TP authentification Kerberos (complément théorique)

Objectifs

Comprendre le fonctionnement du mécanisme d'authentification Kerberos

- Authentification
- SSO

1. Présentation

Kerberos est un protocole d'authentification réseau, qui présente la particularité d'allier à la fois sécurité et confort d'utilisation. Il s'agit d'un système d'authentification unique (SSO, Single Sign On). A l'image du mécanisme CAS (Central Authentification Service) assurant un service similaire pour les services web, Kerberos permet de mutualiser et déporter l'authentification pour l'accès à de multiples services.

Il s'appuie sur un mécanisme de clés secrète (chiffrement symétrique) et l'utilisation de tickets (et non de mots de passes) pour accéder aux services.

Il évite ainsi le risque liés à l'utilisation de mots de passes et à la compromission de ces derniers.

2. Historique

Kerberos a été développé par le MIT dans les années 80 alors que le standard à l'époque était d'utiliser les systèmes de login et mot de passe.

Il a été adopté par Microsoft à la sortie de son système Windows 2000 et est utilisé depuis lors par les serveurs Active Directory pour assurer l'authentification au sein des domaines.

3. Fonctionnement global

Kerberos fait intervenir 4 acteurs :

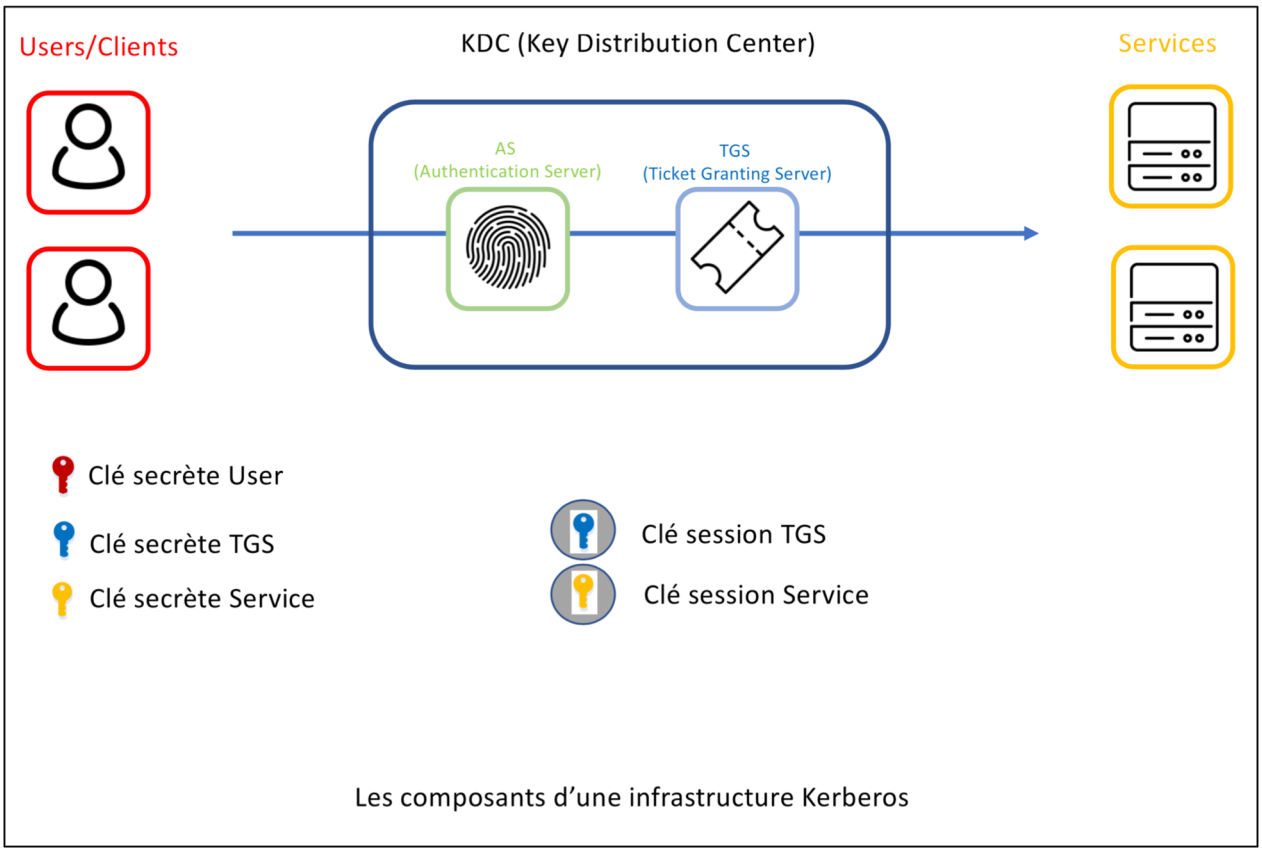
- Le serveur d'authentification (Authentication Server) ;
- Le serveur de ticket (Ticket Granting Server) ;
- Le client (désirant accéder à un service) ;
- Le service (auquel veut accéder le client et dont l'accès est protégé par Kerberos).

