BELOUCIF ASSIA

Chapitre 2: Introduction à l'authentification

Introduction

- **Définition**
- L’authentification désigne le processus visant à vérifier qu’un entité (personne, service, machine) est bien légitime pour accéder au système.
- **Différences entre**
  - **Identification** dire qui je suis (e.g., login, empreinte)
  - **Authentification** vérifier/prouver qui je suis (e.g., password)
  - **Autorisation** vérifier si j’ai le droit (contrôle d’accès)

Objectifs

- Au-delà du contrôle d’accès, le principe d’authentification permet d’assurer plusieurs contrôles comme:
  - l'imputabilité (apporter la preuve de qui a fait quoi)
  - et la traçabilité des actions (conserver l'historique des actions).

Les facteurs d’authentification

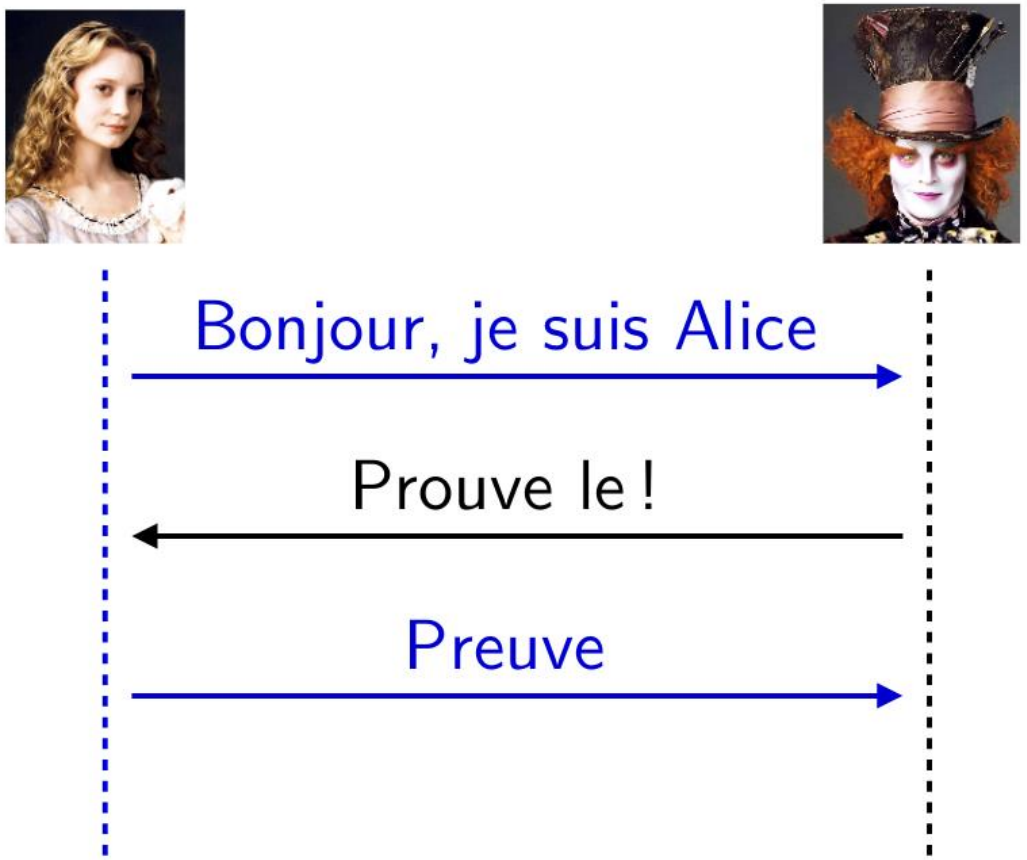
- Quelque chose que l’on **connait**
  - PIN, Mot de passe, etc.
- Quelque chose que l’on **possède**
  - Tokens, Carte à puce, badge, etc.
- Quelque chose que l’on **est**
  - Biométrie

Something you know, Something you have, Something you are

Types d’authentification

- **Authentification simple:**
  - Repose sur un seul élément d'authentification
  - **Exemple:** login/password
- **Authentification multifacteur:**
  - Repose sur deux éléments ou plus
  - **Exemple :** l'utilisateur insère sa carte à puce et spécifie son code PIN

