DE LA RECHERCHE À L'INDUSTRIE

Master 2 SeCReTS
Sécurité applicative

Kerberos

www.cea.fr

10 décembre 2017

Introduction et historique

Kerberos & Herakles poterie grecque VIe av JC

- kerberos vient de la mythologie grecque : chien à 3 têtes qui garde l'entrée des enfers
- nom choisi pour le service d'authentification d'un projet du MIT (Massachusetts Institute of Technology) appelé Athena (1983)
- protocole d'authentification réseau
- v1, v2, v3 : versions de developpement
- v4 : 1989
- actuelle : v5, de 1993 (RFC 4120).

Qu'est ce kerberos ?

Basé sur

- Needham et Schroeder "Using Encryption for Authentication in Large Networks of Computers" (1978)
- Denning et Sacco "Time stamps in Key distribution protocols" (1981).

Kerberos permet l'authentification des utilisateurs et des services sur un réseau

Qu'est ce kerberos ?

Particularités de *Kerberos*

- Part de la supposition que le réseau peut être non sûr
  - Les données sur le réseau peuvent êtres lues ou modifiées
  - les adresses peuvent être faussées
- Utilise une tierce partie de confiance
  - Toutes les entités du réseau (utilisateurs et services) font confiance à cette tierce partie
- utilise des mécanismes de chiffrement basés sur des algorithmes à clefs **symétriques**
  - Tous les principaux partagent cette clef secrète avec le serveur kerberos

Intérêts du protocole

- centraliser l'authentification
  - authentification des utilisateurs et des services
- fournir un moyen sûr d'authentification à travers un réseau non-sûr
  - pas de transmission en clair de mots de passe, utilisation de *tickets* pour prouver l'identité
- méthode d'authentification unique (**SSO**)
  - on s'authentifie une seule fois pour accéder à l'intégralité des services *kerberisés*

Implémentations

- MIT
- Heimdal
- Microsoft (Windows 2000)
- MacOS X

Rappels de cryptographie

Chiffrement symétrique

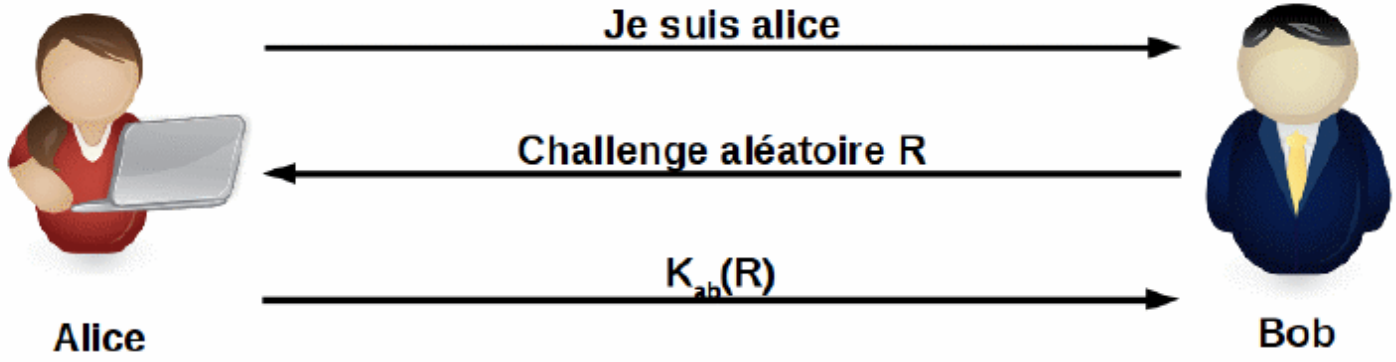
- la même clef est utilisée pour chiffrer et déchiffrer
- exemple : DES, 3DES, AES

Chiffrement asymétrique

- utilisation d'un couple de clefs (publique et privée)
- ce qui est chiffrée par l'une ne peut être déchiffré que par l'autre
- exemple : RSA, DSA

Fonctionnement du protocole

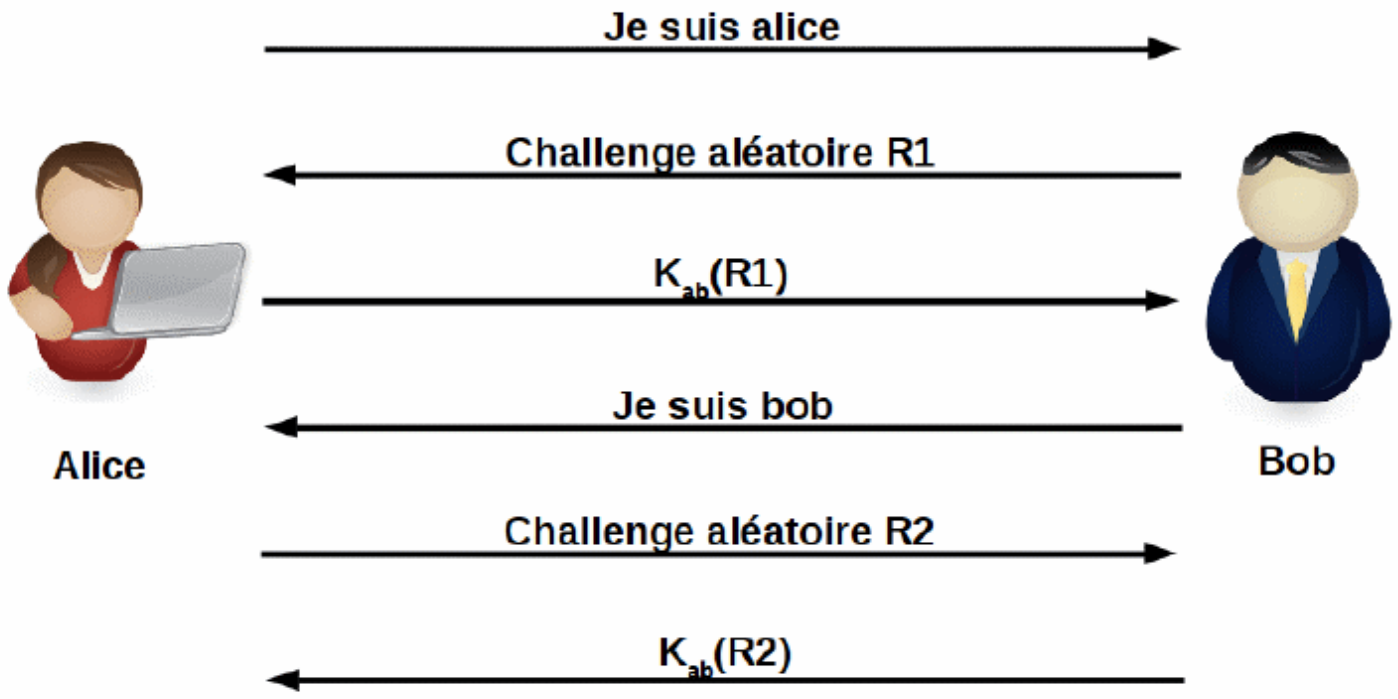
- Authentification à l'aide d'algorithme de chiffrement à clefs secrètes
  - Alice initie la communication : client ou utilisateur
  - Bob : service ou serveur applicatif
  - Alice veut accéder au service Bob.



