# Introduction

Kerberos est un protocole d’authentification créé en 1988 par le M.I.T. Il est utilisé pour vérifier l’identité d’un utilisateur ou d’un hôte. Kerberos communique en UDP, par défaut, sur le port 88. L’authentification se repose sur un mécanisme de tickets et de clés secrètes, qui est un chiffrement symétrique.

# Fonctionnement

Dans un réseau utilisant Kerberos, plusieurs entités sont présentes :

* **Le client** (C) : Détient une clé secrète (KC).
* **Le serveur (S) :** Détient **une clé secrète (KS).**
* **Le centre de distribution des clés : *Key Distribution Center* (KDC) en anglais, propose deux services :**
  + **Le service d’émission de tickets : *Ticket-Granting Service* (TGS) en anglais, détient une clé secrète (KTGS) et connait la clé secrète du serveur (KS).**
  + **Le service d’authentification : *Authentication Service* (AS) en anglais, connait la clé secrète du client (KC) et du service d’émission des tickets (KTGS).**

**Lorsqu’un utilisateur souhaite s’authentifier avec le service Kerberos pour accéder à un service proposé par un serveur, celui-ci doit respecter les étapes suivantes :**

* **Le client envoie une requête au service d’authentification (AS).**
* **Le service d’émission de tickets (TGS) envoie au client une réponse avec les éléments suivants :**
  + **Une clé de session (KC, TGS) entre le client et le service d’émission de tickets chiffrée avec la clé secrète du client (KC).**
  + **Un ticket (TTGS) chiffré avec la clé secrète du service d’émission de tickets (KTGS). Ce ticket permet au client de faire d’autres requêtes au service d’émission de tickets. Il contient les éléments suivants :**
    - **Le nom et l’adresse du client.**
    - **La période de validité du ticket envoyé au client.**
* **Le client envoie une requête au service d’émission de tickets avec les éléments suivants :**
  + **Le ticket du service d’émission de tickets (TTGS).**
  + **Un message chiffré avec la clé de session du service d’émission de tickets (KC, TGS). Ce message contient les éléments suivants :**
    - **La date d’émission de la requête.**
    - **Le nom du client.**
* **Le service d’émission de tickets envoie au client une réponse avec les éléments suivants :**
  + **Une clé de session entre le client et le serveur (KC, S) chiffrée avec la clé de session entre le client et le service d’émission de tickets (KC, TGS).**
  + **Un ticket (TS) chiffré avec la clé secrète du serveur (KS).**
* **Le client envoie une requête au serveur avec les éléments suivants :**
  + **Le ticket du serveur (TS)**
  + **Un message chiffré avec la clé de session entre le client et le serveur (KC, S). Ce message contient les éléments suivants :**
    - **La date d’émission de la requête.**
    - **Le nom du client.**
* **Le serveur vérifie la validité de la requête en déchiffrant le ticket avec sa clé secrète (KS). Si celle-ci est valide, alors il permet au client d’accéder à ces ressources**

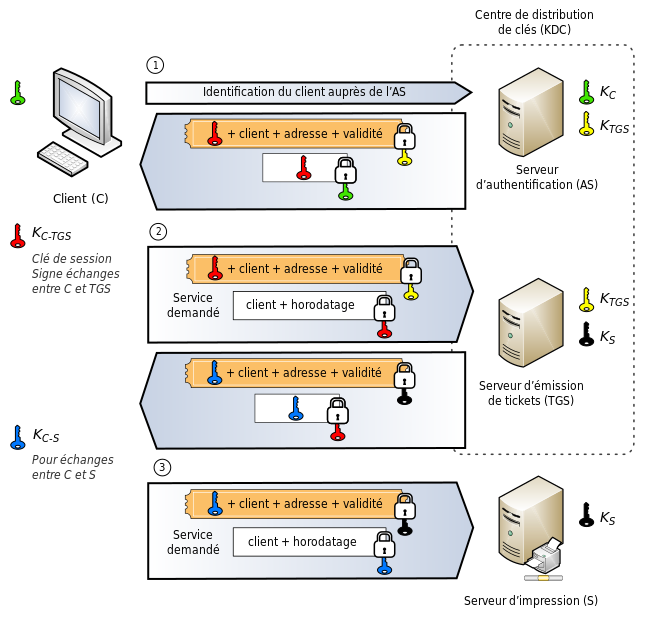


Illustration 1: Fonctionnement de Kerberos

La clé secrète Kerberos est le mot de passe du compte utilisateur par défaut "krbtgt" qui est désactivé par défaut, mais qui ne doit donc pas être supprimé.

Documentation :

* <https://learn.microsoft.com/fr-fr/windows-server/security/kerberos/kerberos-authentication-overview>

# Mise-à-jour de la clé secrète

Le compte Kerberos a un historique avec les deux clés secrètes les plus récentes, il est donc important de changer cette clé deux fois de suite de façon à supprimer l’ancienne clé de l’historique.

Cependant, il est important d’attendre la période maximale de validité d’un ticket Kerberos entre deux changements de clé. Par défaut la période maximale de validité d’un ticket Kerberos est de 10 heures, mais il est conseillé d’attendre trois jours pour permettre aux contrôleurs de domaine de répliquer les modifications.

Il est donc recommandé de modifier la clé secrète Kerberos tous les 40 jours à 6 mois maximum.

Documentation :

* <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-reset-the-krbtgt-password>