Introduction à Kerberos

Jean-Marc Pouchoulon Octobre 2023

Kerberos

- Décrit comme « a secure , SSO, trusted third party mutual authentification service »
  - **Secure** : Pas de mot de passe en clair échangés sur le réseau
  - **SSO**: On s'authentifie une fois et avec ce ticket on peut aller sur de multiples hosts ou service
  - **Trusted third Party**: Un client, Un serveur, Un KDC , chaque partenaire s'authentifiant. La sécurité repose sur le KDC qui est le nœud névralgique

kerberos

- Basé sur la cryptographie a clef symétrique.
- Conçu pour internet , pensé donc pour des réseaux non sécurisés.
- Développé au MIT, il existe aussi aussi une flaveur Heimdal et une autre Active Directory: Le monde windows aussi utilise ce protocole aussi et donc son intérêt est de fournir une solution de masse à large spectre.
- Très utilisé dans le monde Unix ? Il faut kerberiser les applications et l'époque est aux applis web...
- Néanmoins une solution intéressante pour les services orientés systèmes et réseaux.

Vocabulaire Kerberos

- Principal : un participant dans une interaction, identifiable de manière unique – utilisateur, hôte, service
- Chaque principal est associé à une clef unique
- Ces clefs sont stockées dans le KDC ou dans un fichier keytab
- Un principal est unique , et sa représentation est de la forme user/instance@DOMAINEKERBEROS (Case Sensitive, le domaine Kerberos en majuscule)

Ex: root/admin@IUTBEZIERS.FR

nfs/machine1.iutbeziers.fr@IUTBEZIERS.FR

host/machine1.iutbeziers.fr@IUTBEZIERS.FR

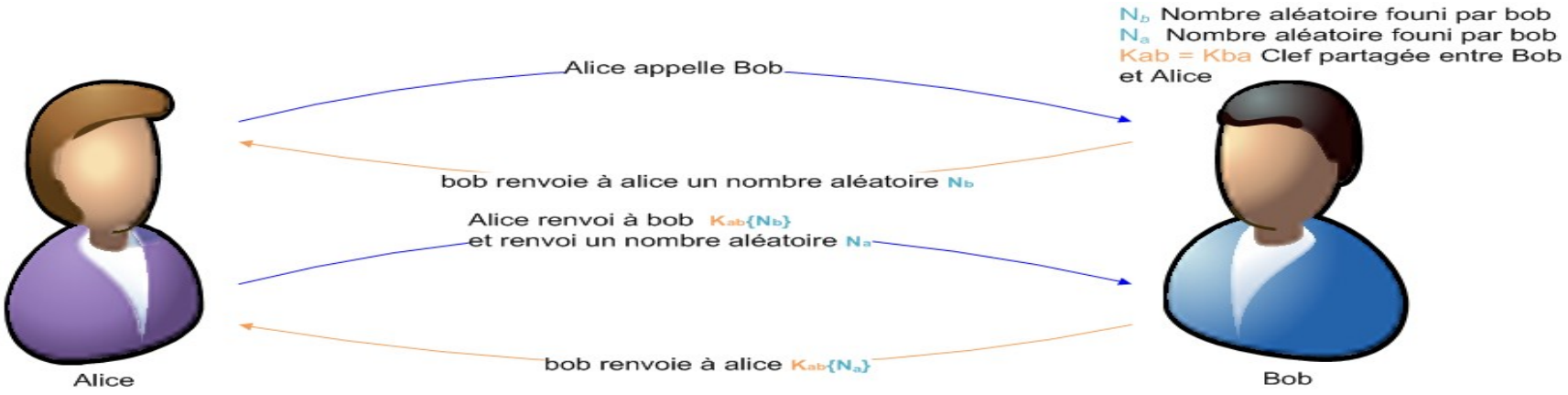
Vocabulaire Kerberos

- Authentification : action de prouver qu'un Principal est vraiment l'entité qu'il prétend être.
- Autorisation : action de déterminer quelles actions un principal peut effectuer dans un contexte donné