Authentification de Alice via la clef partagée K_{ab}

Fonctionnement du protocole

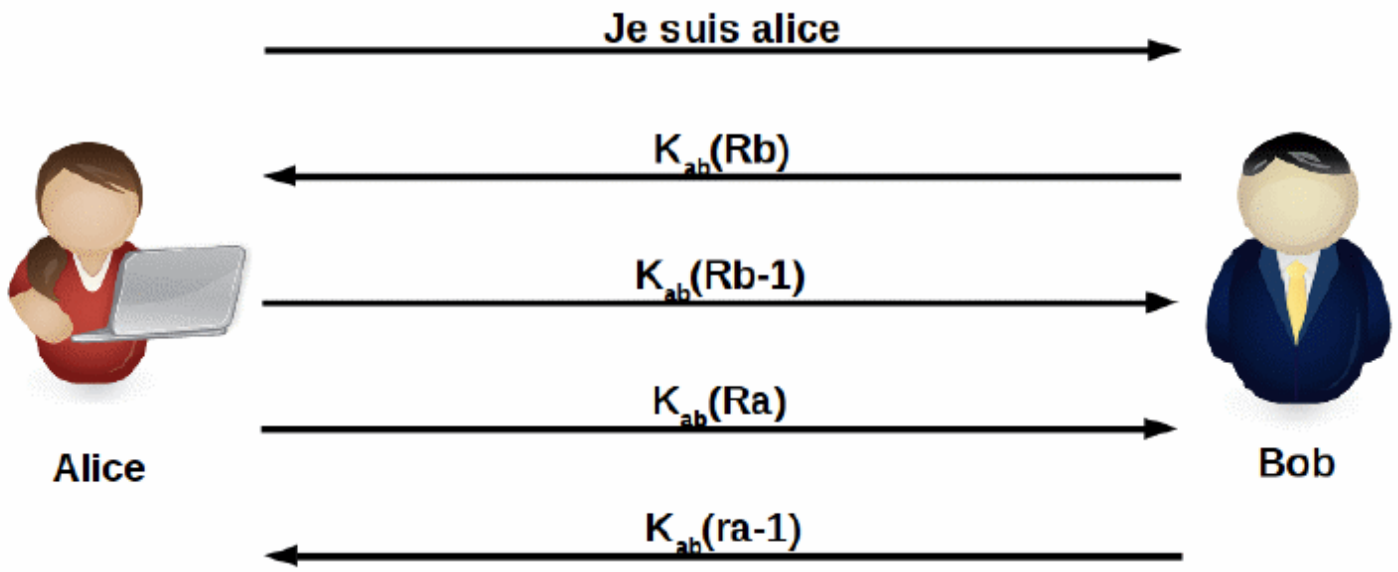
- Authentification mutuelle



Authentification de Alice et Bob via la clef partagée K_{ab}

Fonctionnement du protocole

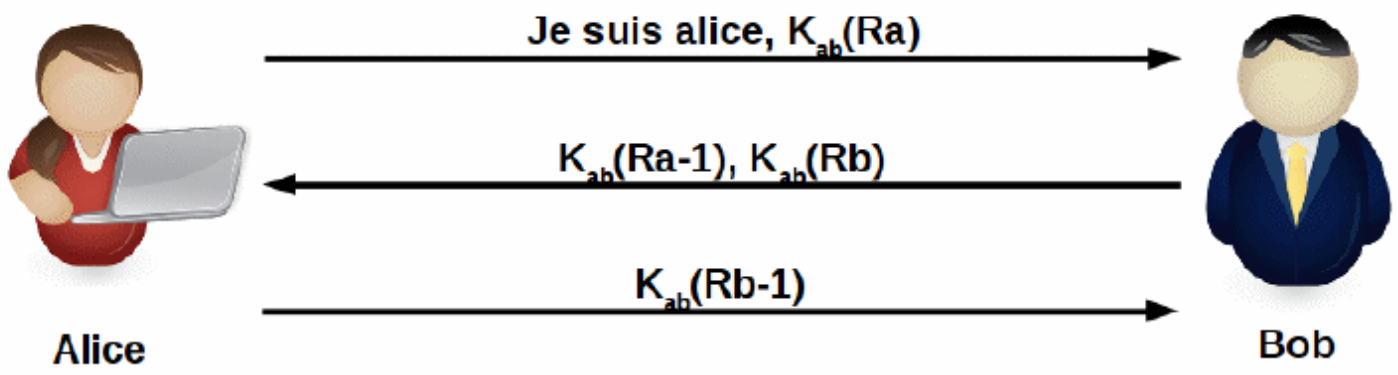
- Authentification mutuelle autre méthode



Authentification de Alice et Bob via la clef partagée K_{ab}

Fonctionnement du protocole

- Authentification mutuelle autre méthode (suite)



Authentification de Alice et Bob via la clef partagée K_{ab}

Fonctionnement du protocole

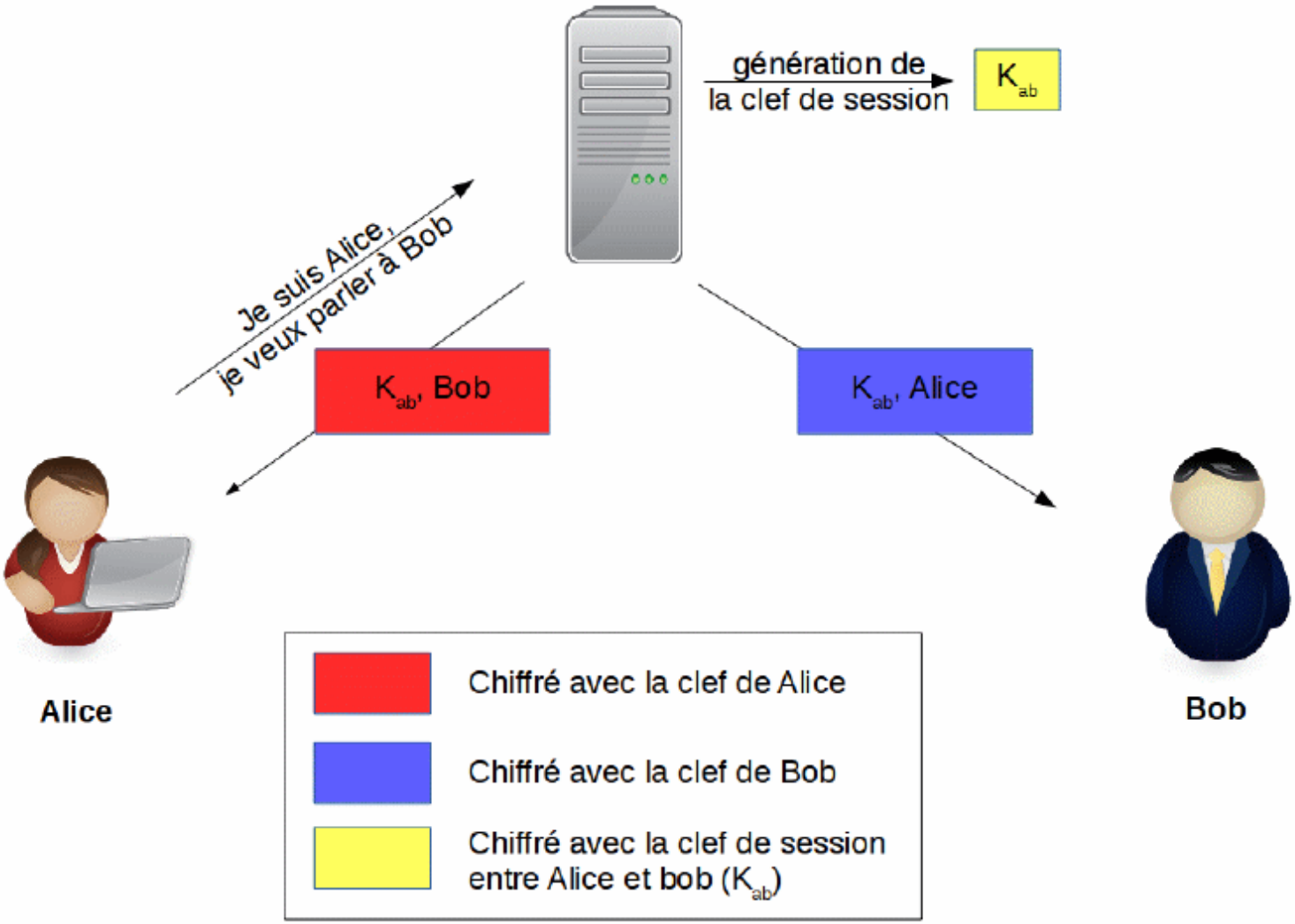
Inconvénients

- peu extensible
- la généralisation à m utilisateurs et à n services implique une distribution préalable de m x n clés partagées