Authentification des clients par mot de passe



Bon pratique pour choisir un mot de passe

- Recommandation: choisir dix caractères au minimum
- Mélange aléatoire de chiffres, lettre majuscules et minuscules, ainsi qu'un ou plusieurs caractères spéciaux.
- Aucun mot du dictionnaire
- Aucun chiffre ou nombre rapportant à votre vie privé
- Obliger l'usager à changer régulièrement de mot de passe.
- Ne pas utiliser le même mot de passe pour plusieurs comptes/applications
- Surveiller les tentatives d'accès illicite par comptage (les afficher).
- Prévenir l'usager des connexions précédentes sur son compte en affichant la date et l'heure (par exemple du dernier accès).
- Ne faites pas confiance dans des dispositifs d'accès à Internet (PC, portables, tablettes, smartphones, etc.) dont vous ne connaissez pas le niveau de sécurité ;
- Faites attention à la sécurité de votre propre dispositif d'accès à Internet (mises à jour, antivirus, etc.) ;
- Activer les fonctions de double authentification (par SMS, application, jeton, etc.) quand elles sont disponibles.

Authentification des clients par mot de passe

Un protocole très simple

1. $A \rightarrow B : A, pw$
2. $B \rightarrow A : 1$ si $\langle A, h(pw) \rangle \in \text{passwordtable}$

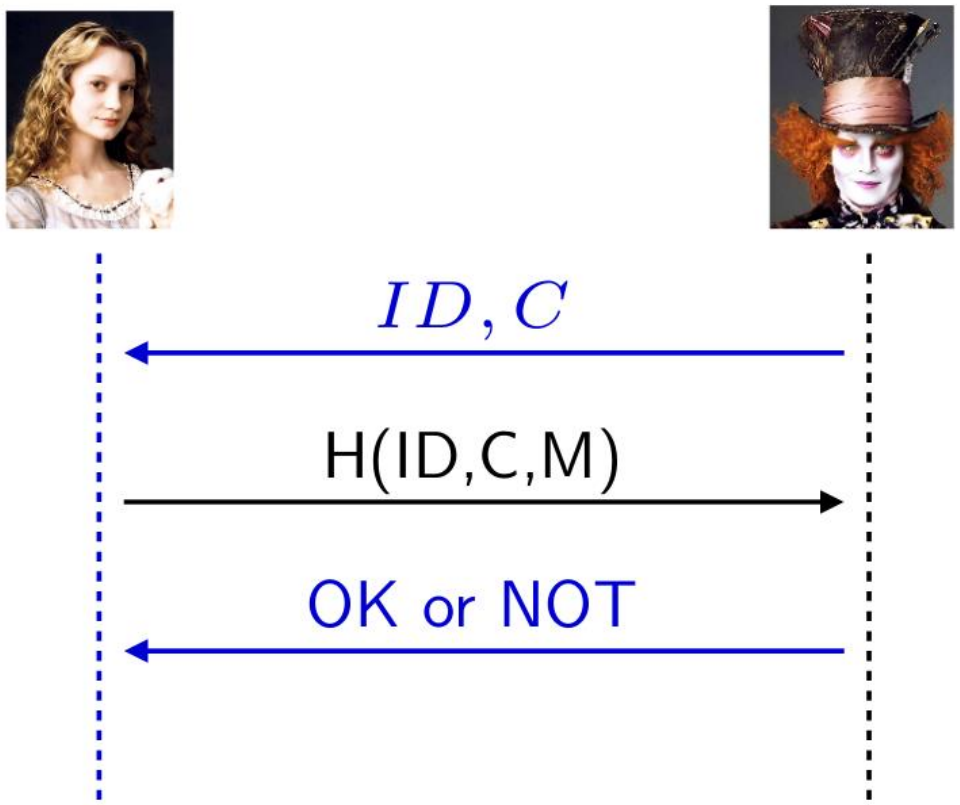
La table des mots de passe passwordtable

Le vérificateur stocke les paires $\langle A_i, h(pw_i) \rangle$

Challenge-response authentication

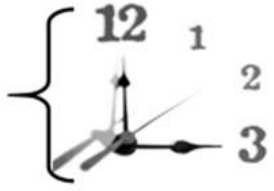
- Les protocoles d'authentification que l'on peut considérer comme forts reposent souvent sur des protocoles dits défi-réponse.
- Le message envoyé par le prouveur pour s'authentifier dépend à la fois d'une clé secrète, mais aussi d'un défi variable envoyé par le vérifieur.
- Lorsqu'un prouveur souhaite prouver son identité à un vérifieur, ce dernier lui envoie alors un défi (une valeur aléatoire par exemple) et le prouveur doit lui transmettre une réponse calculée à partir de ce défi spécifique (une signature de ce défi par exemple).

