi di versamento di SACER tramite il protocollo OAUTH 2.

Questo documento non fornisce indicazioni di dettaglio sui protocolli utilizzati, in quanto standard internazionali, ma spiega come l'utilizzo di OAUTH 2 sia stato implementato all'interno di SACER.

Glossario

Per i termini utilizzati nel presente documento si rimanda al Glossario del Manuale di conservazione e al Glossario di cui all'Allegato 1 delle **Linee Guida**, alle definizioni del D.Lgs. 82/2005 e del DPR 445/2000 e loro successive modificazioni e integrazioni.

1. Premessa

OAuth è un protocollo di rete aperto e standard, progettato specificamente per lavorare con l'Hypertext Transfer Protocol (HTTP). Essenzialmente consente l'emissione di un token di accesso da parte di un server autorizzativo ad un client di terze parti.
Quello che viene comunemente chiamato OAUTH 2.0 non è altro che l'aggiornamento con alcuni miglioramenti del protocollo OAUTH di cui mantiene i principi ma ne aggiorna le modalità tecniche per renderlo più sicuro e flessibile.
Tramite il protocollo OAUTH 2 le applicazioni possono accedere a risorse protette di un servizio per conto di un utente. In questo caso l'accezione "utente" può attribuirsi sia ad una utenza personale che applicativa[1].
OAuth 2.0 definisce flussi di autorizzazione per applicazioni native, applicazioni Web e dispositivi mobili.

2. Modalità di utilizzo dell'autenticazione con OAUTH 2.0 in SACER

L'autenticazione tramite OAUTH 2 è utilizzata in SACER per autenticare le chiamate ad alcuni servizi di versamento. Non tutti i servizi utilizzano questa modalità: la documentazione specifica dei servizi indica a quali risorse viene dato l'accesso tramite il protocollo OAUTH 2[2].
In SACER il protocollo OAUTH 2 non viene utilizzato per le utenze associate a persone fisiche.
Tra i vari flussi previsti dal protocollo OAUTH 2.0, SACER utilizza il flusso: Client Credentials Grant Type.

2.1. Flusso di autenticazione

Il Client Credentials Grant Type si utilizza quando un'applicazione server side richiede l'accesso ad una risorsa HTTP senza un Resource Owner[3], quindi senza che una persona reale stia usando l'applicazione Client.
Questo flusso del protocollo OAUTH 2 non può essere utilizzato quando chi effettua la richiesta è una persona reale.
Il flusso prevede che un applicazione client effettui una chiamata rest all'authorization server per la richiesta di un token applicativo.
L'authorization server esegue i controlli e, se l'esito degli stessi è positivo, rilascia l'access token.
L'applicazione client effettua le successive chiamate di richiesta inserendo nella chiamata l'access token ricevuto inizialmente.

[1] Informazioni di dettaglio sul protocollo OAUTH sono disponibili su: https://www.oauth.com/

[2] Servizi di versamento UD, Servizi di aggiornamento metadati, Servizi di aggiunta documenti, Servizi di versamento fascicoli. Disponibili qui: https://poloarchivistico.regione.emilia-romagna.it/documentazione/specifiche-tecniche-dei-servizi-di-versamento-di-unita-documentarie

[3] Resource owner: il proprietario dell'informazione esposta

2.1.1. Richiesta del token applicativo

Per ottenere il token applicativo è necessario invocare l'apposito metodo. Per SACER è necessario passare 4 parametri per ricevere il token applicativo:

- **Client ID:** è l'identificativo univoco per le app invocate. In SACER ogni servizio di versamento che utilizza OAUTH2 è censito come app[4]. Quindi ogni servizio di versamento ha un CLIENT_ID diverso dagli altri;
- **Client Secret:** è un segreto noto solo all'applicazione e al server di autorizzazione. È essenzialmente la password dell'applicazione[5];
- **Username:** è il nome dell'utenza applicativa[6];
- **Password:** è la password riferita all'username[7].

La risposta del servizio di autorizzazione conterrà alcune informazioni tra cui:

- **access token:** è il token necessario per i servizi specifici di versamento;
- **expires_in:** è la durata espressa in secondi dell'acces token.