Amélioration possible

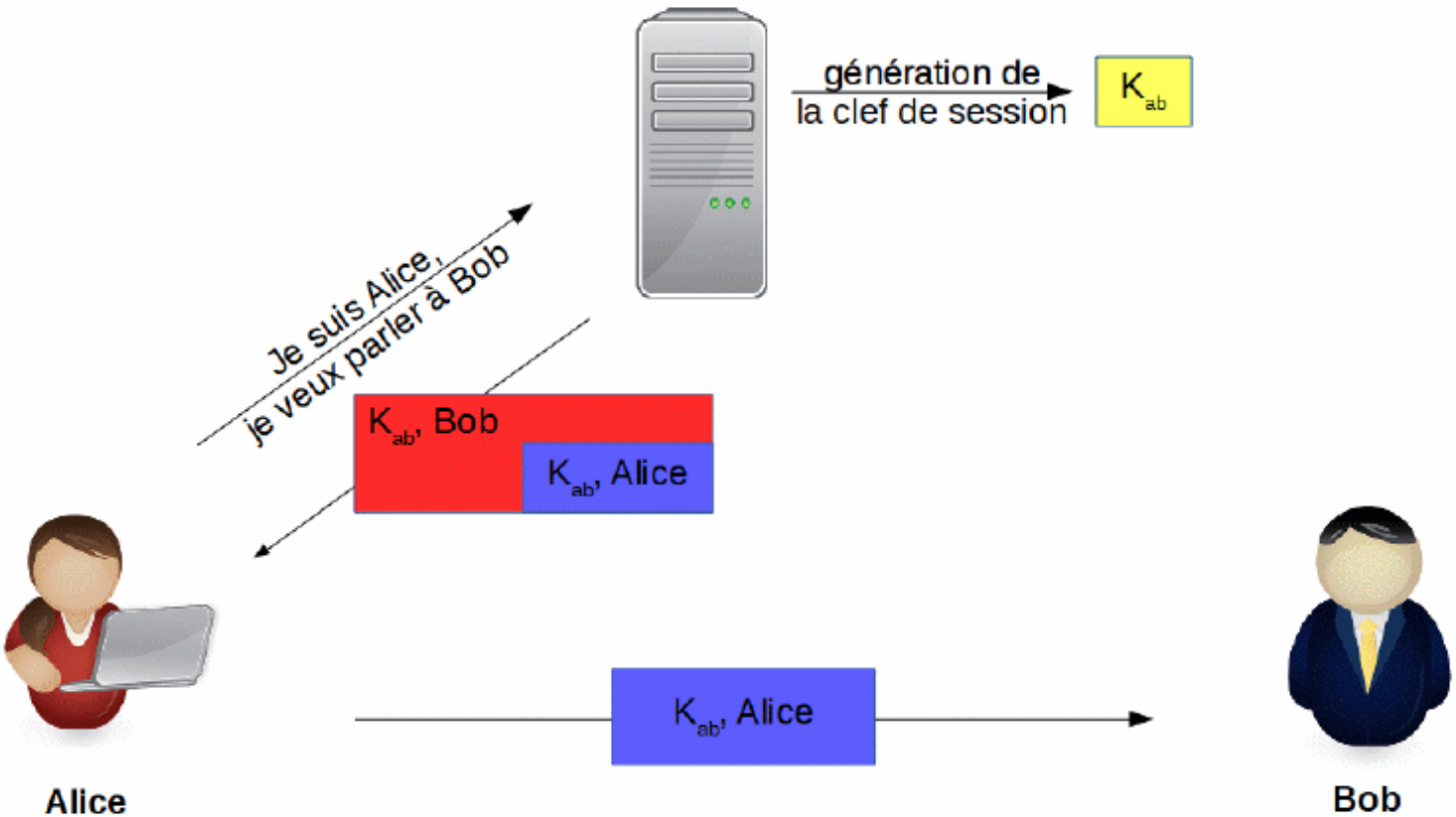
- Utiliser une tierce partie avec laquelle tous les utilisateurs et les services partagent leur clé
- avantages
  - gestion centralisée de compte
  - plus facile de sécuriser une base de clés partagées que plusieurs

