

# 摩登 OAuth 2.0：簡介

隨著時間的推移，OAuth 2.0 相關的標準越來越多，該系列文章旨在介紹更現代的 OAuth 2.0 知識。本章乃第一章簡介。

OAuth 2.0 開發者應該不陌生。其正式發表至今已逾六年，加之眾多知名公司使用，圍繞著這些公司的開放（或偽開放）平台，開發者也越來越多，名氣也就愈發響亮了。但是認真讀過標準的卻沒有多少人，不按標準來實現 OAuth 2.0 服務的公司不可勝數。而況這些年里，OAuth 2.0 又有許多新的標準規範誕生。我因為在寫 [Authlib](#)<sup>①</sup>，相關的標準略有閱讀，或有所得，不才分享一二，但求解惑三四人。

## 歷史

OAuth 的歷史最早可追溯到 2006 年 11 月，Twitter 需要一套 API 的授權訪問方案，彼時並沒有一套開放的標準規範來實現 API 的授權。由 Twitter 的開發者 Blaine Cook 首倡<sup>②</sup>，最終於 2007 年 7 月完成了 OAuth 的初版草案。2007 年 12 月 4 日 OAuth Core 1.0 正式發佈。

這是 OAuth 1.0 的歷史。其後 OAuth 1.0 進入 IETF，2010 年 4 月 RFC5849 發佈。這期間，即 2009 年 IETF 成立了一個 OAuth 工作組，後來的 OAuth 2.0 正是由這個工作組創建的，用以取代 OAuth 1.0。

無論是 OAuth 1.0 還是 OAuth 2.0，他們解決的都是同一個問題，即「如何讓一個應用在用戶的授權下訪問操作用戶授權的有限資源」。

## 框架

OAuth 2.0 與 OAuth 1.0 並不兼容，其實是個全新的體系。不同於 OAuth 1.0，OAuth 2.0 是一個框架，而 OAuth 1.0 是一個協議<sup>③</sup>。框架，意味著開發者可以在 OAuth 2.0 這一體系里添磚加瓦，修補 OAuth 2.0 的不足，亦可以利用其構建新的協議。

時至今日，OAuth 2.0 框架體系里已經誕生了許多標準協議，亦有許多草案等待完善。除卻最初的 RFC6749 (OAuth 2.0 Framework) 和 RFC6750 (Bearer Token)，這裡列舉些許別的 RFC：

1. RFC7009: OAuth 2.0 Token Revocation
2. RFC7519: JSON Web Token
3. RFC7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants
4. RFC7591: OAuth 2.0 Dynamic Client Registration Protocol
5. RFC7636: Proof Key for Code Exchange by OAuth Public Clients

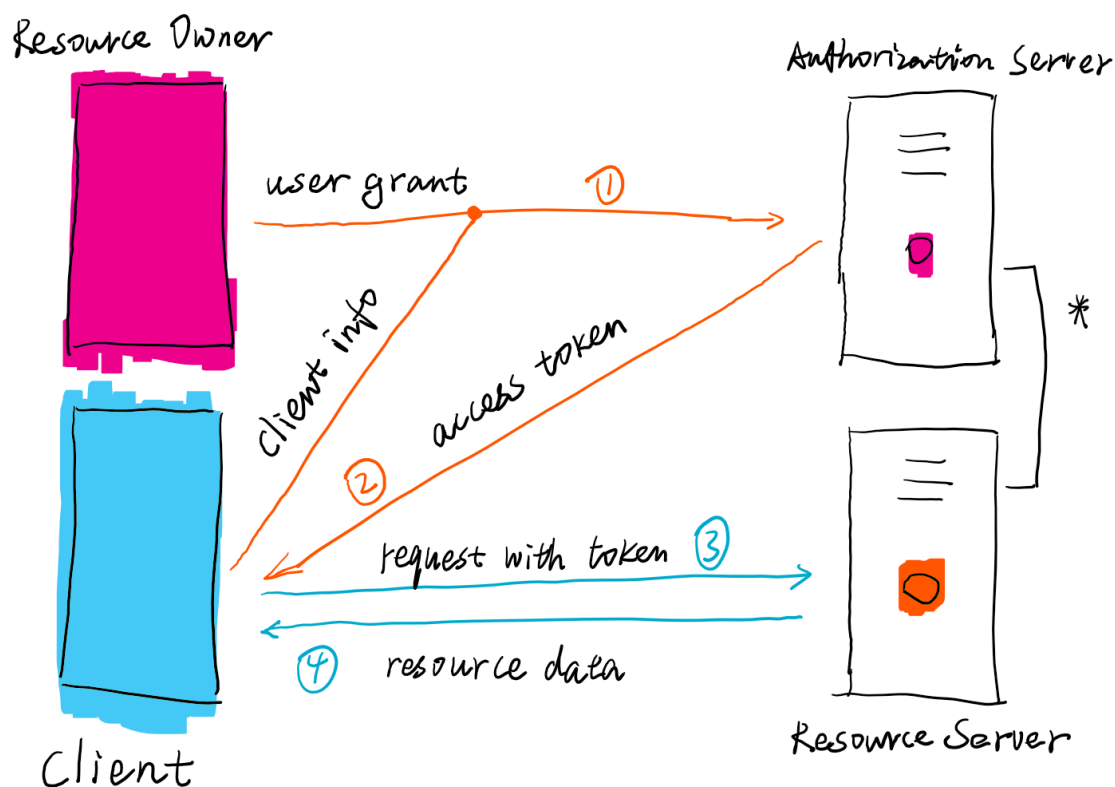
發現沒有，就連 JWT 亦是 OAuth 工作組起草的。更全面的 RFC 列表可參考 [OAuth Status Page](#)。

## 角色

在 OAuth 2.0 框架內，通常有 4 種角色。分別是：

1. Resource Owner：資源所有者。例如一個圖片分享網站，圖片就是資源，而圖片的上傳者便是資源所有者，通常便是這個圖片分享網站的用戶。
2. Resource Server：資源服務。提供訪問這些圖片數據的 API。
3. Client：客戶端。例如能訪問這個圖片分享網站的 iOS App。
4. Authorization Server：認證服務。在資源所有者的允許下，提供訪問權限給客戶端。

有時你能明顯感受到這些角色的存在，有時則不然。但通常這四種角色都會存在於一個完整的 OAuth 2.0 授權訪問流程里，如圖所示：





一個完整的 OAuth 2.0 授權訪問流程

OAuth 2.0 的授權流程：

1. 客戶端提供其自身的信息，在資源所有者的允許下，向認證服務請求 Access Token。
2. 認證服務驗證通過後，返回 Access Token 給客戶端。
3. 客戶端使用 Access Token 向資源服務請求用戶數據。
4. 資源服務驗證 Access Token 有效後，返回資源數據。

須知，資源所有者的授權有多種方式，客戶端提供自身信息有多種方式，請求 Access Token 的方法亦有多種方式，便連返回的 Access Token 種類也可以有多種形態。而這些不同的方式不同的形態，在 OAuth 2.0 框架體系里是可以擴展的，隨著時間的推移，會有更多的草案變成標準，亦會有更多人提出其他草案。

2. OAuth started around November 2006, while Blaine Cook was working on the Twitter OpenID implementation. [Read more](#) 
3. **RFC5849: The OAuth 1.0 Protocol** vs **RFC6749: The OAuth 2.0 Authorization Framework** 

ENJOY

#oauth