ESUP Portail

Le mécanisme de Single Sign-On CAS (Central Authentication Service)

ESUP Portail – groupe SSO - Pascal Aubry

http://www.esup-portail.org

Généralités

- Sous forme de servlets java
- Ne traite que l'authentification (mais extensions à priori aisées)
- S'intègre dans uportal sans développement
- Utilisé par différentes universités américaines
- Fonctionnalité de proxy très intéressante
- Nombreuses bibliothèques clientes
  - perl, java, pl-sql, PHP, …
- Modules apache et pam

Fonctionnement de base

- Similaire aux autres mécanismes de SSO, mais
  - Utilisation de tickets opaques
  - Sécurité accrue
- Pas de fonctionnement multi-tier
  - Nécessite un « contact » direct entre l'application ayant besoin d'authentification et le navigateur web

Tickets utilisés

- **TGC** : Ticket Granting Ticket (Cookie)
  - Valable pour un utilisateur
  - Cookie de session privé et protégé (https) du serveur CAS vers le navigateur
  - Permet d'obtenir les ST
  - Évite les ré-authentifications (rejouable)
- **ST** : Service Ticket
  - Valable pour un service et un utilisateur
  - Authentifie une personne, pour une application (une URL)
  - À usage unique (non rejouable)

URLs utilisées

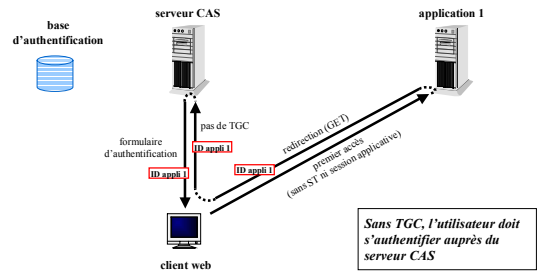
- **/Login** : connexion, HTTPS
  - En cas de succès, positionnement du TGC
  - Permet d'éviter une ré authentification
- **/Logout** : déconnexion, HTTP(S)
  - Suppression du TGC
  - Suppression des références de l'utilisateur au niveau du serveur CAS

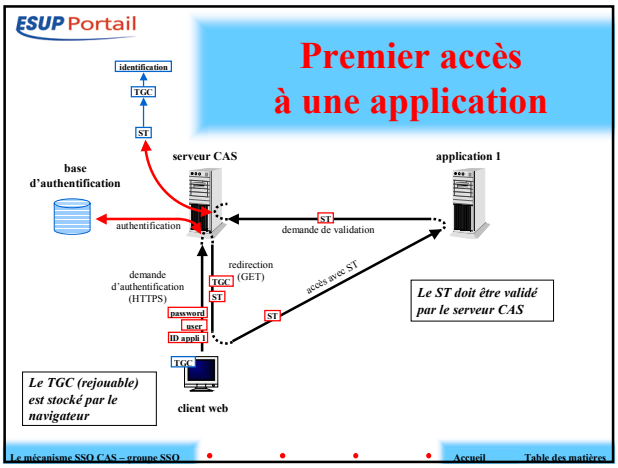
} navigateurs web

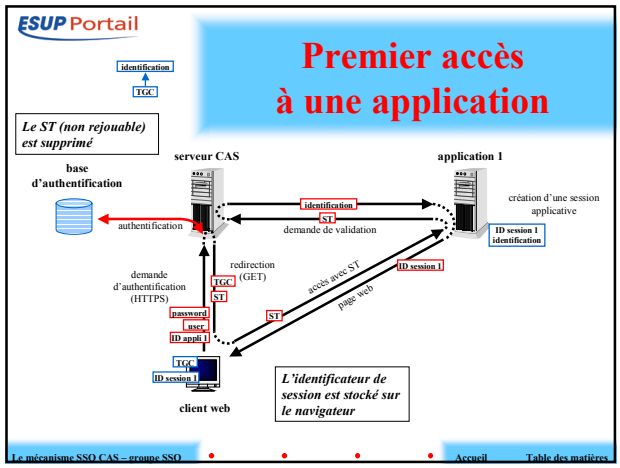
- **/Validate** (ou **/serviceValidate**), HTTP(S)
  - Passage du ST pour validation
  - Retour de l'identifiant de l'utilisateur
  - Invalidation du ST