Esempio di risposta:


```
"access_token": "KKlKaGJHY2lPaUpErMMpJMU5pSXNJblI1Y0NJZ09pQWlTbGRVSWl3aWEybGtJaUE2SUNJMlN
XWmZTSEE1UVdVNVNYVm5NbE5yY2xQnk4THRodG9yNy1TcDl2YmRtRjFGbkJ5V3B4VzlOVzOT1RucEJNalYzTkdOQk
4yTkZSWEpITFZKQlkyRm9NbUl3SW4wLmV5SmxlSEFpT2pFMk5qWTVOakUyTnpZc0ltbGhkQ0k2TVRZMk5qazJNVEE
zTml3aWFuUnBJam9pWlRreU1EVXdPR1F0T1dabVl5MDBZV05oTFdGbVkyTXRZelJqTURVeFpUUXpaREJsSWl3aWFY
TnpJam9pYUhSMGNITTZMeTl6YzI4dGNHRnlaWEl0ZEdWemRDNXlaV2RwYjI1bExtVnRhV3hwWVMxeWIyMWhaMjVoT
G1sMEwyRjFkR2d2Y21WaGJHMXpMMUJoY21WeUlpd2lZWFZrSWpvaVlXTmpi0luTjFZaUk2SW1ZNk9EYzRabUl6WkR
NdFpXRXpNaTAwWVRZMExUZ3hOV0V0T0RjMVltRTRNMlprWVdFd09tWjBjRjlyWlhSMGJHVmZjR2x1WnlJc0luUjVj
Q0k2SWzh0Wm1GelkybGpiMnh2SWl3aWMyVnpjMmx2Ymw5emRHRjBaU0k2SWpjMFpXTmhOVFF6TFdaa01tTXROR0kz
T0MxaVpXVXpMOTI3ODQ3NTYyNzgxOXlPRFU1T1NJc0luSmxZV3h0WDJGalkyVnpjeUk2ZXlKeWIyeGxjeUk2V3lKM
lpYSnpZWFJ2YZMjl3WlNJNkltVnRZV2xzSUhCeWIyWnBiR1VpTENKemFXUWlPaUkzTkdWallUVTBNeTFtWkRKakxU
UmlOemd0WW1WbE15MWlNVEExT0dJMk1qZzFPVGtpTENKbGJXRnBiRjkyWlhKcFptbGxaQ0k2Wm1Gc2MyVXNJbTVoY
ldVaU9pSm1kSEJmYTJWMGRHeGxYM0JwYm1jZ1puUndYMnRsZEhSc1pWOXdhVzVuSWl3aVozSnZkWEJ6SWpwYkluWm
xjbk5oZEc5eVpTSmRMQ0p3Y21WbVpYSnlaV1JmZFhObGNtNWhiV1VpT2lKbWRIQmZhMlYwZEd4bFgzQnBibWNpTEN
KbmFYWmxibDl1WVcxbElqb2lab21VaVhYMHNJbkpsYzI5MWNtTmxYMkZqWTJWemN5STZleUpoWTJOdmRXNTBJanA3
SW5KdmJHVnpJanBiSW0xaGJtRm5aUzFoWTJOdm111155793625ldGdVlXZGxMV0ZqWTI5MWJuUXRiR2x1YTNNaUxD
SjJhV1YzTFhCeWIyWnBiR1VpWFgxOUxDSnplJ3WDJ0bGRIUnNaVjl3YVc1bklpd2labUZ0YVd4NVgyNWhiV1VpT2l
KbWRIQmZhMlYwZEd4bFgzQnBibWNpTENKbGJXRnBiQ0k2SW1SaFJHVm1hVzVwY21WQVpHRkVaV1pwYm1seVpTNXBk
Q0o5LkxPRTVuWU9uX0x0VE5RWTB4MVdpOU4waWc0RkI5M3FUY0ZmMTNYLWJvX2FlZlJfLWNJaFJ2Q240dU0xeHRzR
3dKaktZZUFZOFZwNlgwU01rMmVMeVdrdUk3c2JHSEF4R1UwLXBCNTlM1Z1ZENJcPc3FKR19EOUNlOFp6WXQwczNoN
EZPcxc1pnV2Nub25BVmVBQ1VXR0kyYU1sUk9KODA1TmZNZVhhOWd0RTFaaE5zOURHLXJZSTUtYkpRX0lQOXNONnNn
dzFYb2lPQ3pYOWZocVpQU2ZPWm9tVEFoNzNqNjdyTlZWQzRsdk9XdGUzWVZiYUMzVTBfUG5RYjFWVW5jT0d1YUdJa
jhTMWdXTFdoeVNkUmVvbHdFcEJOUxVeHRzTG1QSnU0cUNDWmlPNjExMmhLTHZXV0RtLLZPZwtKbFlYSmxjaUlzSW1
GNmNDSTZJblpsY25OaGJXVnVkR",
    "expires_in": 600,
    "refresh_expires_in": 0,
    "token_type": "Bearer",
    "not-before-policy": 0,
    "session_state": "sopdkfpsokdfpo-b1058b628599",
```