Challenge-response authentication



Authentification OTP (One Time Password)

- Authentification avec un mot de passe à usage unique (un mot de passe par session)
- Basée sur l'utilisation d'un secret partagé entre l'authentificateur et le serveur d'authentification ==> permet de générer les mêmes OTP chez les deux systèmes
- Un OTP est généré à partir du secret partagé et du temps de la transaction=> n'est valable que pour la transaction ou la session.



Authentification biométrique

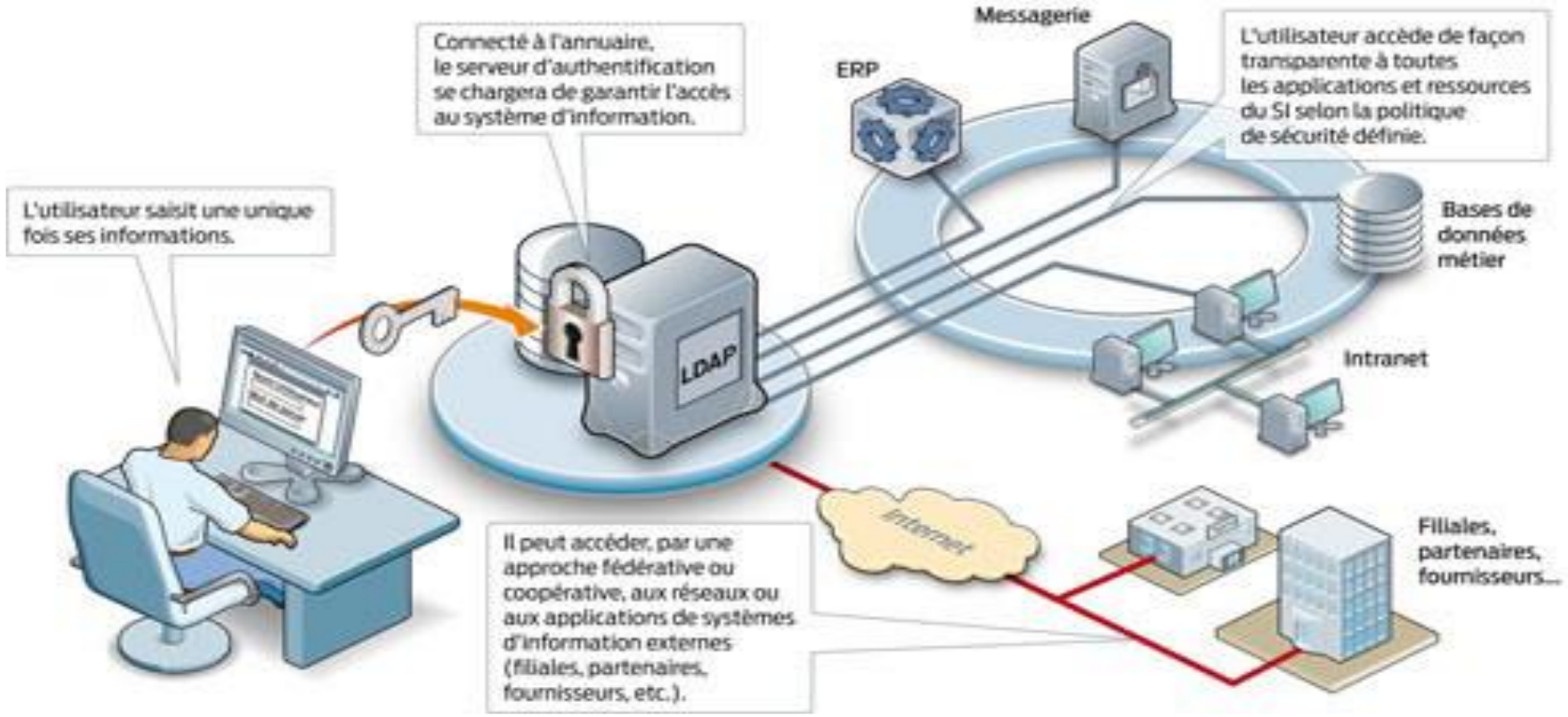
- utilisation des caractéristiques physiologiques uniques d'un individu pour l'identifier. En confirmant la signature biométrique, l'individu est authentifié.
- Il s'agit par exemple des scanners d'empreintes digitales pour déverrouiller les téléphones.
- Un avantage de l'authentification biométrique sur les systèmes basés sur la connaissance ou les jetons, est que l'identification d'une personne pour l'authentification est plus fiable, puisque les caractéristiques biométriques ne sont généralement pas partageables.