L'AS (Authentication Server) et le TGS (Ticket Granting Server) sont regroupés au sein du KDC (Key Distribution Center).

Au préalable de toute authentification il va falloir enregistrer/créer les utilisateurs désirant bénéficier utiliser Kerberos au niveau de l'AS. L'AS dispose donc dans une base de données, pour chaque utilisateur enregistré, un hash des mots de passe des utilisateurs (appelé Clé Secrète Utilisateur ou encore Secret User Key).

De même tout service désirant faire reposer son authentification sur l'infrastructure Kerberos devra au préalable également s'être enregistré au niveau du TGS. Le TGS dispose donc également dans une base de données, pour chaque service enregistré, une clé symétrique partagée (appelé Clé Secrète Service ou encore Secret Service Key).

Ces secrets (clés symétriques) ayant été partagées et enregistrées par les protagonistes, l'usage de Kerberos pour l'authentification sera alors possible.



Les composants d'une infrastructure Kerberos

Un client (enregistré au niveau du KDC, plus précisément au niveau de l'AS) qui désire accéder à un service dont l'authentification repose sur Kerberos (et enregistré au niveau du KDC, plus précisément du TGS) sera lors de sa tentative de connexion initiale au service, redirigé vers le serveur AS qui se chargera de son authentification et sollicitera ensuite le TGS (en lui envoyant un TGT (Ticket Granting Ticket) afin que celui-ci crée un ST (Service Ticket) permettant ensuite au client d'accéder au service désiré et à d'autres par la suite sans avoir besoin une nouvelle fois de s'authentifier.

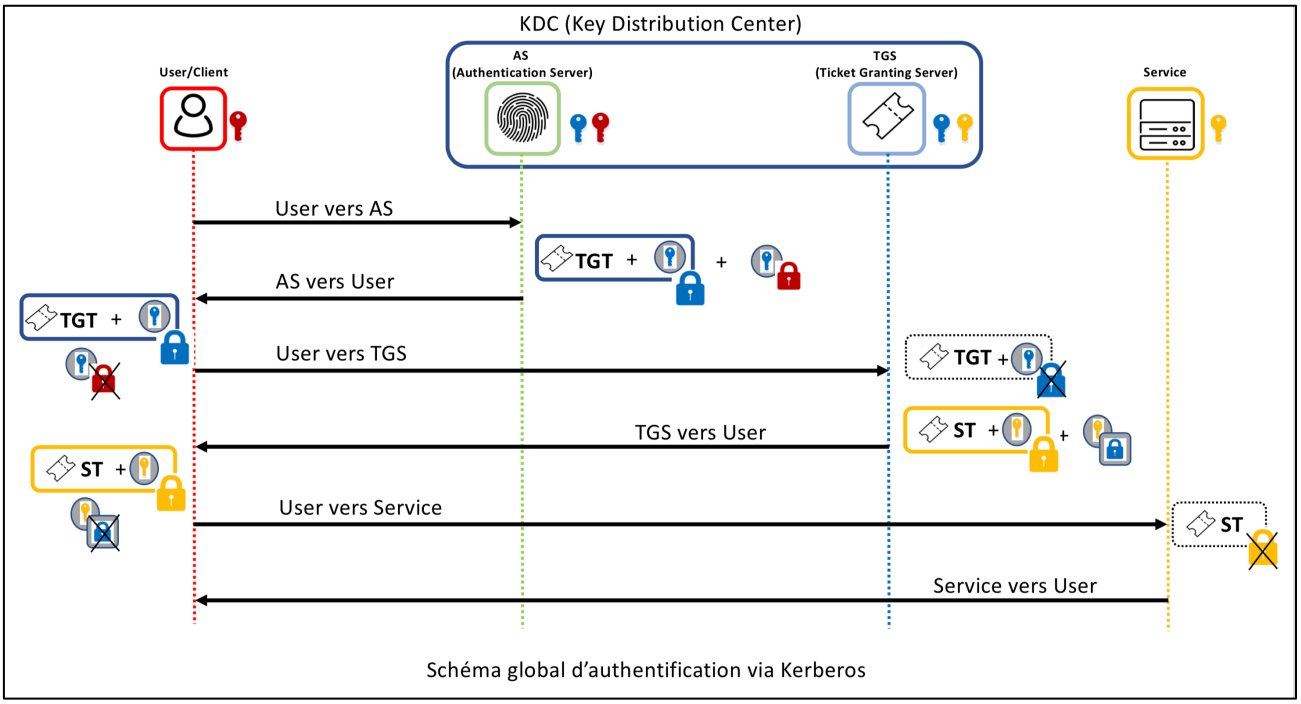


Schéma global d'authentification via Kerberos

4. Fonctionnement détaillé

a. Dialogue entre le client et l'AS (authentication Server)