Vocabulaire Kerberos

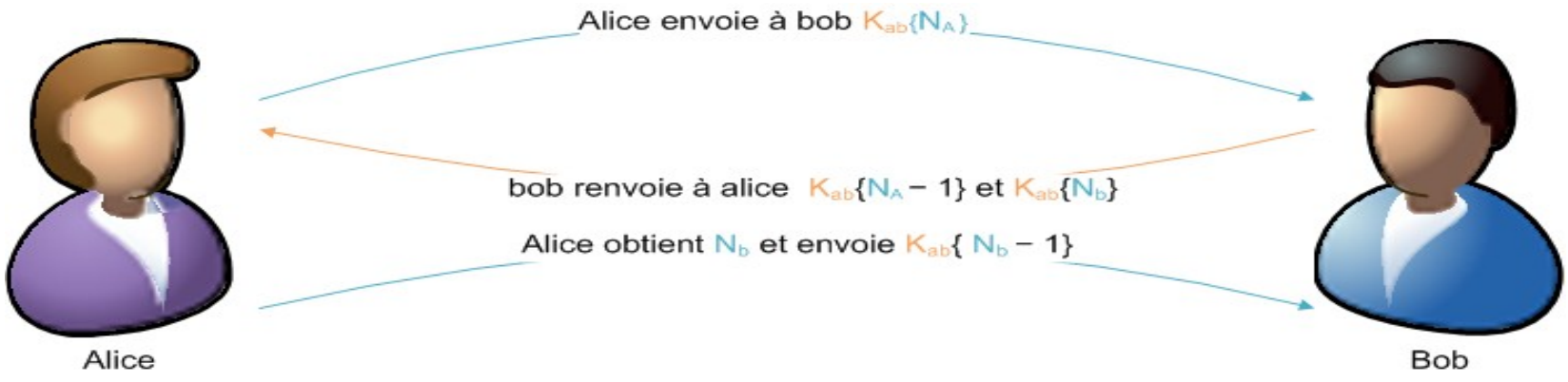
- Realm/royaume kerberos: C’est une entité logique sur lequel les principals (machines , services , utilisateurs) vont s’authentifier.
- Il peut y avoir approbation entre plusieurs royaumes (domaines AD) soit de façon directe par partage d’une clef secrète, soit de façon transitive (hiérarchie DNS par exemple).
- Chaque Royaume a son Key Distribution Center

Principe du secret partagé



Alice décrypte N_B puisqu'elle connait Kab et s'authentifie auprès de Bob et réproquement.

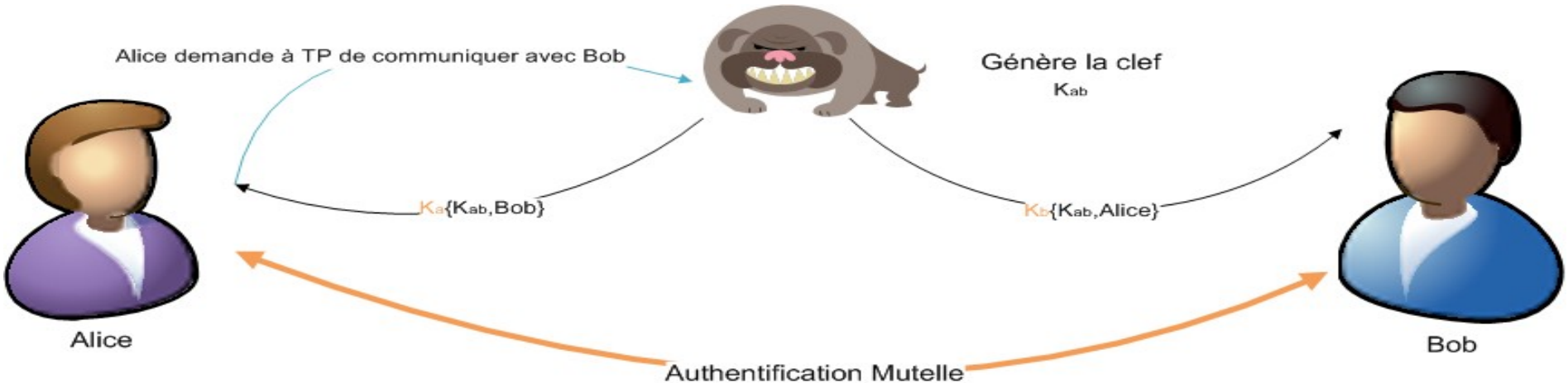
variante


Alice envoie à bob $K_{ab}\{N_A\}$
bob renvoie à alice $K_{ab}\{N_A - 1\}$ et $K_{ab}\{N_b\}$
Alice obtient N_b et envoie $K_{ab}\{N_b - 1\}$
Alice
Bob