Authentification par certificat(SSL)

- Avec ce type d’authentification l’utilisateur doit posséder un certificat client pour accéder au serveur.
- Cette approche est plus sécurisé parce que les certificat sont gérés de façon centralisé par des autorités spécialisées.
- Il faut s’assurer que le certificat est valide en vérifiant ces deux dates: « Non valide avant » et « Non valide après ».
- le certificat sera vérifié par rapport à une liste de révocation de certificats – CRL. C'est une liste signée publiée par l'AC qui répertorie les certificats qui ont été explicitement révoqués.
- la possession de la clé privée est vérifiée grâce à un mécanisme de défi-réponse. Le serveur va demander un bit de données aléatoire à signer à l'aide de la clé privée correspondant à la clé publique présentée pour l'authentification.

Authentification SSO (Single Sign On)

- Méthode où lutilisateur s'authentifie une seule fois pour accéder à plusieurs applications ou services.

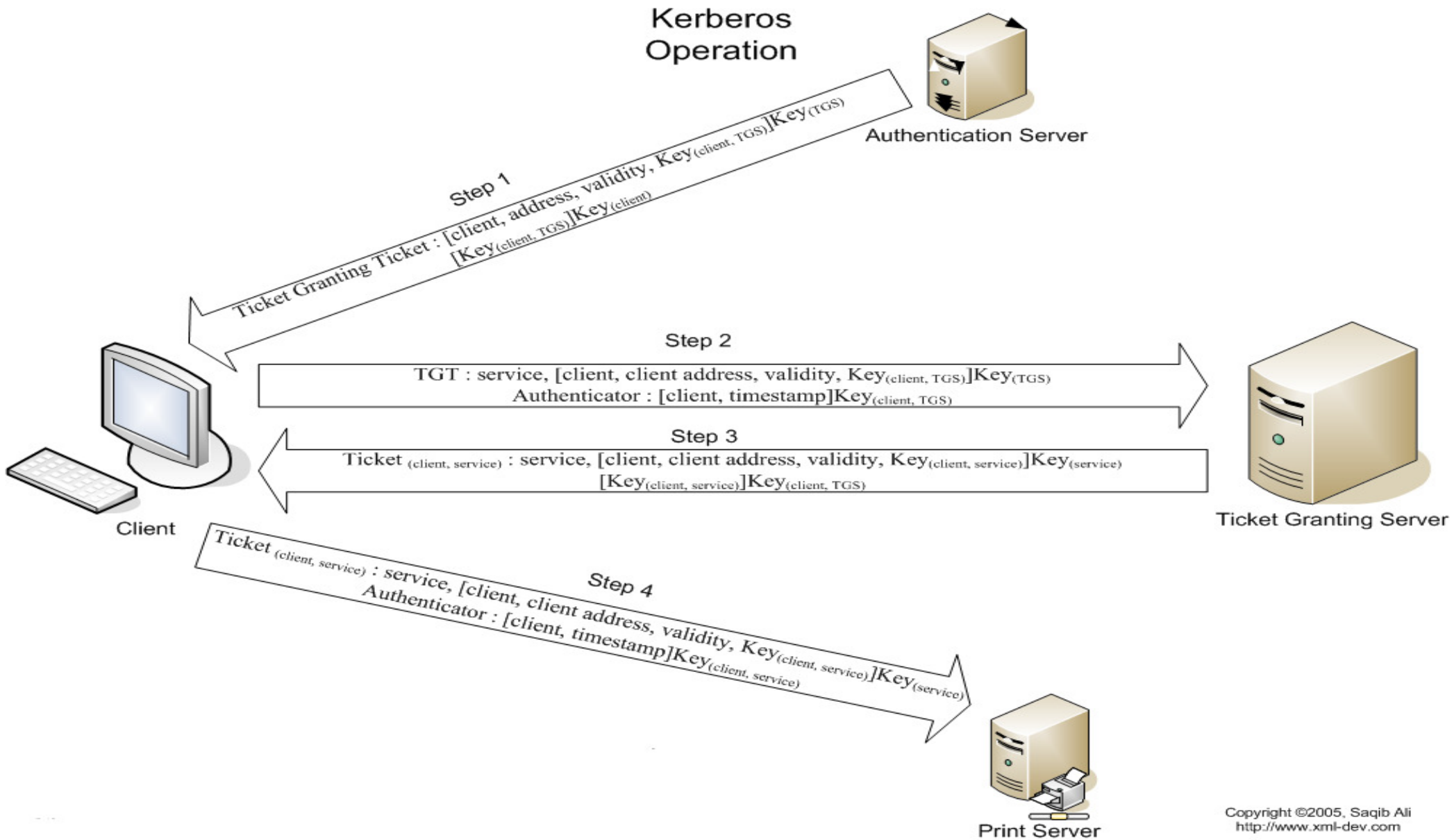


Kerberos

- Un des systèmes d'authentification les plus répandus dans les systèmes distribués.
  - Unix depuis le milieu des années 80
  - Microsoft depuis Windows 2000
- Système client-serveur basé sur la cryptographie symétrique
  - Bien que Microsoft utilise une extension non standardisée basée sur la cryptographie asymétrique pour l'authentification par cartes à puce.

Kerberos: Les principales composantes

- **Principals:** Représentent les divers usagers, applications et services voulant s'authentifier les uns aux autres.
- Key Distribution Center (KDC) : Composante principale de l'architecture qui offre les deux principaux services:
  - Authentication Service (AS)
    - Service authentifiant un principal.
  - Ticket Granting Service (TGS)
    - Service offrant à un principal un ticket permettant d'être authentifié par un autre principal. Ce ticket peut contenir aussi les droits d'accès du principal.
- Donc, le KDC se doit de conserver tous les secrets et les clés cryptographiques permettant d'effectuer les diverses opérations.



Kerberos: Le protocole