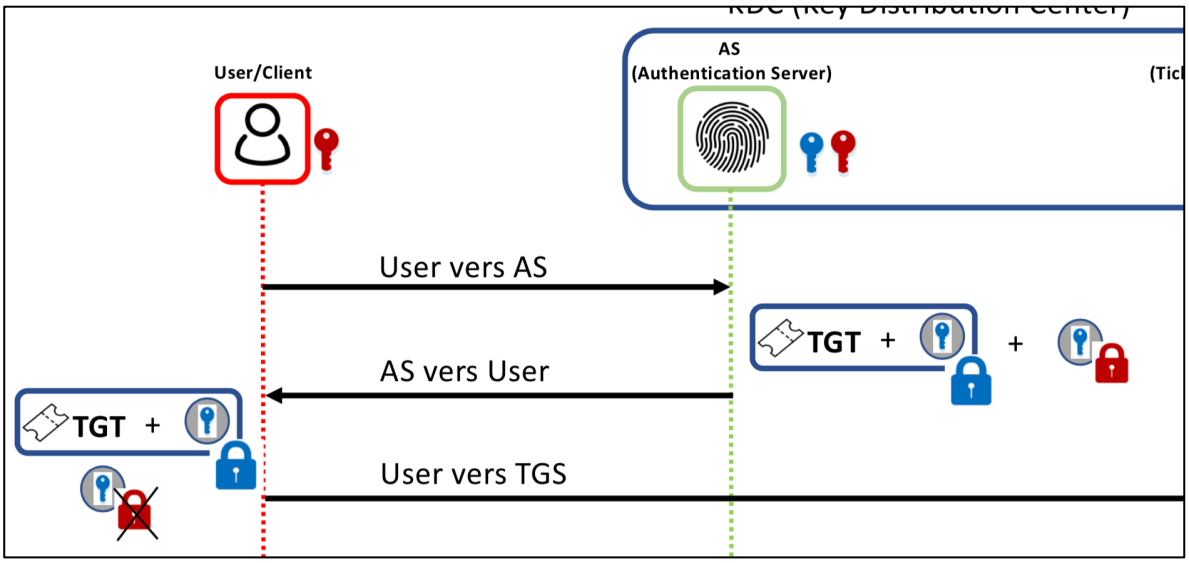


Figure 1 : dialogue client - serveur d'authentification

Le client envoie une requête en clair à l'AS comportant son nom d'utilisateur (user/id) dans le domaine, le nom du service auquel il désire accéder, sa propre adresse IP et enfin une estampille temporelle (timestamp) :
- User/id ;
- Service Name ;
- User IP address ;
- Timestamp ;

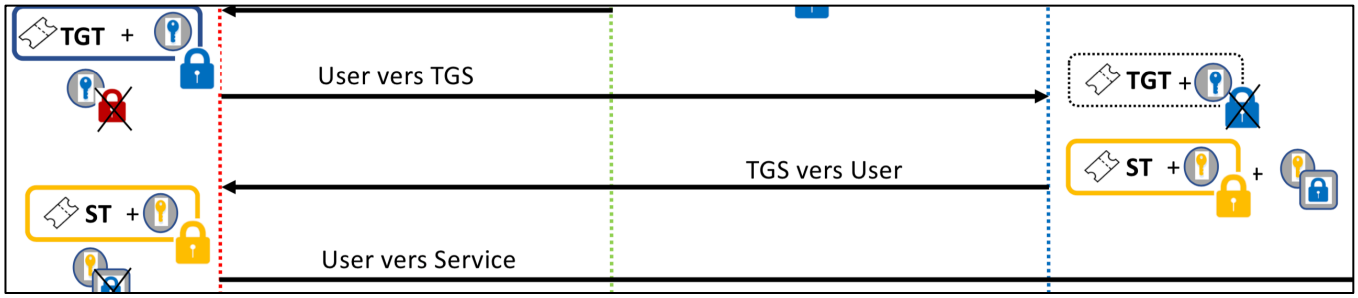
L'AS vérifie la présence du client dans sa base de données, l'adresse IP du client.
Il utilise la **clé secrète user** (de l'utilisateur) afin de chiffrer symétriquement (avec AES) une partie de sa réponse contenant notamment **la clé de session TGS** (partie-1) :
- TGS Name ;
- Timestamp ;
- Lifetime ;
- Clé de session TGS.

