CAS

I) Généralités :

Un serveur CAS (Central Authentification Service) basé généralement sur Kerberos est l'une des solutions SSO (Single Sign-On).

II) Fonctionnement :

Le serveur CAS authentifie, transmet et certifie l'identité des utilisateurs.

Le mot de passe circule entre le navigateur du client et le serveur à travers un canal crypté.

L'acceptation d'un cookie privé et protégé sur le poste client permet une ré-authentification transparente.

L'application (ou serveur d'application) reçoit du serveur d'authentification (CAS) un ticket service (non rejouable, durée vie limitée) qui circule en clair via le navigateur (CGI). L'application valide le ticket service auprès du serveur CAS en utilisant le protocole http.

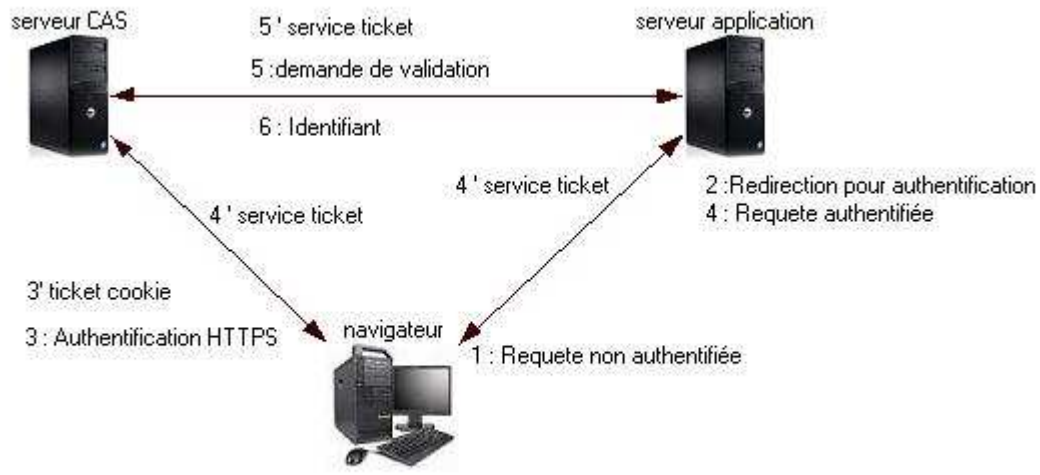
Si le ticket est validé, le serveur CAS fournit à l'application l'identifiant de la personne.
L'application n'a ainsi jamais accès au mot de passe

III) Les architectures CAS :

3.1) Agent d'authentification :

L'agent d'authentification est la brique du SSO intégrée à l'application sous forme d'une librairie applicative ou d'un module apache.

Solutions parfois coûteuses et difficile.

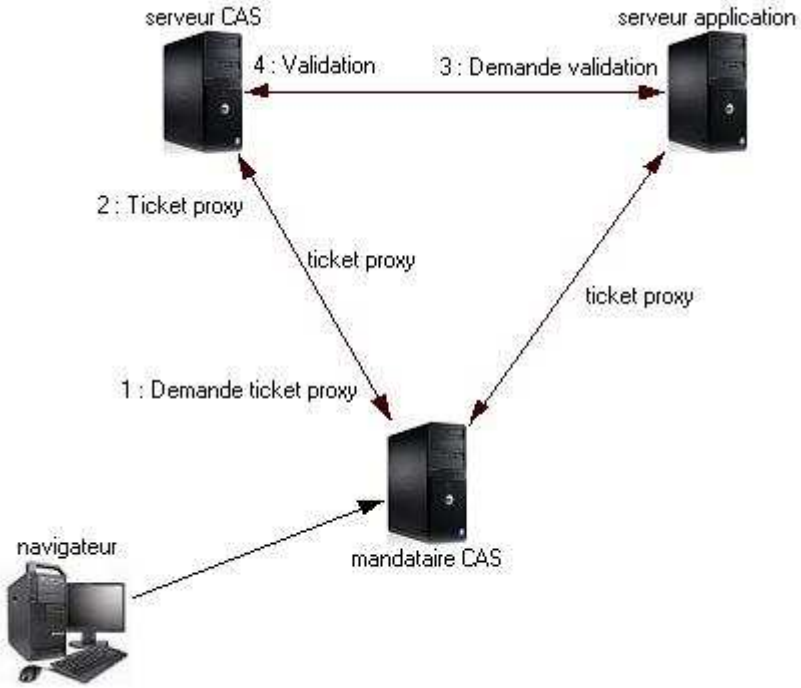


3.2) Fonctionnement multi-tiers :

Le fonctionnement n-tiers consiste à mettre en place un mandataire CAS qui effectuera les demandes des clients au serveur CAS.

Ce mandataire fonctionne sur le principe du proxy. Ce mandataire peut être un portail web ou une passerelle de courrier électronique.

Fonctionnement 2-tiers :



Fonctionnement n-tiers :