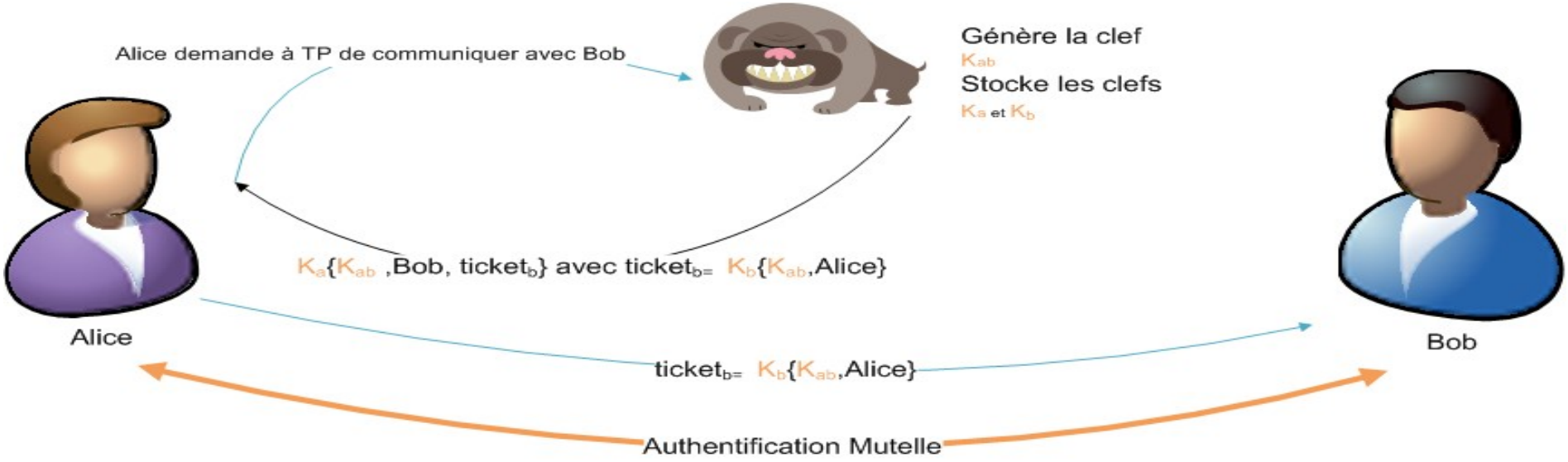
Généralisation difficile

- La généralisation à m utilisateurs et n services, implique la distribution préalable de m×n clefs partagées.
- On introduit une tierce partie de confiance pour tous les acteurs (c’est notre KDC)

