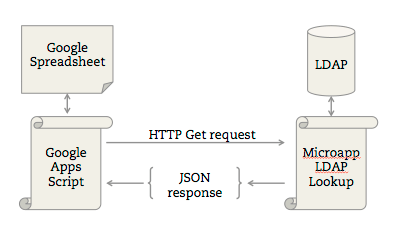
Authentication Protocols: LDAP vs Kerberos vs OAuth2 vs SAML

Authentication of users towards applications is probably one of the biggest challenges the IT department is facing. There are a lot of different systems a user needs access to and that’s why the authentication protocols are typically open standards – we are introducing the five most commonly used ones. When reading questions about the “correct authentication protocol” on Stackoverflow like ”Could you help me determine which authentication protocol I should use for the following use case?” It becomes pretty clear that this can be an overwhelming topic. Tech republic and others have done a great job in summarizing the sheer chaos in providers and standards.

## **LDAP**

[LDAP](https://msdn.microsoft.com/en-us/library/aa367008(v=vs.85).aspx) (Lightweight Directory Access Protocol) is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.

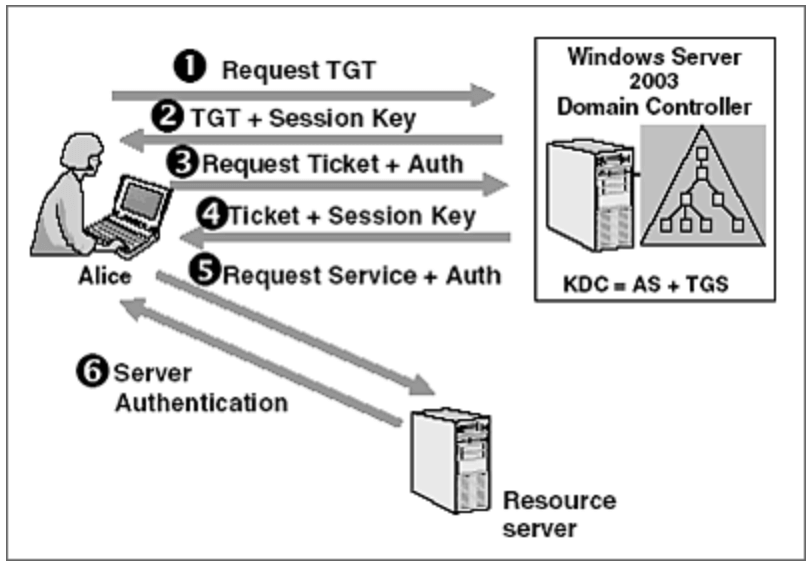


[Source](http://sites.nd.edu/devops/2014/01/19/google-apps-scripts-ldap-and-wookiee-steak/)

‍

## **Kerberos**

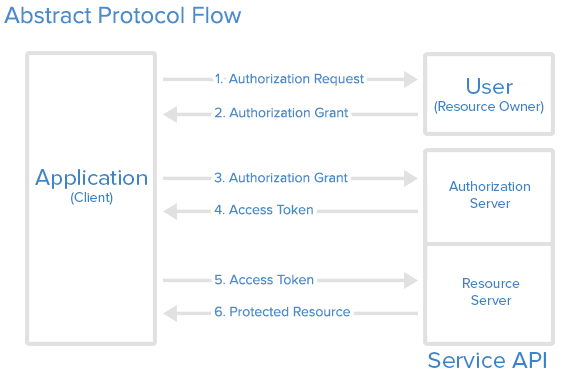
[Kerberos](https://web.mit.edu/kerberos/) is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.



[Source](https://searchwindowsserver.techtarget.com/feature/Five-steps-to-using-the-Kerberos-protocol)

## **Oauth 2**

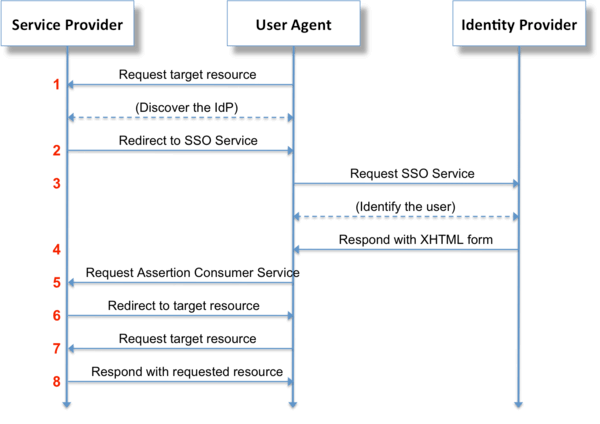
[OAuth 2](https://tools.ietf.org/html/rfc6749) is an authorization framework that enables applications to obtain limited access to user accounts on an HTTP service, such as Facebook, GitHub, and DigitalOcean.



Source: [Digital Ocean](https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2)

## **SAML**

Security Assertion Markup Language ([SAML](http://saml.xml.org/)) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider. SAML is a product of the OASIS Security Services Technical Committee.



Important to go through the following:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-scenarios>

A screenshot of a cell phone

Description automatically generated

Example:

{

"access\_token": "91d5507e-33e8-4ea8-8c5b-f0b6014b3e3d",

"token\_type": "Bearer",

"expires\_in": 3600,

"refresh\_token": "dc634c06-4eec-4cca-aae4-d7a23e992757", - REFRESH TOKEN

"scope": "oob",

"Claims": [

{

"claimType": "http://schemas.tesco.com/ws/2011/12/identity/claims/clientid", ---🡪 APPLICATION ID

"value": "trn:tesco:cid:b1cf0673-b053-43c5-8355-4101cf24e7ff"

},

{

"claimType": "http://schemas.tesco.com/ws/2011/12/identity/claims/scope",

"value": "oob" -🡪 SCOPE

},

{

"claimType": "http://schemas.tesco.com/ws/2011/12/identity/claims/userkey",

"value": "trn:tesco:uid:uuid:2ea74be1-57c7-32ef-b752-ef42d70cb1c4"

},

{

"claimType": "http://schemas.tesco.com/ws/2011/12/identity/claims/confidencelevel",

"value": "12"

},

{

"claimType": "http://schemas.microsoft.com/ws/2008/06/identity/claims/expiration",

"value": "1580223570". -🡪 EXPIRY

}

]

}