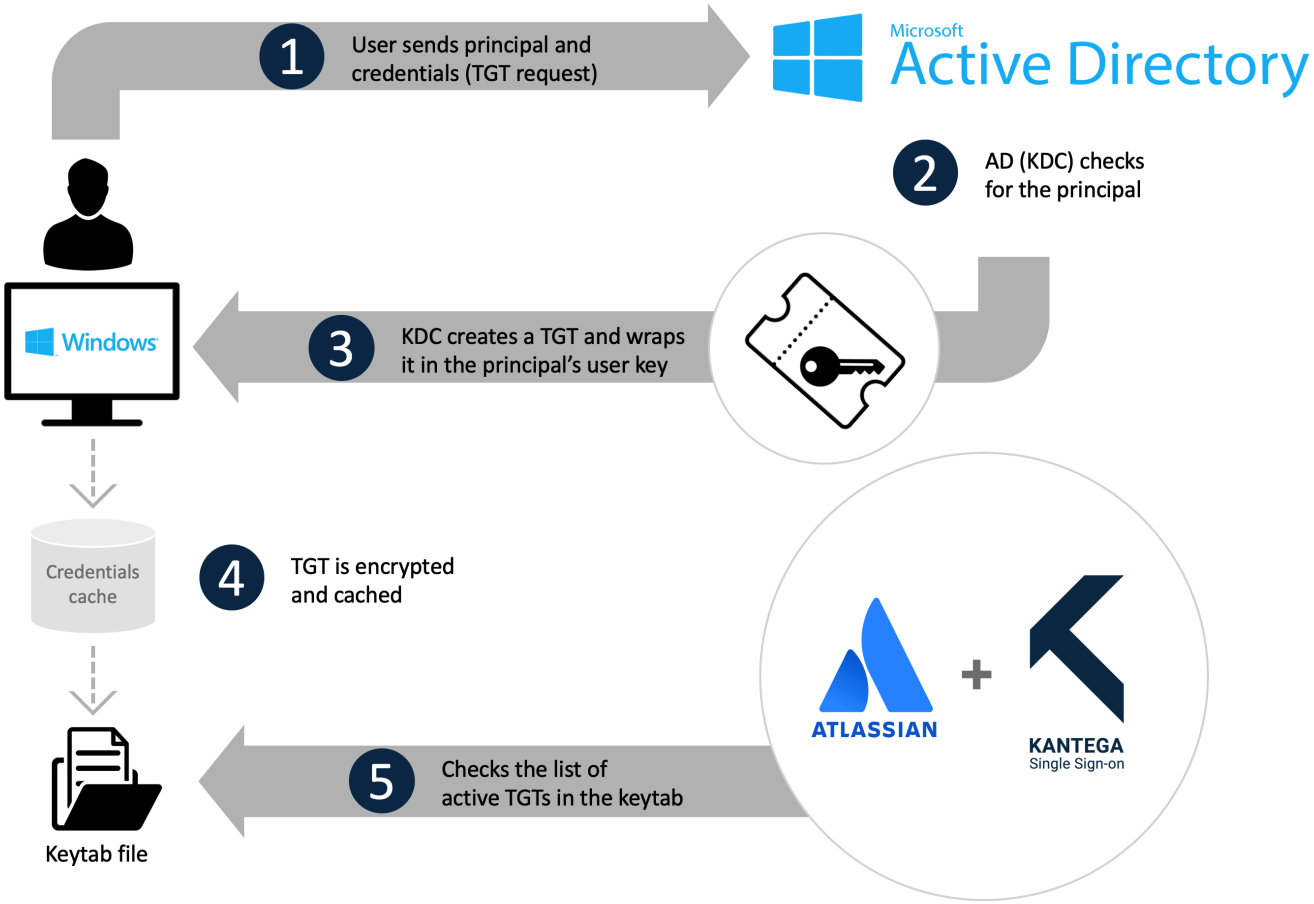
How Kerberos works

When Kerberos is set up in the Kantega Single sign-on add-on it will upon first visit from a browser send a request to the browser if a Kerberos ticket is availabe. Then, if the browser is Kerberos enabled and runs in a Kerberos enabled environment (this is often, but not always a Windows environment), the browser will request it's operating system for a Kerberos ticket for the given web site. The web site is during this request identified against Active Directory or other KDC (Key Distribution Center) using the site's canonical name (the DNS A record). The KDC names this identity as service principal name.