Authentification mutuelle avec tierce partie

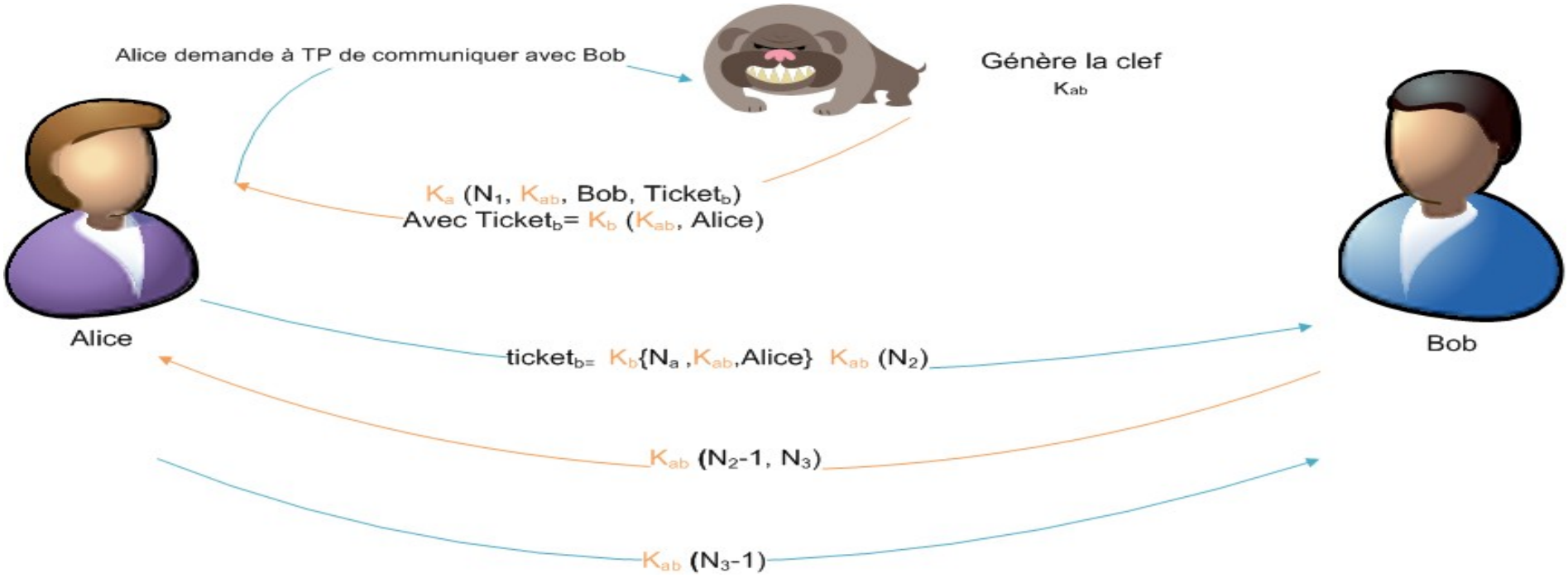


Tierce partie bis



C'est Alice qui envoie deux tickets (on évite de surcharger la Tierce Partie)
K_b n'est pas connu d'Alice et donc elle ne peut rien faire sauf renvoyer le ticket

protocole de Needham et Schroeder



Deux parties dans le serveur Kerberos

- Le service d'authentification (**AS** pour Authentication Service)
- Le générateur de ticket de service (**TGS** pour Ticket Granting Service)
- Kerberos introduit l'utilisation de timestamps à la place des nombres aléatoires ce qui nécessite de synchroniser par NTP les serveurs.

Authentification Service dans le détail

Une demande de **TGT** est en fait une demande d'accès au service **TGS**. Le **TGT** est donc *le ticket du service* **TGS.**

L'**AS**

- Accepte les requêtes des clients.
- Cree le *Ticket Granted Ticket* qui est basé sur les informations de la requête (Nom du principal pour les clients et les services)
- Génère K_{ab} entre les principaux.

Ticket Granting Service

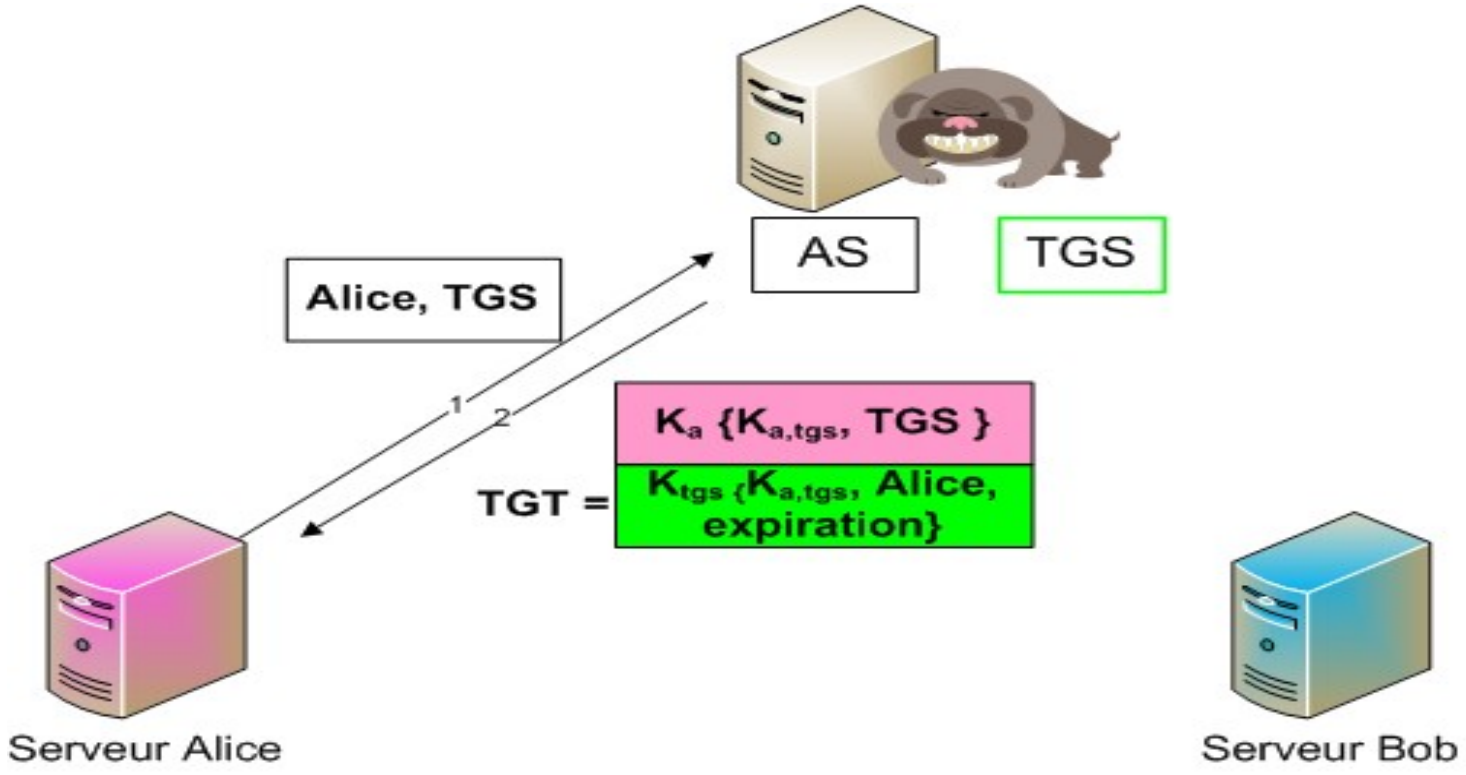
Le **TS** (Ticket Service) pour un service donné (Nfs par