1. L’usager entre son identificateur et son mot de passe.
2. L’usager utilise une fonction de hachage à sens unique et produit sa clé secrète.
3. Le client envoie une requête au AS: « Usager X voudrait utiliser un service Y ».
    - Aucun mot de passe ou clé n’est envoyé.
4. L’AS vérifie que le client existe dans sa base de données. Si tel est le cas, l’AS retourne deux messages au client:
    - Msg A: Clé de session entre le client et le TGS chiffrée.
    - Msg B: Ticket-Granting Ticket.

Kerberos: Le protocole

5. Le client déchiffre le message A, vérifie si le timestamp correspond à celui envoyé à l'étape 3 et obtient sa clé pour communiquer avec le TGS.

    – Le client ne peut pas déchiffrer le message B destiné au TGS.

6. Afin d'accéder à un serveur, le client envoie une requête au TGS:

    – Msg C: Le Ticket-Granting Ticket de B et le nom du service demandé.

    – Msg D: Authenticator composé du nom du client et d'un nonce chiffré avec la clé de session entre le client et le TGS.

Kerberos: Le protocole

7. Le TGS déchiffre l'authenticator et retourne au client:
   - Msg E: Le Client-to-server ticket incluant le nom du client, son adresse, la période de validité et la clé de session client/serveur, le tout chiffré avec la clé du service.
   - Msg F: La clé de session client/serveur chiffré avec la clé de session client/TGS.
8. Le client déchiffre le message F, vérifie si le timestamp correspond à celui envoyé à l'étape 6 et obtient sa clé pour communiquer avec le serveur.
9. Afin d'accéder à un service, le client envoie au serveur une requête de service:
   - Msg G: Le Client-to-server ticket de E et le nom du service demandé.
   - Msg H: Authenticator composé du nom du client et d'un nonce chiffré avec la clé de session client/serveur.

Kerberos: Le protocole

10. Le service déchiffre le ticket et renvoie le timestamp du message H incrémenté de 1 chiffré avec la clé de session client/serveur.
11. Le client déchiffre ce dernier message et vérifie si le timestamp a été incrémenté tel que prévu. Dans ce cas, le client peut faire confiance au serveur et l'utiliser.
12. Le serveur offre le service au client.