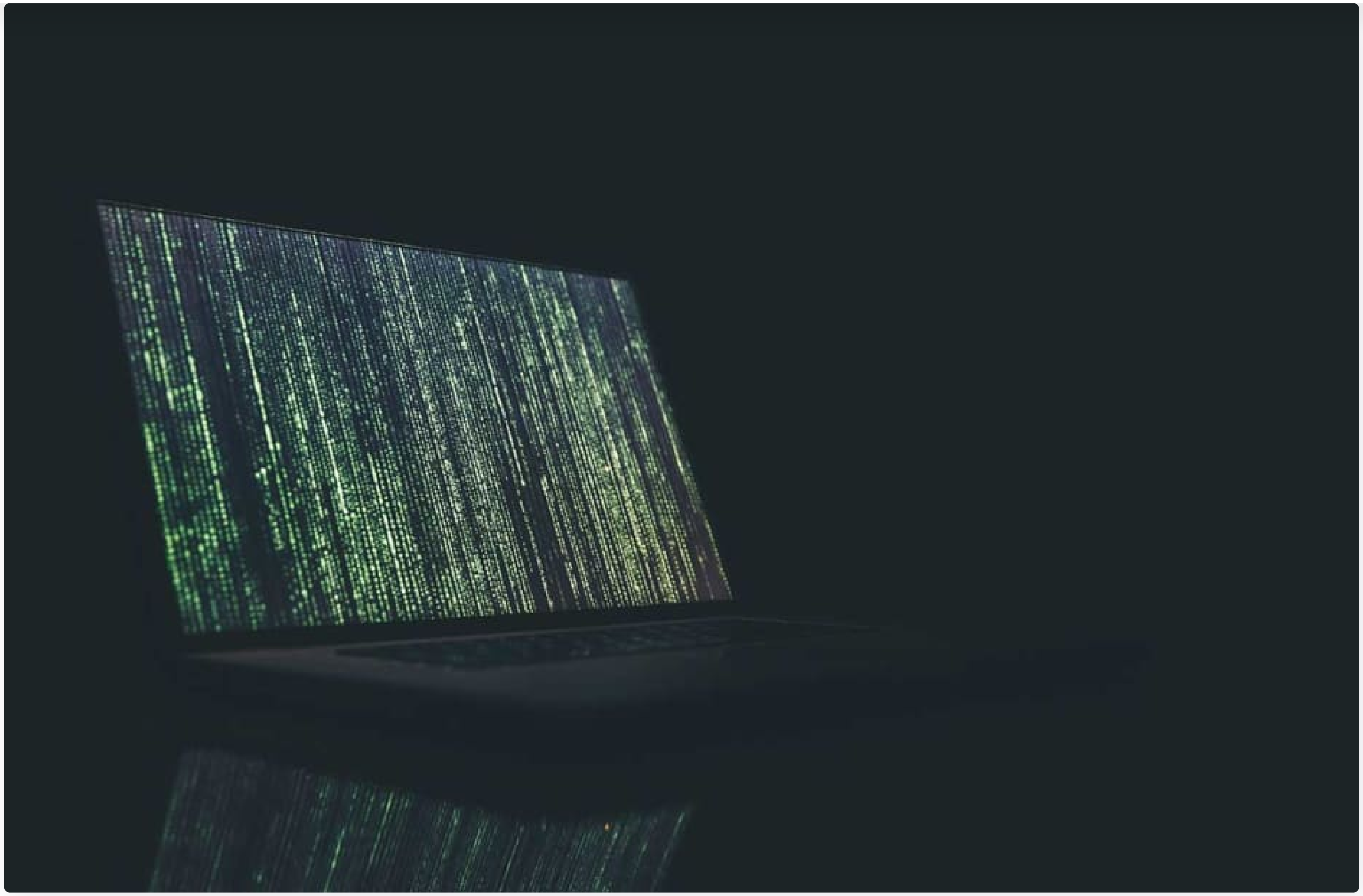
kisi blog

Authentication Protocols: LDAP vs Kerberos vs OAuth2 vs SAML vs RADIUS

By Bernhard Mehl

June 11, 2018



User authentication in applications is one of the biggest current challenges the IT department is facing. There are a lot of different systems a user needs access to, and that's why most authentication protocols are typically open standards.