) est envoyé par le TGS sur présentation d'un

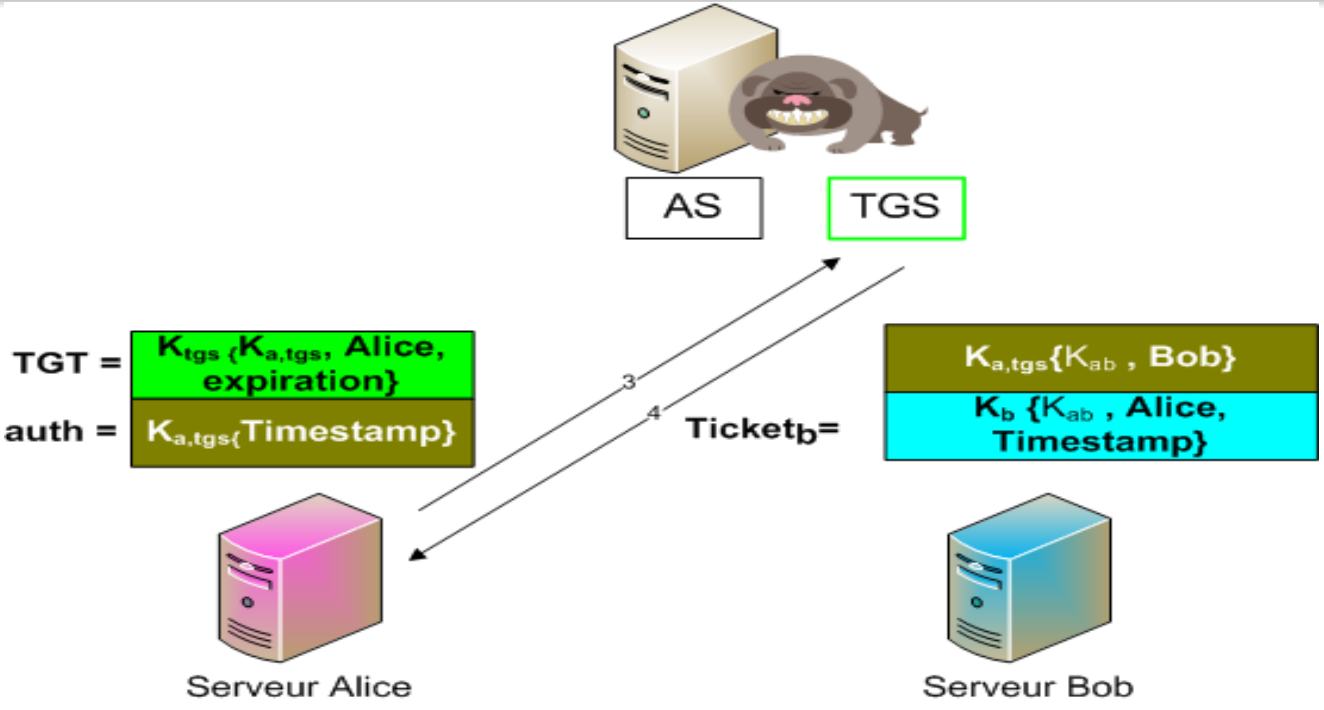
TGT et d'un timestamp chiffré avec la clef de session

$K_{a, tgs}$.