The KDC will then in cooperation with the operating system generate a valid Kerberos ticket for the web site and send this back to the browser. The browser will send the ticket back to the web site and the Kantega Single sign-on add-on will pick up the ticket and verity it's validity against the Keytab file. The Keytab file was earlier extracted from the KDC and installed in the Kantega Single sign-on add-on and is to be considered a certificate to approve each Kerberos ticket signed by the KDC.

If the Keytab file is outdated, the Kerberos ticket will not match it's signature, and login will be aborted. The character of the Kerberos ticket is that it's size in kilobytes will increase when the user has been given many roles/access groups in the KDC. It's size may get up to 20-30 kilobytes or more. Since the way the Kerberos ticket is transferred is in the HTTP headers of the web page request, the maximum header size of the involved web servers running the web site must often be increased. This involves increasing the header size of the Atlassian product's built in Tomcat web serer and also eventual reverse proxies used for instance to terminate SSL. The Web Server Test under the Kerberos tab in the Kantega Single sign-on add-on will analyze if header size is set up correctly and give advice if neccesary on how to increase this for some common web servers.

Before you configure your environment for Kerberos, it might also be useful to know how browser users are authenticated using Kerberos:

Is Kerberos supported by the browser?

First, the browser decides if Kerberos should be enabled for the given site. See our browser configuration guide.

If Kerberos is not enabled in the browser, you'll see the normal username / password dialog instead.

Determining the Canonical Host Name

Your browser needs to determine the canonical DNS name of your site.

If **issues.example.com** is an A record, then that is also the canonical name of the site.

However, issues.example.com can also be a CNAME alias to a different host, say server123.example.com. In that case, **server123.example.com** is the canonical name of the site.

Forming the Service Principal Name of the site.

The Service Principal Name (SPN) of a site is always "HTTP/" + canonical host name + "@" + REALM.

The Realm is the Active Directory domain name, in dot-separated, uppercase format, e.g **EXAMPLE.LOCAL**

With the canonical name **issues.example.com**, and a realm of **EXAMPLE.LOCAL**, the Service Principal Name is:

HTTP/issues.example.com@EXAMPLE.LOCAL

Acquiring a Kerberos service ticket

Your browser now sends a request to Active Directory, asking for a service ticket for HTTP/issues.example.com@EXAMPLE.LOCAL

Active Directory performs a search in the @EXAMPLE.LOCAL domain for an account with a servicePrincipalName attribute of HTTP/issues.example.com

If only a single account is found with this SPN, then a service ticket is issued to the client

Verifying the service ticket

The browser wraps the Kerberos service ticket in an SPNEGO packet and sends it to the site as an HTTP header.

Our add-on decodes, parses and verifies the service ticket against the configured keytab file.

If the Kerberos ticket is valid, the user name is extracted, an account is looked up in the product using any configured User Directories and the user is logged in.

Advanced note: The user name inside the Kerberos ticket is usually on the format *sAMAccountName@domain*, so for a user Mark Miller, this could be for instance *marmil@example.local*.
If your users are in Microsoft Active Directory, and you have set up this user directory using userPrincipalName as the User Name Attribute (e.g. *mark.miller@example.com*), then we will look up user's userPrincipalName from AD using the *sAMAccountName* from the Kerberos ticket. This will also make Kerberos login work when the User Name Attribute is userPrincipalName.