When reading questions about authentication protocols on Stack Overflow, it becomes pretty clear that this can be a confusing and overwhelming topic.

In this blog post, we introduce the five most commonly used authentication protocols and explain how they work and

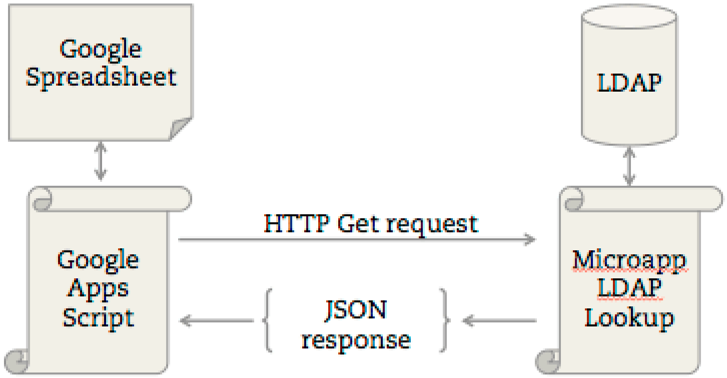
LDAP

LDAP (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 a corporate intranet.

It is fair to say that LDAP has become a popular program. It served as the foundation on which Microsoft built Active Directory, and has been instrumental in the development of today's cloud-based directories (also known as Directories-as-a-Service).

LDAP sends messages between servers and client applications which can include everything from client requests to data formatting.

On a functional level, LDAP works by binding an LDAP user to an LDAP server. The client sends an operation request that asks for a particular set of information, such as user login credentials or other organizational data. The LDAP server then processes the query based on its internal language, communicates with directory services if needed, and responds. When the client receives the response, it unbinds from the server and processes the data accordingly.