Fonctionnement du protocole



Fonctionnement du protocole

- La charge repose sur Alice



Fonctionnement du protocole

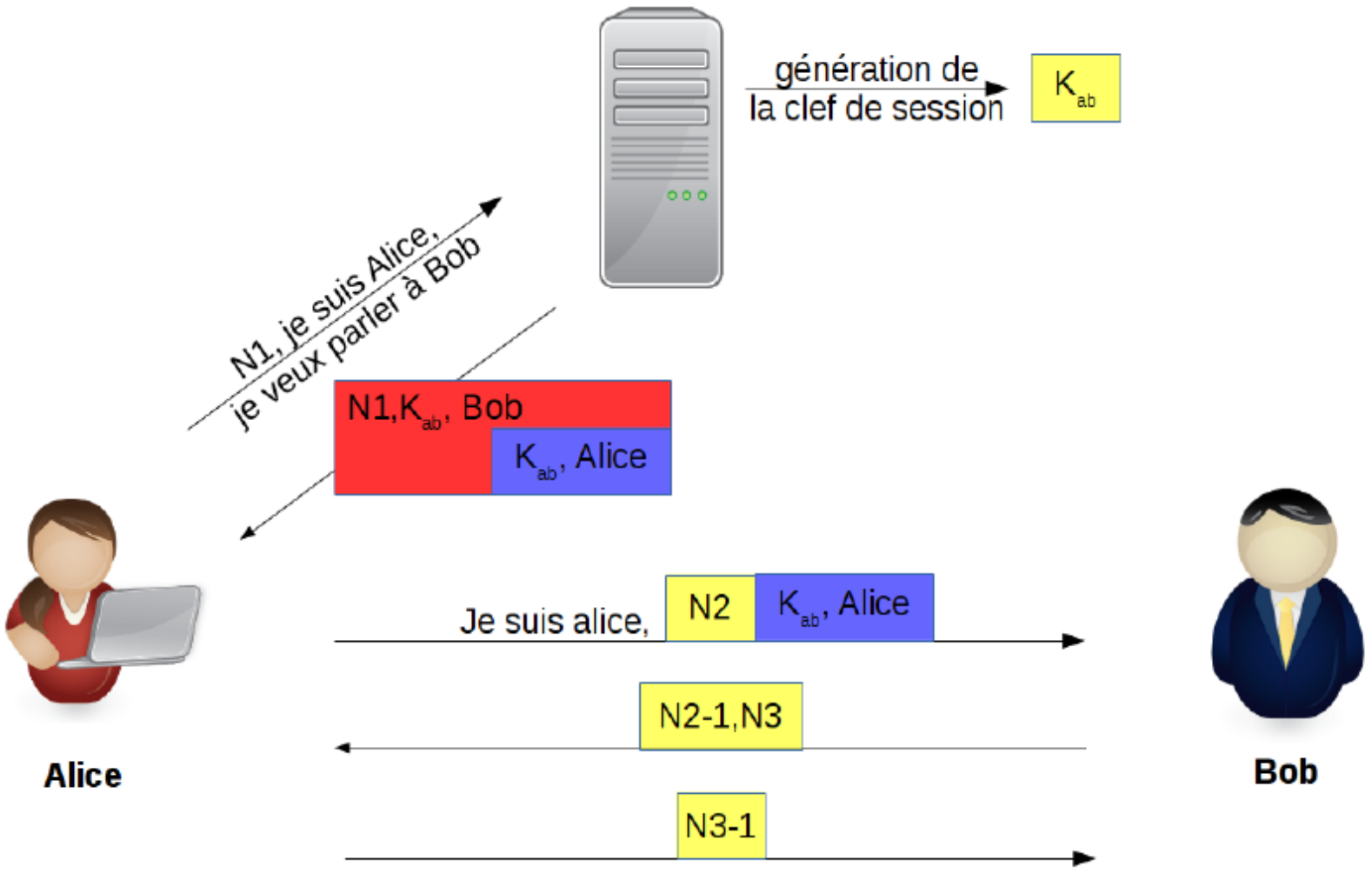
K_{ab}, Alice

Ticket

- Données chiffrées émises par la tierce partie de confiance
- Contient notamment une clef de session unique
- Permet à un utilisateur de s'authentifier auprès d'un service
- Transmet de manière sécurisée :
  - l'identité du client
  - la clef de session partagée par le client et le service.

Fonctionnement du protocole

- Protocole Needham-Schroeder



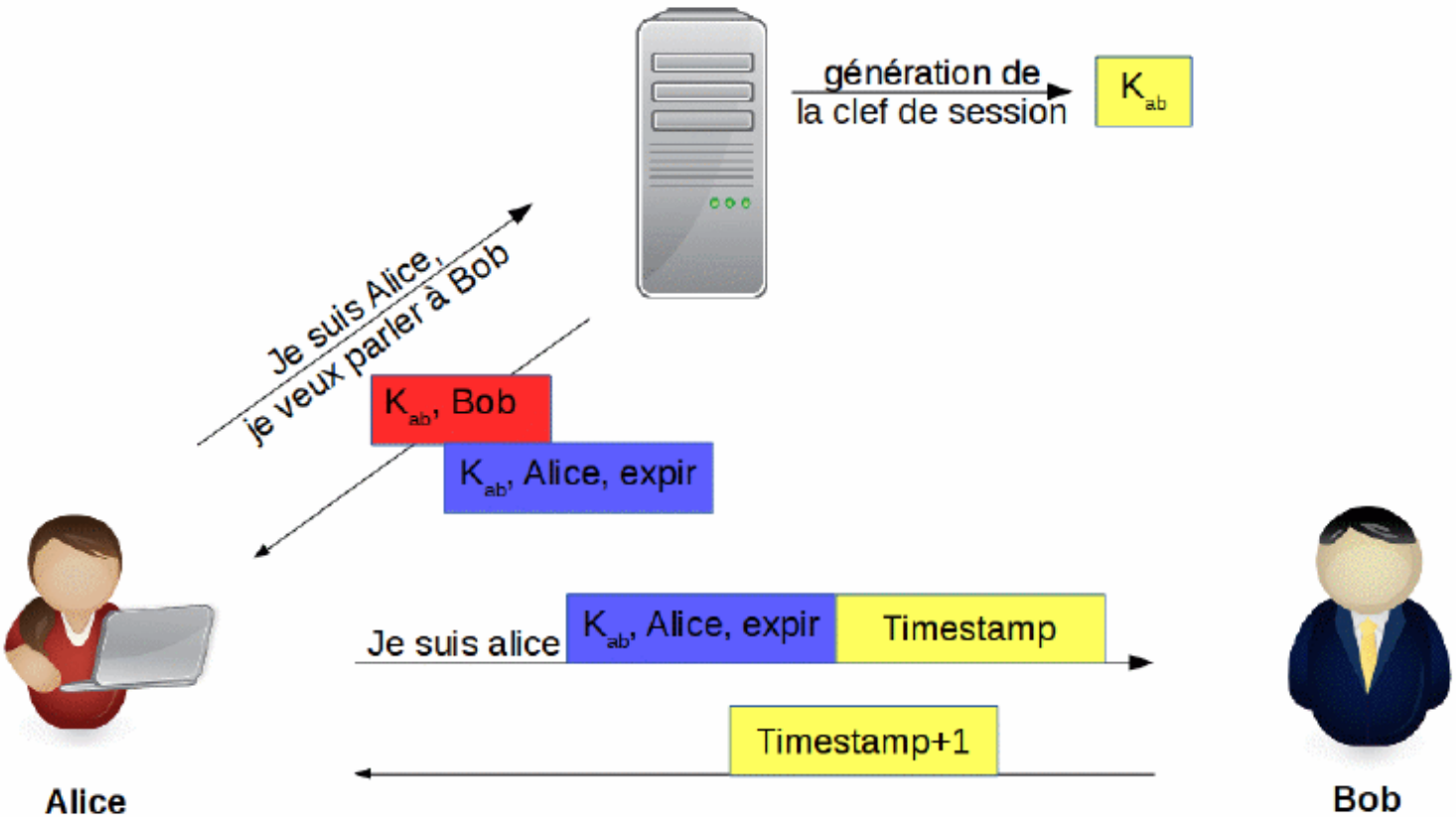
Fonctionnement du protocole

Introduction des timestamps

- utilisés dans la phase d'authentification mutuelle
- introduit les dates d'expiration (limite le rejeu)
- réduit le nombre total de messages dans le protocole
- implique la synchronisation horaire de chaque entité participant à la communication.

Fonctionnement du protocole

- *Kerberos* (presque)



Fonctionnement du protocole

Kerberos utilise ce schéma

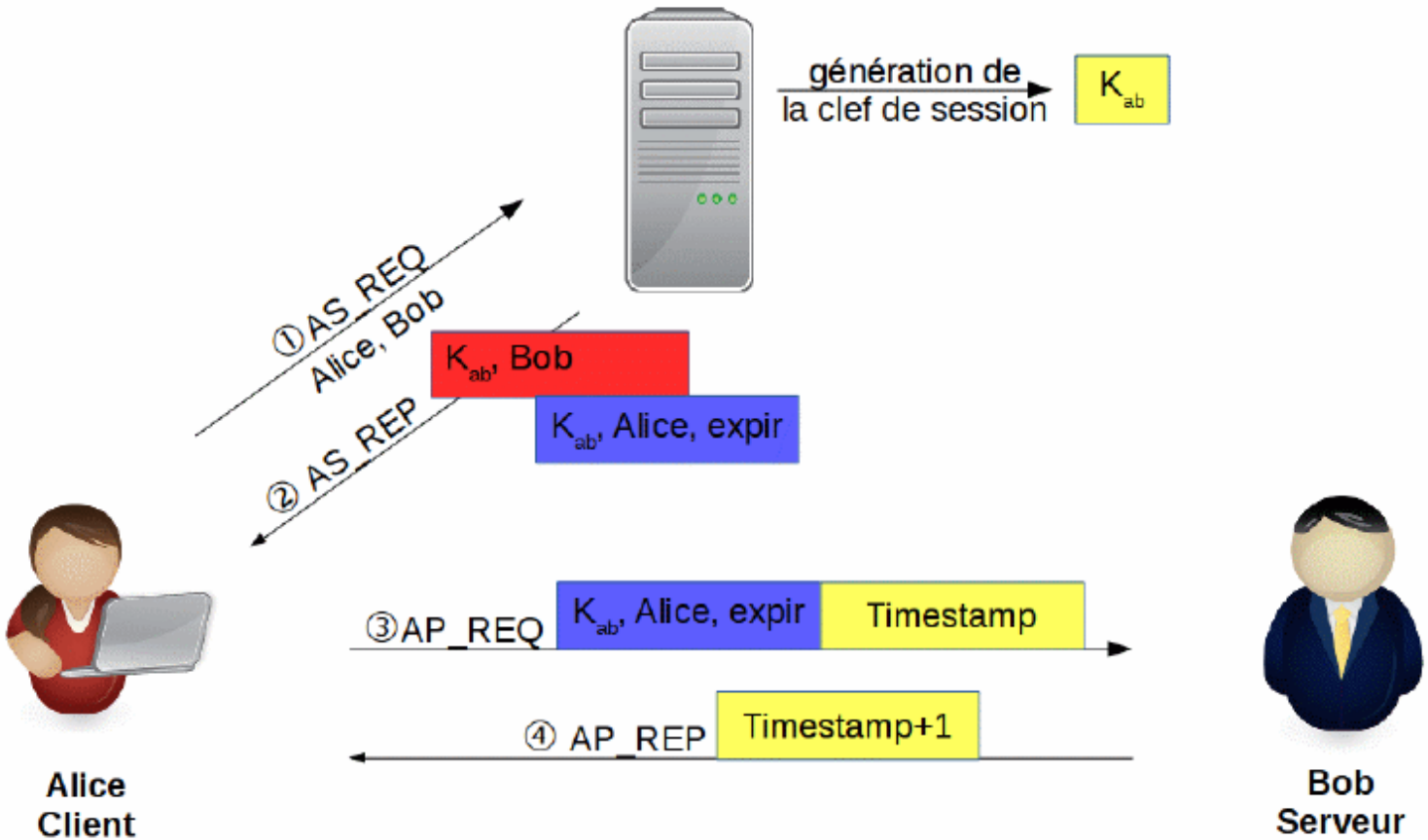
- la tierce partie s'appelle le KDC (Key Distribution Center)
- chaque utilisateur et service partage une clé secrète avec le KDC
- à la demande, le KDC génère une clé de session qu'il distribue de manière sécurisée aux parties communicantes
- les parties communicantes se prouvent réciproquement qu'elles connaissent la clé de session