L'AS fabrique également un TGT (Ticket Granting Ticket) qu'il chiffre symétriquement (avec AES) en utilisant cette fois **la clé secrète TGS** et envoie le tout au client (partie-2) :
- User/id ;
- TGS Name/id ;
- Timestamp ;
- @IP User ;
- Lifetime pour le TGT ;
- Clé de session TGS.

A réception de la réponse de l'AS, le client/utilisateur déchiffre la partie-1 grâce à sa propre clé symétrique (**clé secrète user)** afin de récupérer **la clé session TGS** (qu'il conserve précieusement). Ce déchiffrement s'il fonctionne permet d'assurer indirectement l'authentification du client/user par le serveur AS. Seul le client disposant de **sa clé secrète user** (de l'utilisateur) est en mesure de le faire.

b. Dialogue entre le client et le TGS (Ticket Granting Server)

Le user/client/utilisateur envoie alors le TGT qu'il a reçu de l'AS (sans le modifier, car il ne dispose pas de **la clé secrète TGS** pour accéder à son contenu) et le fait parvenir au TGS. Il utilise également **la clé de session TGS** reçue de l'AS pour chiffrer son User/id et l'envoyer au TGS (Ticket Granting Server).



A réception du TGT le serveur TGS (Ticket Granting Server) annule l'opération de chiffrement symétrique qui protège le contenu du TGT grâce à **la clé secrète TGS** dont il dispose.

Le serveur TGS vérifie la présence dans ses bases d'une association client/service et si c'est le cas produit un ST (server ticket) qu'il protège/chiffre avec **la clé secrète du service final**.

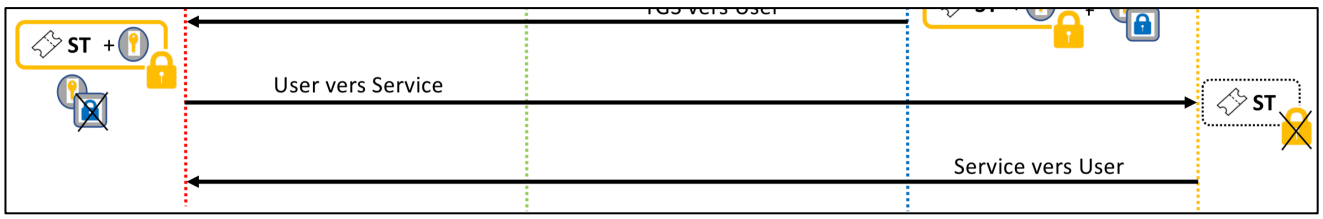
Le serveur TGS génère également une **clé de session service** qu'il inclue dans le ST protégé. Il chiffre **cette clé de session service** avec **la clé de session TGS** et envoie le tout au user/client.

A réception de la réponse du TGS, le client/utilisateur déchiffre **la clé de session service** (qu'il conserve précieusement) en utilisant **la clé de session TGS**.

Le client/user n'est pas en mesure de déchiffrer le ST (Service ticket) car il ne dispose pas de **la clé secrète service**

c. Dialogue entre le client et le service

Enfin pour finir, le client envoie le ST (server ticket) au service. Celui-ci accède au contenu du ST en le déchiffrant **avec sa clé secrète service**.



Le service dispose alors de la clé de session service.

Le service effectue les dernières vérifications de validité du client/use pour accéder à son service grâce au ST (Service Ticket) auquel il accorde une totale confiance.

d. Bilan

A l'issue de l'opération nous avons chaque protagoniste qui a pu vérifier la légitimité de chacun. Le client dispose d'une clé de session TGS (secret partagé) avec le TGS. Le client dispose également d'une clé de session service (secret partagé avec le service).

Tous les protagonistes sont ainsi authentifiés les uns auprès des autres et peuvent se faire confiance.

Les clés de session temporaires garantissent la propriété de « forward secrecy ». Ainsi l'éventuelle compromission des clés secrètes n'affectera pas la confidentialité qui sera garantie par l'usage des clés de session.

Le rejeu des tickets est empêché par à un mécanisme de cache au niveau TGS, du client et du service qui qui gardent mémoire respectivement à leur niveau du ST (pour le client) de l'association user et service (pour le

En cas de connexion à un nouveau service protégé par le service Kerberos (dans un temps raisonnable), l'échange entre le client et l'AS donnant lieu à la création d'un TGT ne sera pas nécessaire. Le client pourra utiliser ST (Service Ticket) précédent.