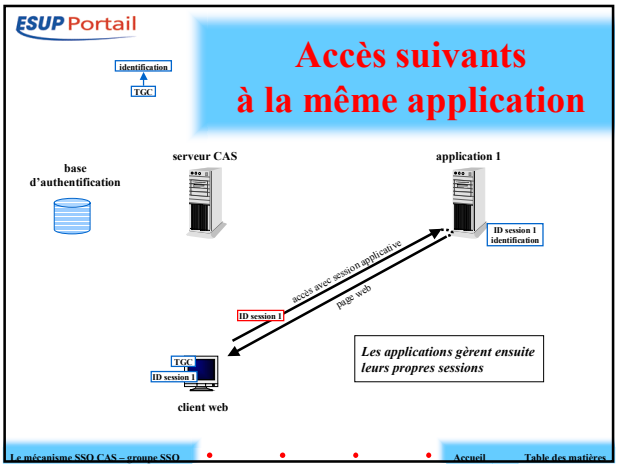
} applications

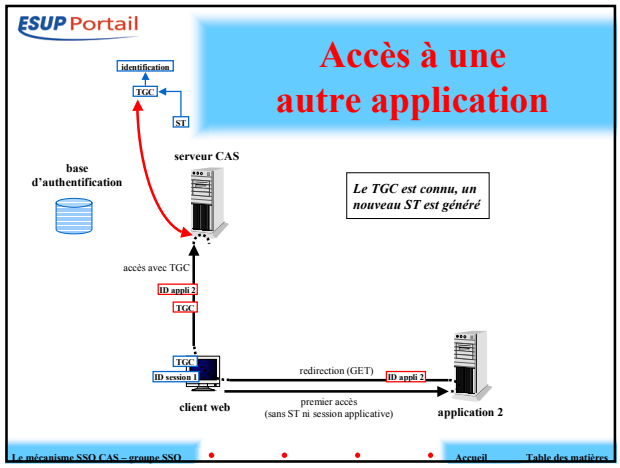
Premier accès à une application

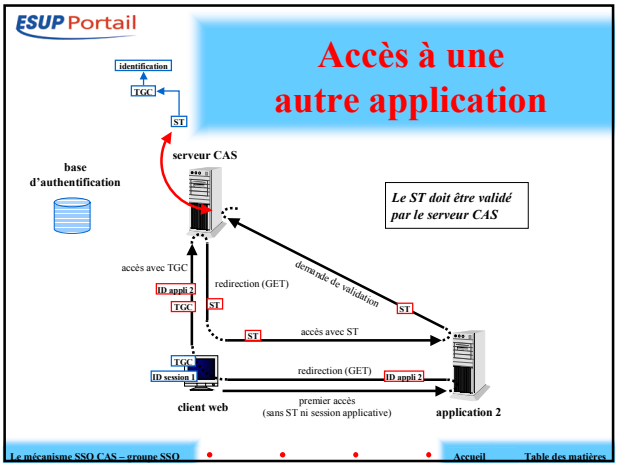


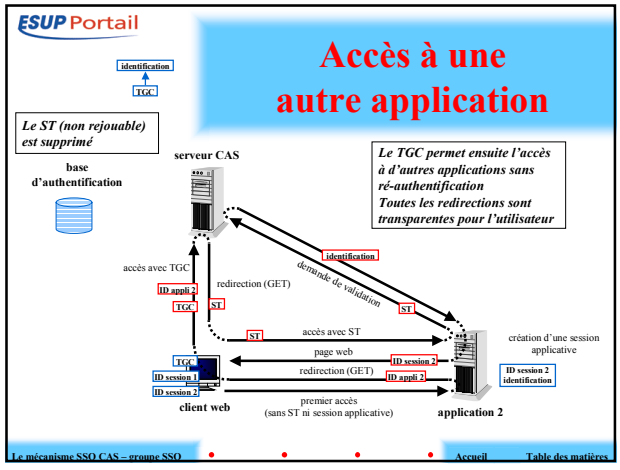

ESUP Portail
Premier accès à une application
identification
TGC
ST
serveur CAS
application 1
base d'authentification
authentification
ST
demande de validation
redirection (GET)
demande d'authentification (HTTPS)
TGC
ST
password
user
ID appli 1
accès avec ST
ST
Le ST doit être validé par le serveur CAS
TGC
client web
Le TGC (rejouable) est stocké par le navigateur
Le mécanisme SSO CAS – groupe SSO
Accueil
Table des matières