Remarques

- les parties communicantes doivent avoir confiance dans le KDC
- la clé de l'utilisateur est dérivée du mot de passe par l'utilisation d'une fonction de hachage
- la clé d'un service est un nombre aléatoire stocké sur le serveur.

Fonctionnement du protocole

- Kerberos simplifié



Fonctionnement du protocole

Royaumes et principaux

- un *REALM* correspond au domaine géré et controlé par un serveur Kerberos. Par convention, le *REALM* kerberos correspond au nom du domaine dns en majuscule. Les *REALM* sont sensibles à la *casse*.
- *principal* :
  - chaque entité (utilisateur, ordinateur, service) ont un *principal*
  - un *principal* commence par un nom d'utilisateur (ou le nom d'un service) suivi d'une instance optionnelle. Leurs association est unique pour un royaume (*REALM*) donné
  - pour un service, le *principal* commence par le type de service suivi de son fqdn

Fonctionnement du protocole

Exemples

- bob@UVSQ.ORG
- HTTP/www.uvsq.org@UVSQ.ORG
- krbtgt/UVSQ.ORG@UVSQ.ORG

Plan

- Kerberos

Fonctionnement du protocole

Le KDC se décompose en trois parties

- une base de tous les principaux et leurs clefs de chiffrement associées
- l'*Authentication Server* (AS) :
  - fourni les *Ticket Granting Ticket* (TGT) chiffrés aux utilisateurs qui se connectent au royaume kerberos.
  - Une fois déchiffré, c'est le TGT qui sera utilisé pour prouver son identité
- le *Ticket Granting Service* (TGS) :
  - fourni les tickets de services aux utilisateurs
  - il faut fournir un TGT valide ainsi que le nom du service demandé pour obtenir un ticket de service.

Fonctionnement du protocole

TGS (Ticket Granting Service)

- service situé sur le KDC qui permet à l'utilisateur d'obtenir des tickets de service (TS).

Ticket Granting Ticket (TGT)

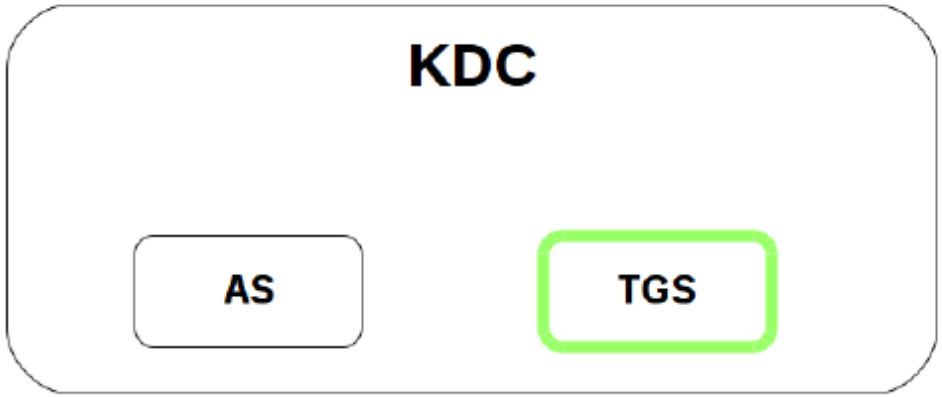
- ticket utilisé pour accéder au TGS et obtenir des tickets de service
- permet l'échange d'un clé de session
- durée de vie limitée
- partagée par l'utilisateur et le TGS
- le TGT et la clé de session pour le TGS sont stockés sur la station de Alice.

Fonctionnement du protocole

Intérêts

- Permet (avec l'option forwardable) le SSO (Single Sign On)
- Limite l'utilisation du mot de passe :
  - moins de données chiffrées avec la clé secrète de l'utilisateur traverse le réseau
  - on limite l'accès aux données susceptibles d'être soumises à des attaque offline par dictionnaire

Fonctionnement du protocole



Alice
Client

Chiffré avec la clef de Alice (K_a)

Chiffré avec la clef de Bob (K_b)