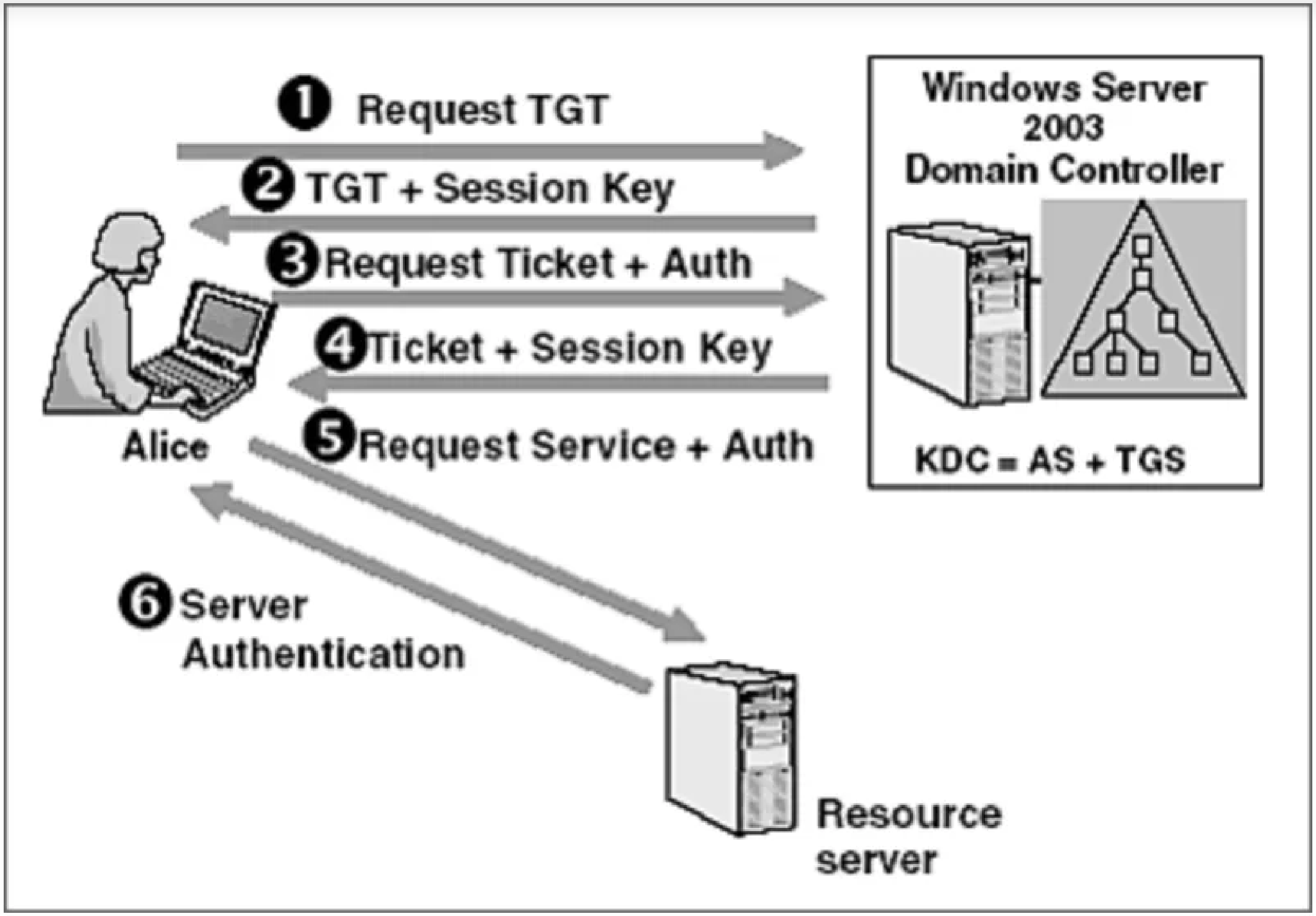


Kerberos

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.

Here are the most basic steps taken to authenticate in a Kerberized environment.

1. Client requests an authentication ticket (TGT) from the Key Distribution Center (KDC).
2. The KDC verifies the credentials and sends back an encrypted TGT and session key.
3. Client requests to access an application on a server. A ticket request for the application server gets sent to the KDC which consists of the client's TGT and an authenticator.
4. The KDC returns a ticket and a session key to the user.
5. The ticket is sent to the application server. Once the ticket and authenticator have been received, the server can authenticate the client.
6. The server replies to the client with another authenticator. On receiving this authenticator, the client can authenticate the server.

