Technical Disclosure Commons

Defensive Publications Series

June 2020

Client Authorization Grants With Account Creation Capability Using OAuth 2.0

Rohey Livne

Vitalii Tomkiv

Jeff Craig

Jason Stoops

Client Authorization Grants With Account Creation Capability Using OAuth 2.0

ABSTRACT

A user of a web or mobile application, e.g., a video-sharing application, may want to access another online service, e.g., a third-party blogging or social media service, without leaving the application. The OAuth 2.0 standard is a common mechanism for authorizing a web application to access an account owned by the user on another online service. However, if the user does not have an account on the online service, accessing the service from within the application is at best tedious, and at worst, not presently possible. This disclosure describes OAuth-based techniques that enable a user of a web or mobile application to invoke an online service unrelated to the application from within the application, even when the user does not have an account with the online service, or an installed app for the service.

KEYWORDS

- OAuth 2.0
- User authentication
- Account creation
- Authorization framework
- Authorization code grant
- Identity provider
- Assertion framework
- Client authorization grant

BACKGROUND

A user of a web or mobile application, e.g., a video-sharing application, may want to access an unrelated online service, e.g., a third-party blogging or social media service, without leaving the application. For example, the user may want to write a comment at the third-party hosted website that provides the service about the video they're watching. The OAuth 2.0 standard is a common mechanism for authorizing a client, e.g., the web application, to access an account owned by the user on an (unrelated) online service. However, if the user does not have an account on the online service, accessing the service from within the application is not presently possible. To post a comment in such a situation, the user is required to exit the application, and install and invoke the online service. This burden can lead to the user giving up the task.

Thus, when linking third party user accounts, the classical OAuth 2.0 flow can result in a high user drop-off, because users do not have accounts at the online service or have problems remembering their account credentials. The use of assertion framework for OAuth 2.0 in conjunction with a trusted identity provider can alleviate the problem slightly, but is still inadequate when consent or additional information is to be obtained from the user.

A set of internet engineering task force RFCs, e.g., RFC6749, RFC7521, RFC7519, etc., address similar problems, using, e.g., extension grants for authorization requests, JSON web tokens, JSON web signatures, etc. However, these RFCs do not solve the problem of creating a new resource owner account, nor do they provide options for a relying party to obtain resource owner consent or additional information during the authorization request.

DESCRIPTION

This disclosure describes OAuth-based techniques that enable a user of a web or mobile application to invoke an online service unrelated to the application from within the application, even when the user does not have an account with the online service, or an installed app for the service.

For example, the web or mobile application can be a video-sharing application, and the online service can be a third-party blogging or social media service. The user does not have an app corresponding to the service nor an account with the service. Per the techniques, as the user watches a video over the video-sharing application, a dialog box pops up within the video-sharing application that enables the user to write a comment within the dialog box, and have the comment posted on the third-party service.

The necessary authentication, identity verification, and account-creation steps are automatically handled, and if, for account-creation purposes, additional information is needed from the user, it is smoothly requested for and obtained from the user in a frictionless manner. Effectively, the described techniques auto-create an account at the third-party online service on behalf of and with the permission of the user.