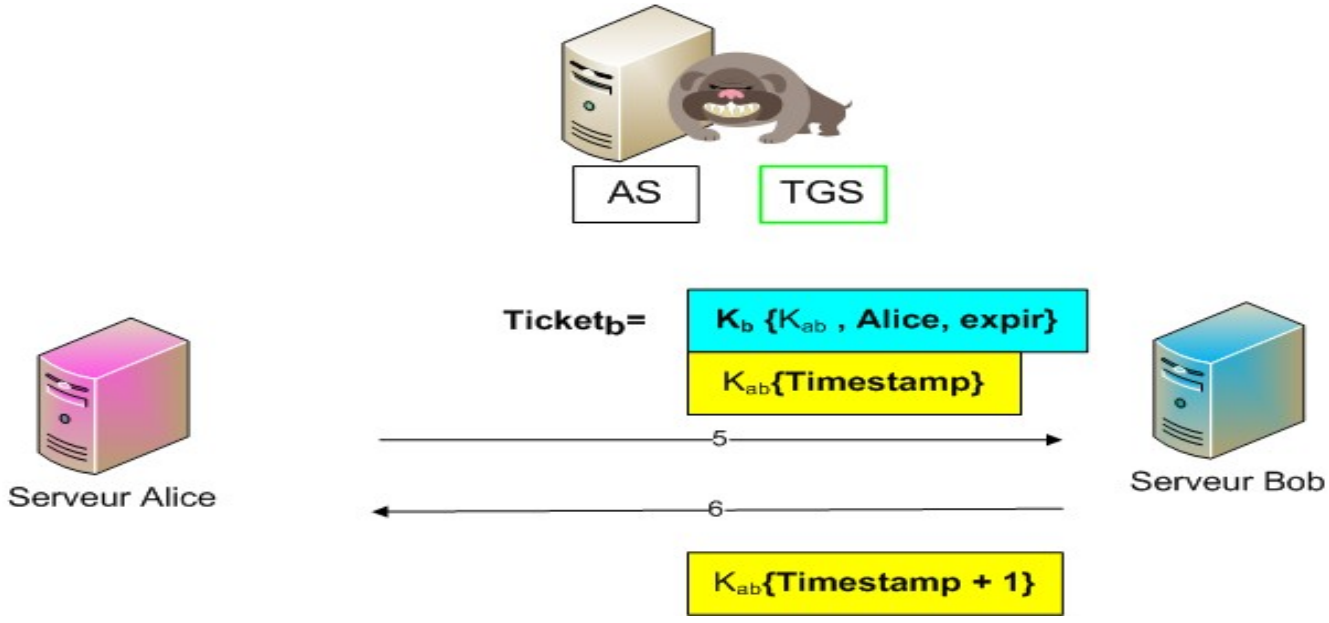
Kerberos accès à l'AS



Kerberos acces au TGS



Kerberos accès au serveur



KDC = AS + TGS

- Le KDC (Key Distribution Center) est chargé de stocker les secrets des principaux et des polices (durée de vie , changement des mots de passes…)
- Pour les utilisateurs on a une clef qui est le résultat d'une fonction de hash du mot de passe. Pour les serveurs ou les services on génère une « randomkey ». Elles sont stockées dans la base de données du KDC
- Un KDC peut être répliqué (en mode batch)
- Un poste client a soit l'adresse du KDC, soit il la trouve dans le DNS via des enregistrements spéciaux.

GSS-API

- Generic Security Services Application Programming Interface. C’est une API permettant de faire de l’authentification entre client et serveur. Son intérêt est de découpler le client des mécanismes sous jacent
- RPCSEC_GSS est bâti au dessus de gss-api , il apporte authentication, intégrité, et encryption (en-têtes signées ,corps RPC signés et encryptés .

(krb5i, krb5p dans lors du mount NFS)