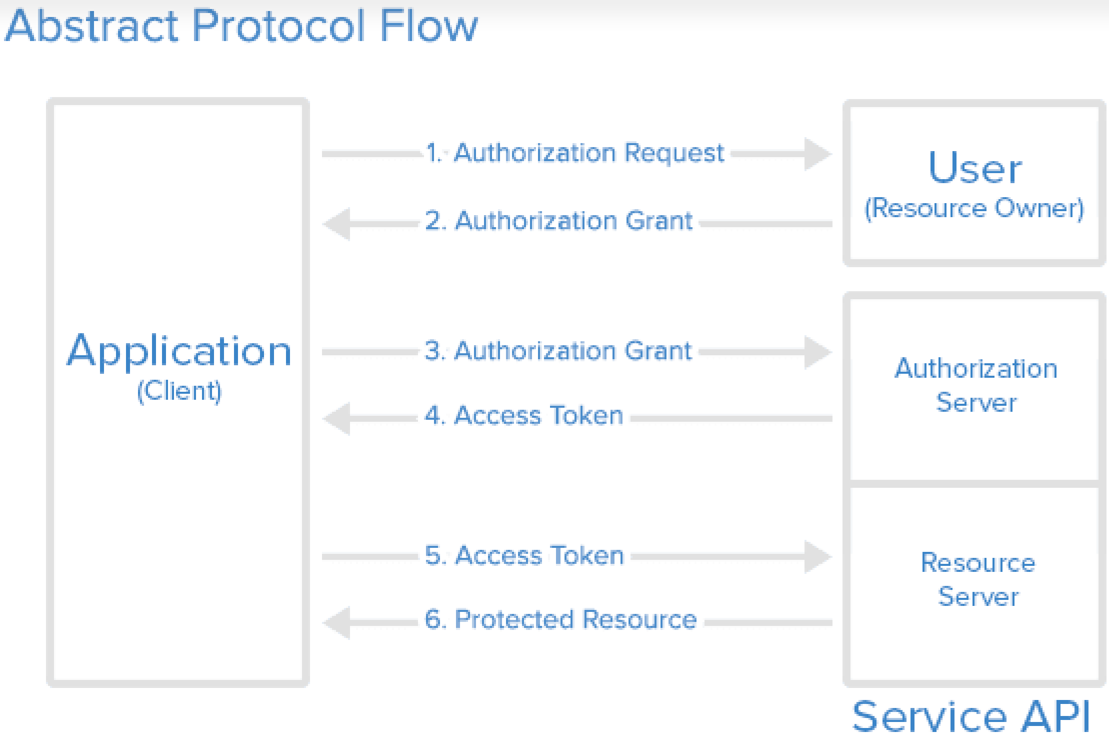


Source

Oauth 2

OAuth 2 is an authorization framework that enables applications to obtain limited access to user accounts on an

1. Application requests authorization for access service resources from the user.
2. If that user approves then the application receives an authorization grant.
3. Application requests an access token from the authorization server (API). This is done by presenting its identity and the authorization grant.
4. If the application identity is authenticated and the authorization grant is valid, the API issues an access token to the application. Authorization is complete.
5. The application requests the resource from the API and presents the access token for authentication.
6. If the access token is valid, the API serves the resource to the application.