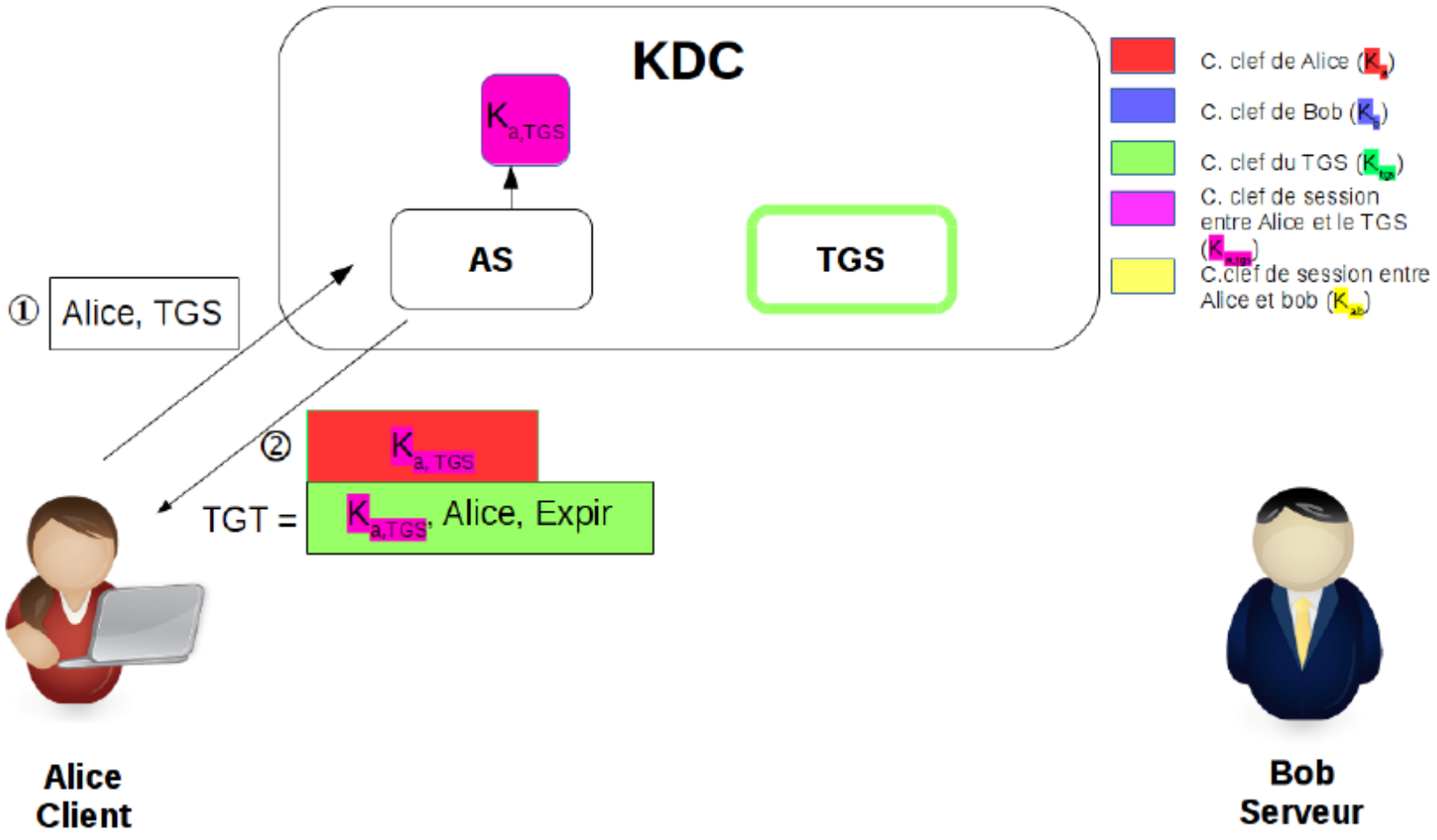
Chiffré avec la clef du TGS (K_{tgs})

Chiffré avec la clef de session entre Alice et le TGS ($K_{a,tgs}$)

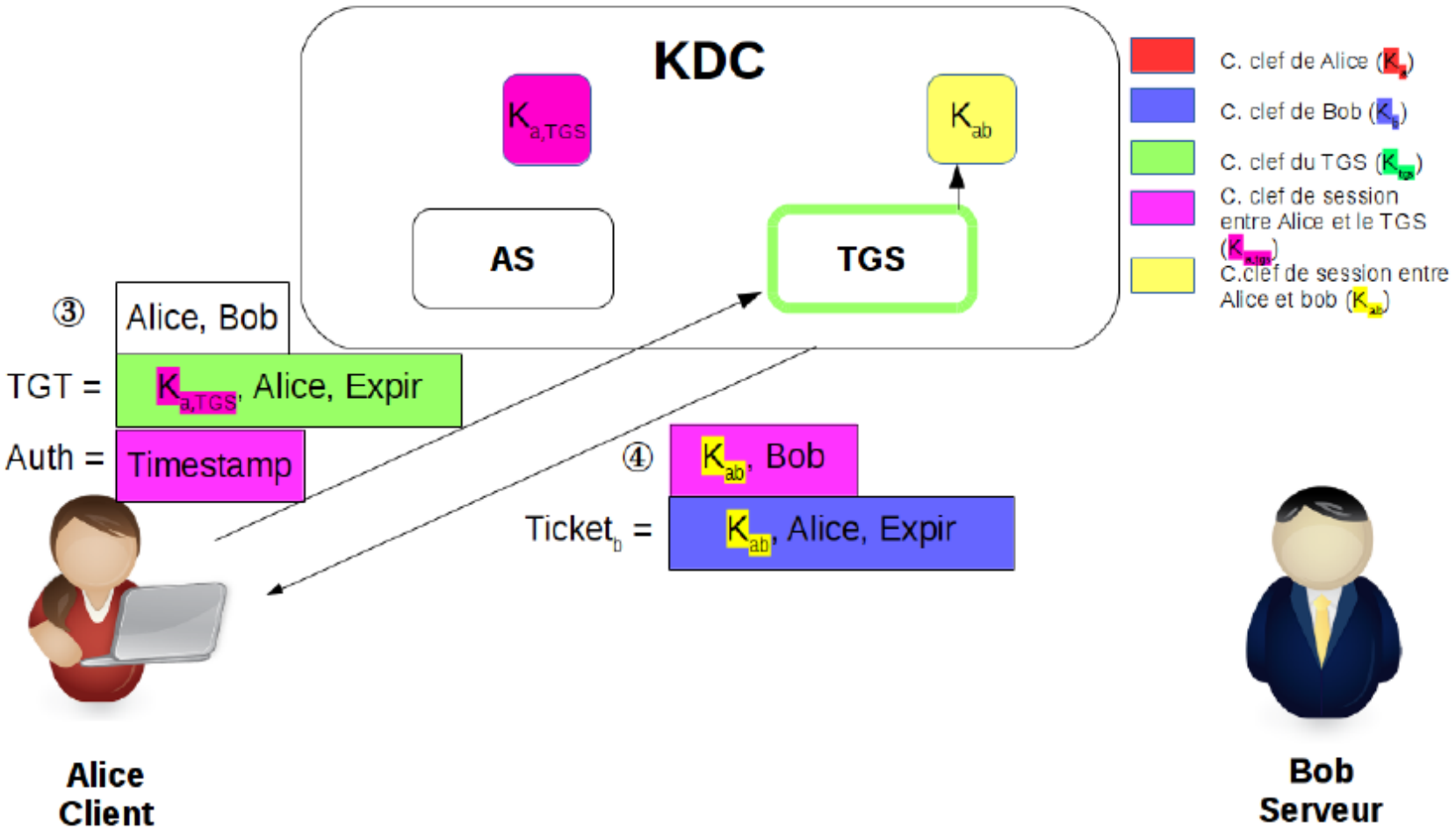
Chiffré avec la clef de session entre Alice et bob (K_{ab})