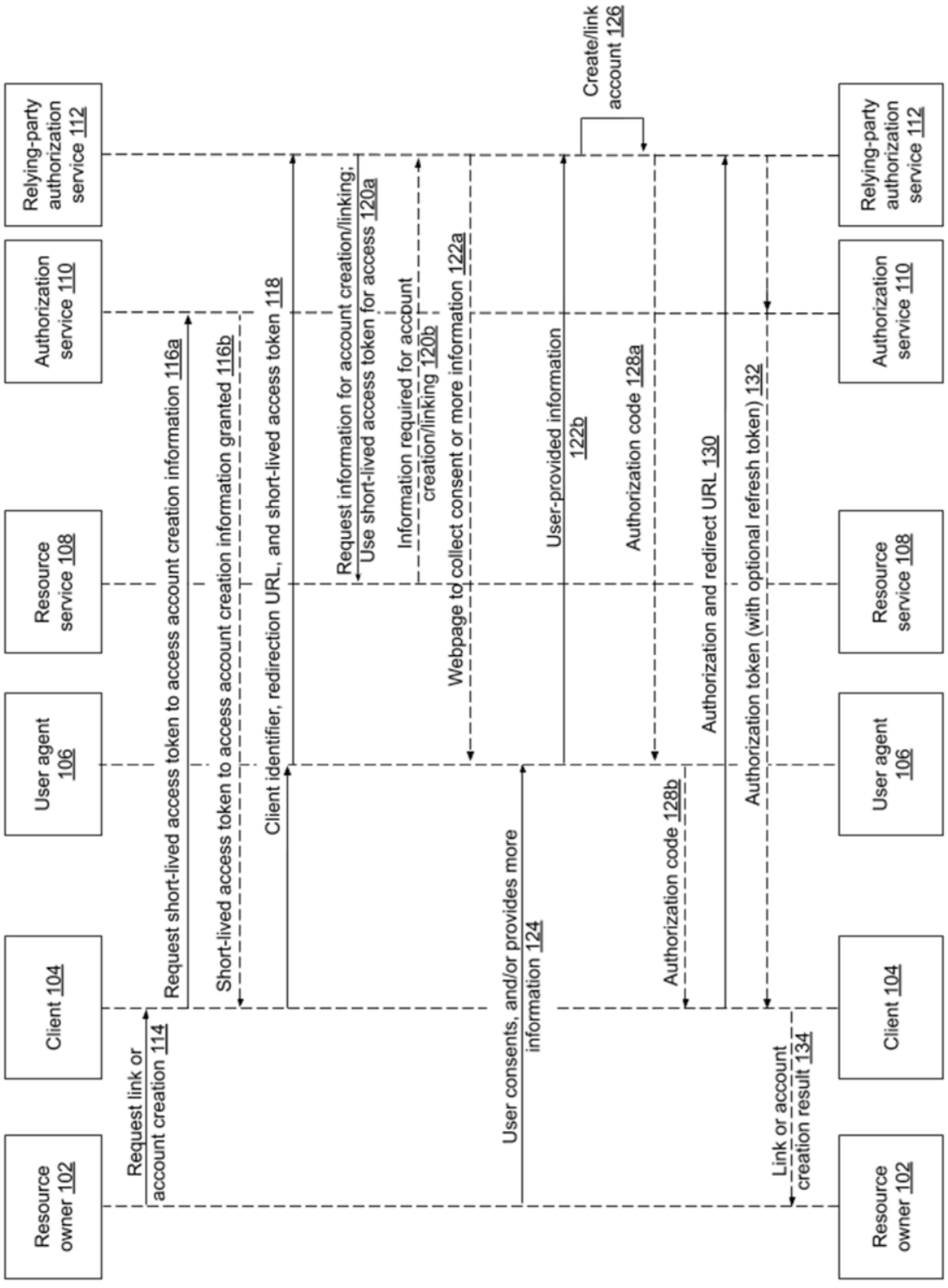

Fig. 1: Assertion framework for OAuth 2.0 that enables client authorization grants that can create accounts and obtain additional information from the user

Fig. 1 illustrates an example assertion framework for OAuth 2.0 that enables client authorization grants that can create accounts and obtain additional information from the user, per the techniques of this disclosure. A resource owner (102) is the user that operates a client (104), e.g., a web or mobile application such as a video-sharing application, and wishes to access an external resource service (108). A user agent (106) can be, e.g., a web browser or other application. An authorization service (110) is an online identity provider, e.g., a service that identifies and authenticates the resource owner (user). A relying-party authorization service (112) is the authorization agent of the external resource service, e.g., the module of the third-party online service that receives authentication from an identity provider.

The resource owner (user) requests the client, e.g., the video-sharing application, to sign in (creating an account as necessary) and to access the resource service (114), e.g., to write a comment on the service from within the client. The client requests from the authorization service a short-lived access token to access account creation information (116a), and receives it from the authorization service (116b). The short-lived access token can be in the form of a user-authenticating URL that can access information about the resource owner from the authorization service, and that can be presented to the resource service to identify the user for purposes of account creation or linking.

The client directs the user agent to transmit to the relying-party authorization service (118) the client identifier, the requested scope, the local state, the redirection URL, and the short-lived access token. For example, the video-sharing application opens the browser, and the browser opens the authorization page of the third-party online service and passes to the authorization page the short-lived access token.

The relying-party authorization service uses the short-lived access token to request from the resource service information relating to account creation or linking (120a) and receives such information from it (120b). For example, the third-party online service uses the short-lived access token to check with the identity service provider as to whether the user is who they claim to be. The authorization service authenticates the resource owner, e.g., grants or denies the client's access request.

If more information is needed from the user for the purpose of account creation, such information is requested of the user (122a) and obtained (112b), e.g., via user input. The authorization service obtains consent from the user (124) to create or link an account on the resource service in the name of the resource owner. User consent and additional information can be obtained via a webpage rendered by the resource service and presented to the resource owner by the user agent.

Based on the information in the short-lived access token and the additional information provided by the user, and under user consent, an account is created or linked (126) at the resource service by the relying-party authorization service. An authorization code is transmitted to the user agent (128a), which in turn forwards it to the client (128b).

The client responds by transmitting the authorization and a redirect URL to the relying-party authorization service (130). The relying-party authorization service transmits an authorization token (with an optional refresh token, 132) to the client via the authorization service. The authorization token is retained at the client or by the resource owner for present and future use. The account or link creation result (success or failure) is reported to the resource owner (134). A new user account is created at the third party site for the user, if the user so desires.

In this manner, this disclosure modifies the authorization code grant protocol of OAuth 2.0, e.g., as in RFC6749 Section 4.1, to combine within the same flow the advantages of the assertion framework with the flexibility provided by the presence of the user agent.

CONCLUSION

This disclosure describes OAuth-based techniques that enable a user of a web or mobile application to invoke an online service unrelated to the application from within the application, even when the user does not have an account with the online service, or an installed app for the service. A new user account is created at the third party site for the user, if the user so desires.

REFERENCES

[1] Internet Engineering Task Force, “RFC6749: The OAuth 2.0 Authorization Framework.”

[2] Internet Engineering Task Force, “RFC7521: Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants.”

[3] Internet Engineering Task Force, “RFC7519: JSON Web Token (JWT).”