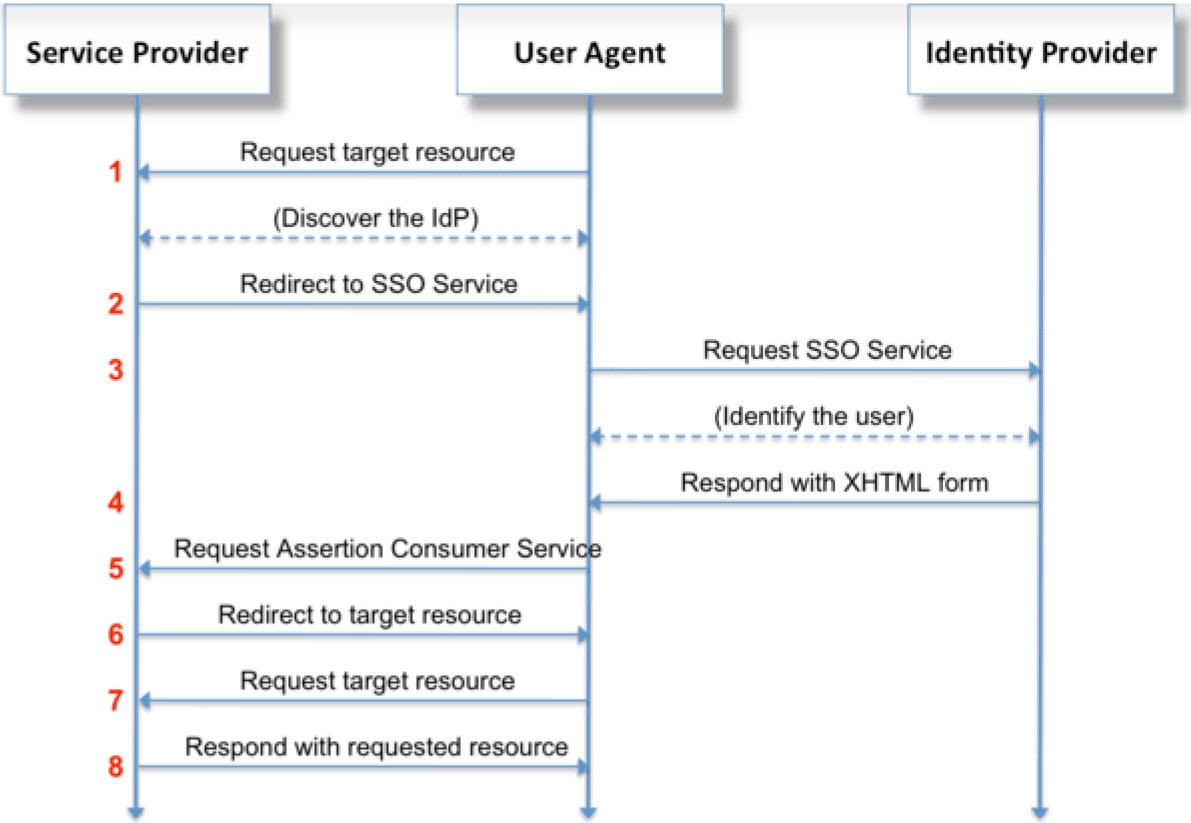
Source: Digital Ocean

SAML

Security Assertion Markup Language (SAML) 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.

JumpCloud is one of the best Single Sign-On (SSO) providers which supports SAML authentication protocols. JumpCloud's SSO provides SAML integrations with 700 popular business applications (including Kisi) and automated user lifecycle management features like Just-in-Time (JIT) provisioning and SCIM provisioning/deprovisioning.

1. User accesses remote application using a link on an intranet or similar and the application loads.
2. Application identifies user's origin (by application subdomain, user IP address, or similar). It redirects the user back to the identity provider, asking for authentication.
3. User either has an existing active browser session with the identity provider or establishes one by logging into the identity provider.
4. Identity provider builds authentication response in the form of an XML-document containing user's username or email address. This is then signed using an X.509 certificate and then posted to the service provider.
5. Service provider (which already knows the identity provider and has a certificate fingerprint) retrieves authentication response and validates it using certificate fingerprint.
6. The identity of the user is established, and the user is provided with app access.



Source

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.

RADIUS authentication begins when the user requests access to a network resource through the Remote Access

Then the RADIUS server checks the accuracy of the information by employing authentication schemes to verify the data. This is done by comparing the user-provided information against a locally stored database or referring to external sources such as Active Directory servers.

The RADIUS server will then respond by accepting, challenging or rejecting the user. Individual users may be granted restricted access without affecting other users. In the case of a challenge, the RADIUS server requests additional information from the user to verify their user ID - which may be a PIN or a secondary password. In the case of a reject, the user is unconditionally denied all access to the RADIUS protocol.

Source

So which one to choose?

LDAP, Kerberos, OAuth2, SAML, and RADIUS are all useful for different authorization and authentication purposes and

The protocol you choose should reflect your application needs and what existing infrastructure is in place. It helps to choose a simple and standardized solution that avoids the use of workarounds for interoperability with native applications. This is why SAML is a good choice as it integrates with JumpCloud's SSO and 700 popular business applications.

If you're looking for more SSO-related content, you can check our guide on how to decide which type of single sign-on you can use.

Relevant Links

- Physical Security Assessment | Best Practices & Audit Process
- What is IoT - Definitions from Industry Experts
- Identity Access Management (IAM) Tools

Bernhard Mehl

Bernhard is the co-founder and CEO of Kisi. His philosophy, "security is awesome," is contagious among tech-enabled companies.

Before: Types of Physical Security Threats

Next: How to Avoid a Demagnetized Key Card or Key Fob

Related Articles

How to Avoid a Demagnetized Key Card or Key Fob

June 10, 2018

Physical Security Conferences for 2020

July 26, 2019

Hacking HID with Wiegand Protocol Vulnerability

December 04, 2018

Products

Product Overview

Kisi Reader Pro

Kisi Controller

Mobile and Keycards

Management Software

Learn More

Company

Support

Contact

Press

(+1) 646 663 4880

kisi

Cookies Privacy Terms GDPR DPA