Bob
Serveur

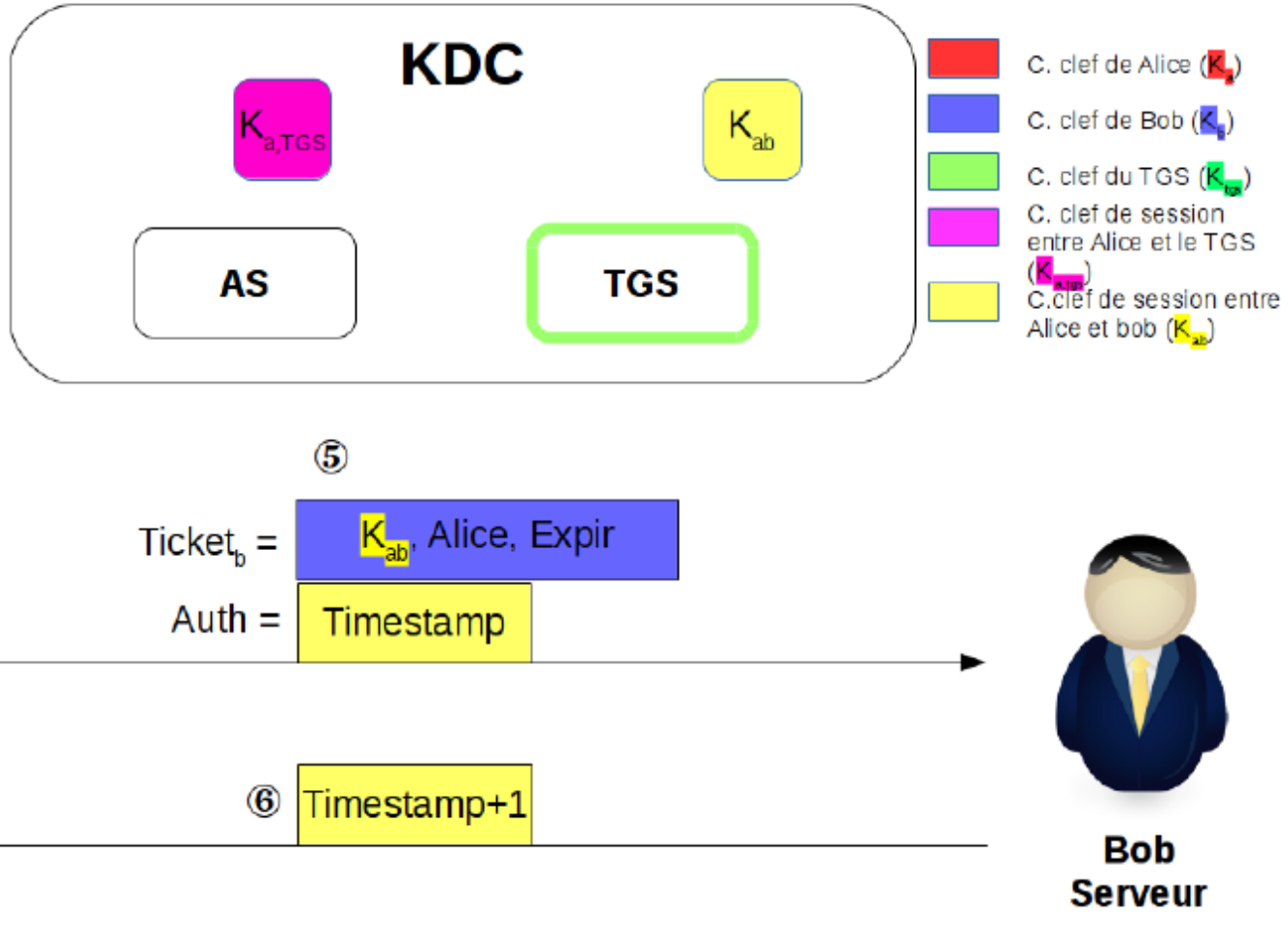
Fonctionnement du protocole



Fonctionnement du protocole



Fonctionnement du protocole



La pré-authentification

Constat

- dans le schéma précédent, n'importe qui peut obtenir un TGT pour Alice
- et de lancer une attaque off-line par dictionnaire

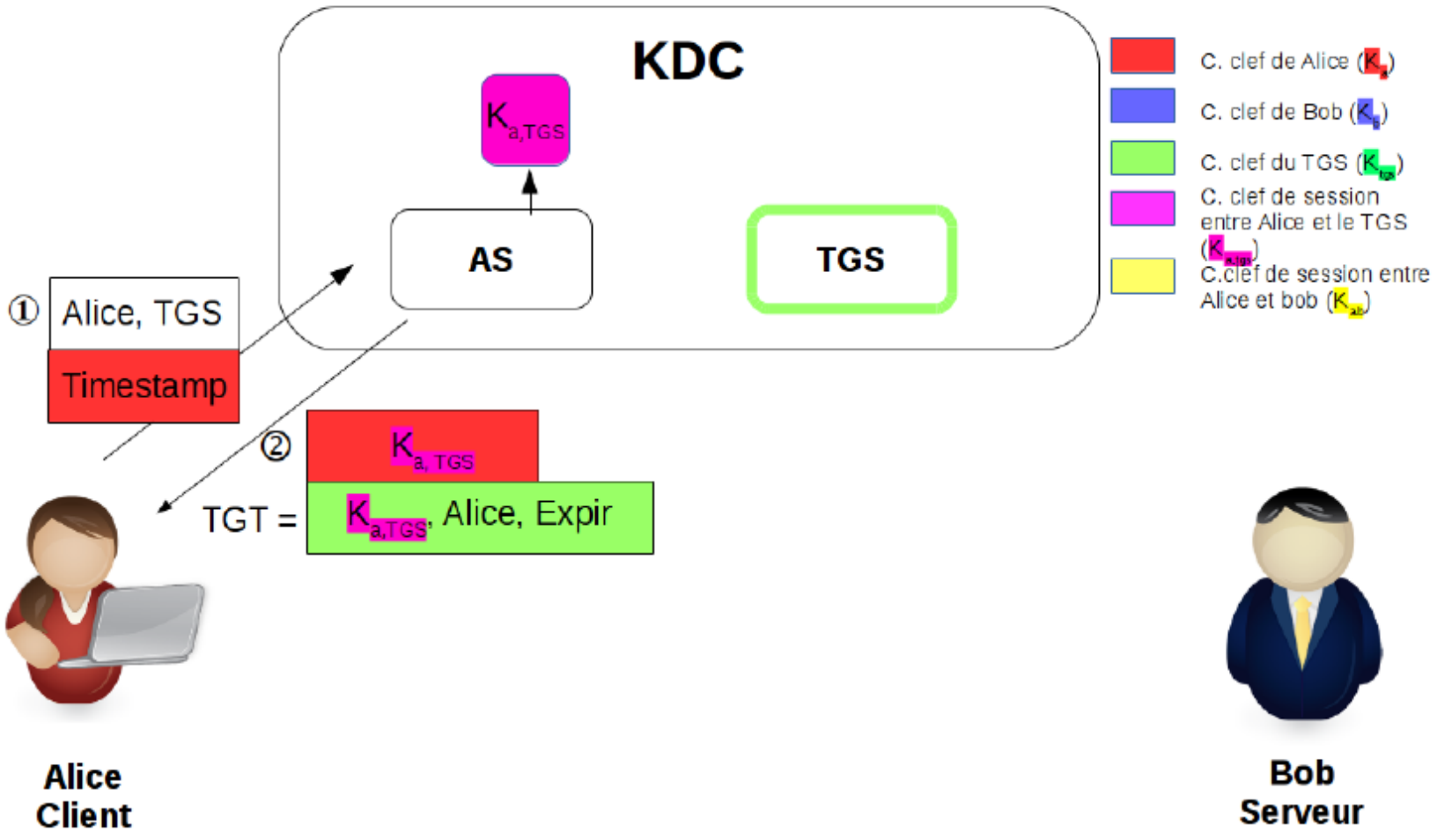
La Pré-authentification

- impose au client de prouver préalablement son identité au KDC
- Alice doit fournit un timestamp chiffré avec sa clé secrète
- empêche un attaquant d'obtenir facilement des données chiffrées avec la clé secrète d'un utilisateur