[4] Va richiesto all'assistenza PARER

[5] Va richiesta all'assistenza PARER

[6] Va richiesta all'assistenza PARER

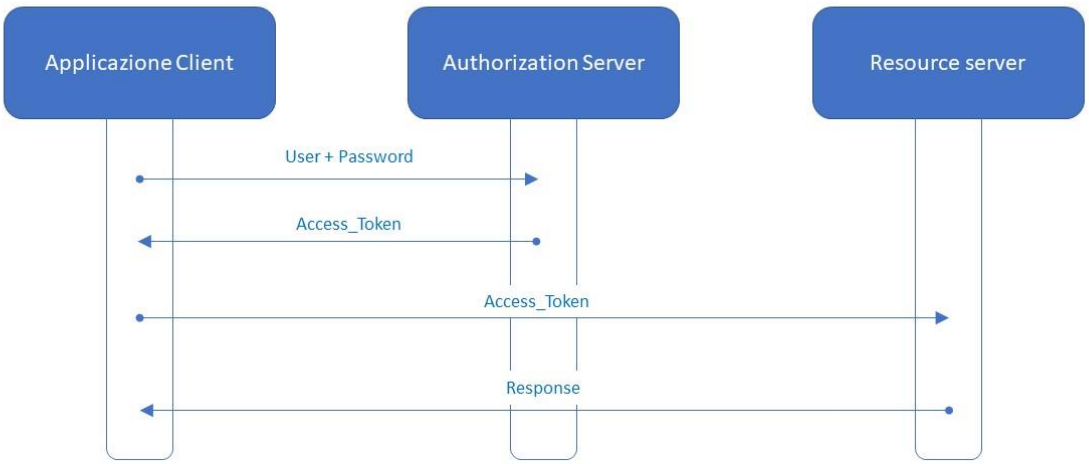
[7] Va richiesta all'assistenza PARER

```
"scope": "email profile"
```

2.1.2. Flusso per l'utilizzo dei servizi SACER

L'invocazione dei servizi utilizzando il protocollo di autenticazione OAUTH 2 presuppone una sequenza di due chiamate:

- la prima per l'ottenimento dell'access token
- la seconda per l'invocazione del servizio



Nel caso in cui però il servizio necessario debba essere invocato più volte (Es: il client ha esigenza di versare 3 fascicoli) la sequenza delle chiamate potrebbe essere gestita diversamente. Entrambe le casistiche elencate sono supportate da SACER:

Caso 1: Chiedere il token applicativo ad ogni chiamata

Riprendendo l'esempio indicato sopra il client ha necessità di versare 3 fascicoli (Fascicolo A, Fascicolo B, Fascicolo C), lo scopo potrebbe essere raggiunto con questo flusso di chiamate:

- *Richiesta* access token;
  - *Risposta* con access token "1";
- *Richiesta* versamento con token "1" di "Fascicolo A";
  - *Risposta* con esito del versamento;
- *Richiesta* access token;
  - *Risposta* con access token "2";
- *Richiesta* versamento con token "2" di "Fascicolo B";

    - *Risposta* con esito del versamento;
- *Richiesta* access token;
    - *Risposta* con access token "3";
- *Richiesta* versamento con token "3" di "Fascicolo C";
    - *Risposta* con esito del versamento.

Caso 2: Utilizzare il token applicativo finché valido

- *Richiesta* access token;
    - *Risposta* con access token "1";
- *Richiesta* versamento con token "1" di "Fascicolo A";
    - *Risposta* con esito del versamento;
- *Richiesta* versamento con token "1" di "Fascicolo B";
    - *Risposta* con esito del versamento;
- *Richiesta* versamento con token "1" di "Fascicolo C";
    - *Risposta* con esito del versamento.

Nel secondo caso proposto il client dovrà gestire l'eventuale scadenza dell'access token. Terminato il periodo di validità dell'access token il client non riuscirà ad accedere alle risorse e dovrà richiedere un nuovo token applicativo.