Remarque

- de telles attaques sont toujours possibles si on "sniff" un TGT…

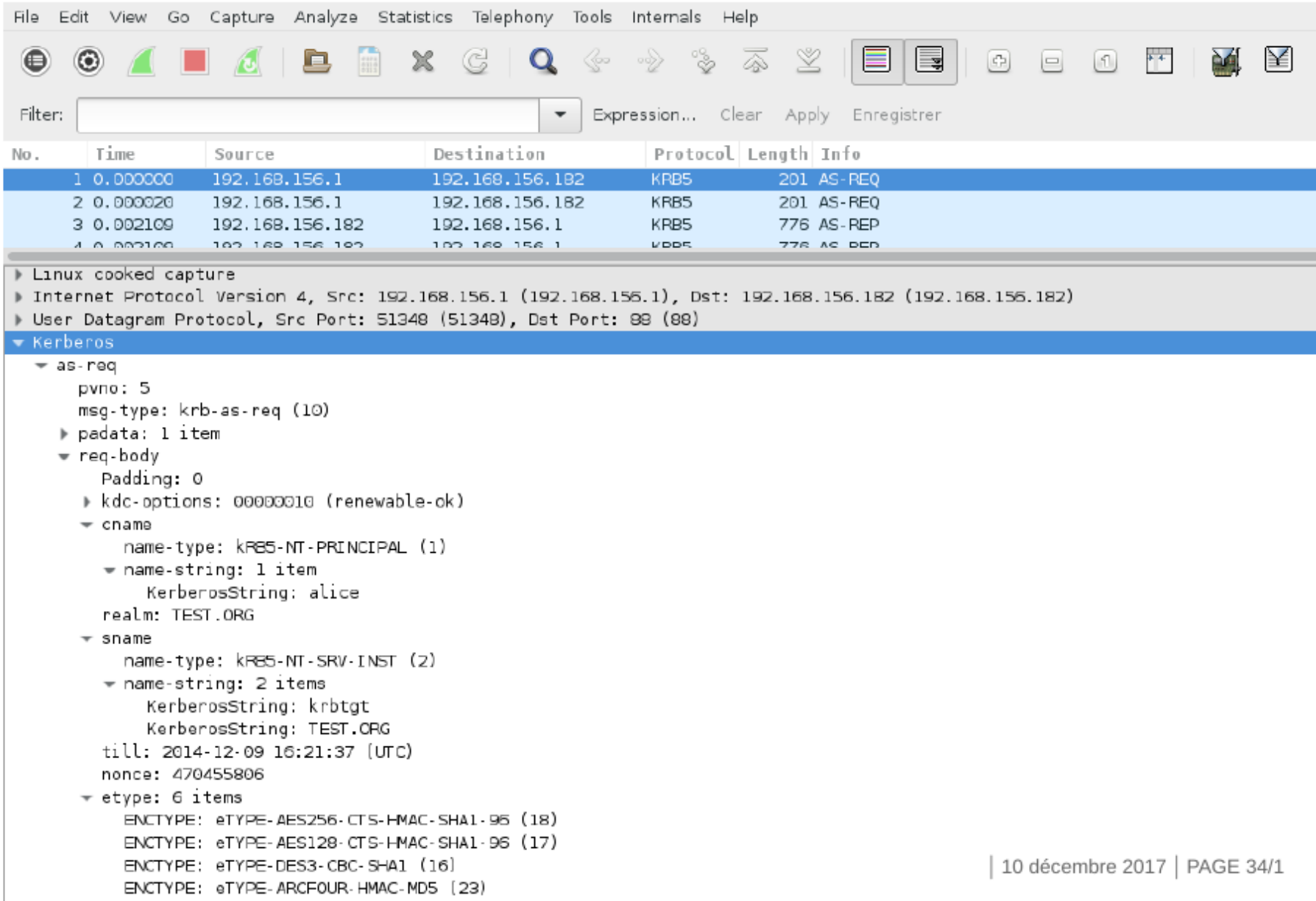
Fonctionnement du protocole



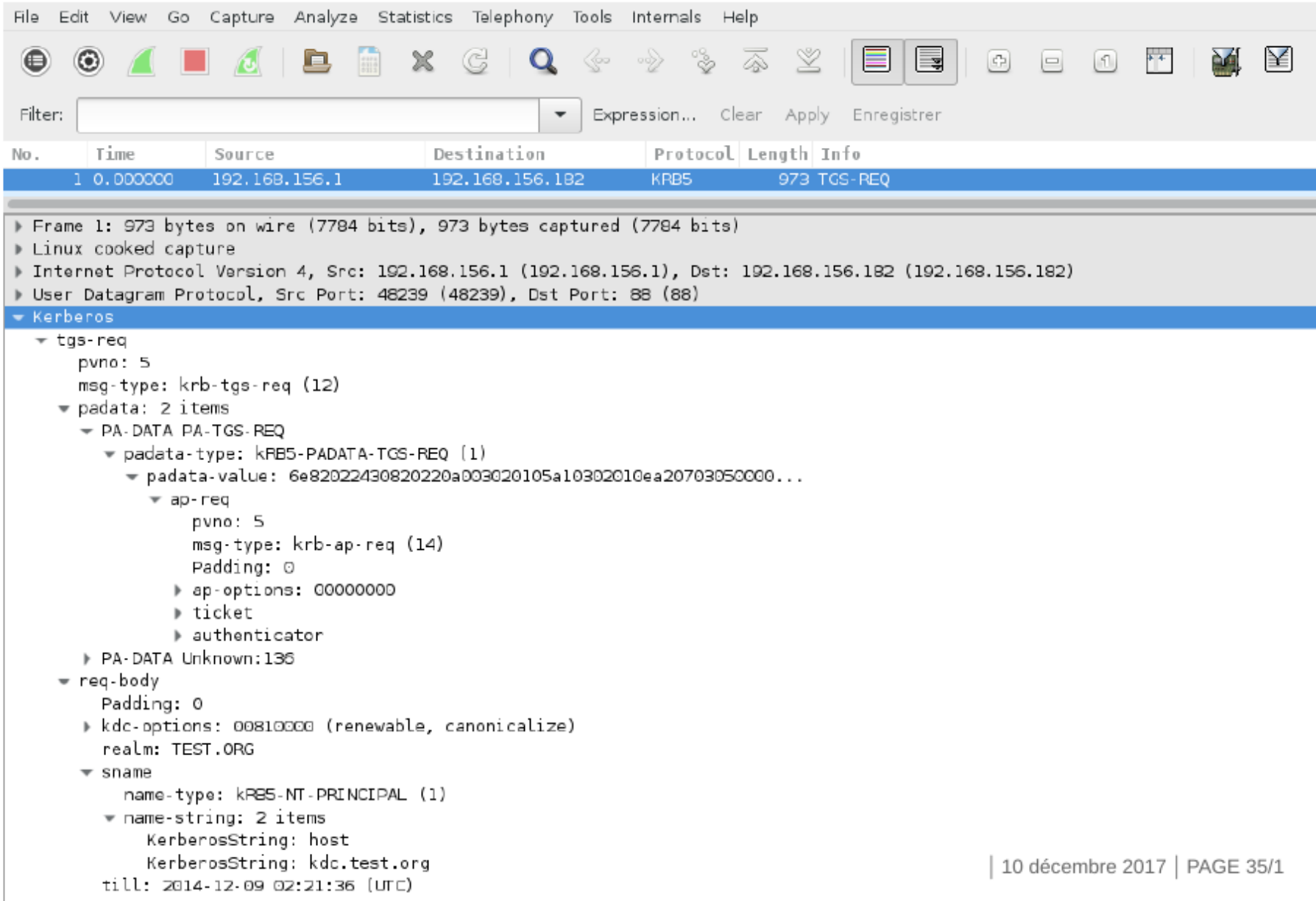
Fonctionnement du protocole

- Quelques captures réseau

Capture AS_REQ



Capture TGS_REQ



Ce qu'il faut retenir

- Kerberos fournit un service réseau jouant le rôle de **tierce partie** de confiance pour toutes les entités à authentifier
- Kerberos tient une base de données des **clefs secrètes** des clients de ce service
- Pour un utilisateur, sa clef secrète est **son mot de passe haché**
- Kerberos connaissant la clef secrète de tout le monde, peut créer des messages pour convaincre une entité de l'identité d'une autre entité
- Kerberos crée aussi des **clefs de sessions** (clefs secrètes temporaires), distribuées aux clients et aux serveurs (tous deux clients du service Kerberos) :
  - utilisées pour chiffrées les messages entre les deux participants
  - détruites à la fin de la communication.

Références

- Emmanuel Bouillon
- *Kerberos, The Definitive Guide*, *Jason Garman*, O'REILLY

Schéma général