ESUP Portail
Premier accès à une application
identification
TGC
Le ST (non rejouable) est supprimé
serveur CAS
application 1
base d'authentification
authentification
identification
ST
demande de validation
création d'une session applicative
ID session 1 identification
redirection (GET)
demande d'authentification (HTTPS)
TGC
ST
password
user
ID appli 1
accès avec ST
ID session 1
page web
ST
TGC
ID session 1
client web
L'identificateur de session est stocké sur le navigateur
Le mécanisme SSO CAS – groupe SSO
Accueil
Table des matières


ESUP Portail
Accès suivants à la même application
identification
TGC
serveur CAS
application 1
base d'authentification
ID session 1 identification
accès avec session applicative
ID session 1
page web
TGC
ID session 1
client web
Les applications gèrent ensuite leurs propres sessions
Le mécanisme SSO CAS – groupe SSO
Accueil
Table des matières


ESUP Portail
Accès à une autre application
identification
TGC
ST
serveur CAS
base d'authentification
Le TGC est connu, un nouveau ST est généré
accès avec TGC
ID appli 2
TGC
TGC
ID session 1
client web
redirection (GET)
ID appli 2
premier accès
(sans ST ni session applicative)
application 2
Le mécanisme SSO CAS – groupe SSO
Accueil
Table des matières


ESUP Portail
Accès à une autre application
identification
TGC
ST
serveur CAS
base d'authentification
Le ST doit être validé par le serveur CAS
accès avec TGC
ID appli 2
TGC
redirection (GET)
demande de validation
ST
ST
ST
accès avec ST
TGC
ID session 1
client web
redirection (GET)
ID appli 2
premier accès
(sans ST ni session applicative)
application 2
Le mécanisme SSO CAS – groupe SSO
Accueil
Table des matières


ESUP Portail
Accès à une autre application
identification
TGC
Le ST (non rejouable) est supprimé
serveur CAS
base d'authentification
Le TGC permet ensuite l'accès à d'autres applications sans ré-authentification
Toutes les redirections sont transparentes pour l'utilisateur
accès avec TGC
ID appli 2
TGC
redirection (GET)
identification
demande de validation
ST
ST
ST
accès avec ST
page web
ID session 2
création d'une session applicative
TGC
ID session 1
ID session 2
client web
redirection (GET)
ID appli 2
ID session 2 identification
premier accès
(sans ST ni session applicative)
application 2
Le mécanisme SSO CAS – groupe SSO
Accueil
Table des matières

ESUP Portail

Le fonctionnement multi-tiers

- Possibilité pour une application (mandataire) d'interroger une autre application (service)
- Aucun lien n'est nécessaire entre le navigateur et l'application tiers
- Possibilité de chaîner les mandataires

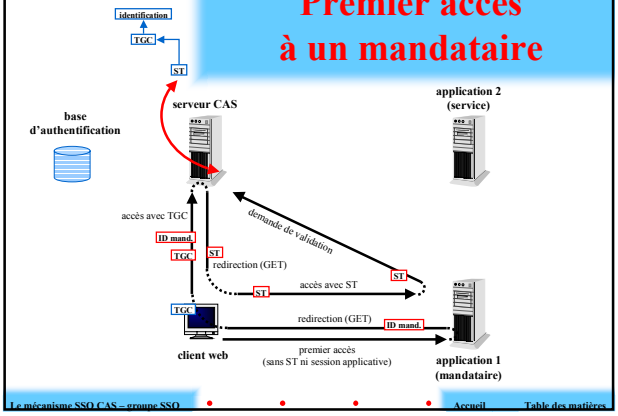
ESUP Portail

Tickets utilisés

- **TGC** : Ticket Granting Ticket
- **ST** : Service Ticket
- **PGT** : Proxy Granting Ticket
  - Valable pour un utilisateur
  - Envoyé par le serveur CAS à une appli proxy CAS
  - Permet d'obtenir les PT
  - Évite les ré-authentifications des applications (rejouable)
- **PT** : Proxy Ticket
  - Valable pour un service et un utilisateur
  - Équivalent du ST pour les mandataires
  - Utilisé pour les services n'ayant pas de lien avec le navigateur

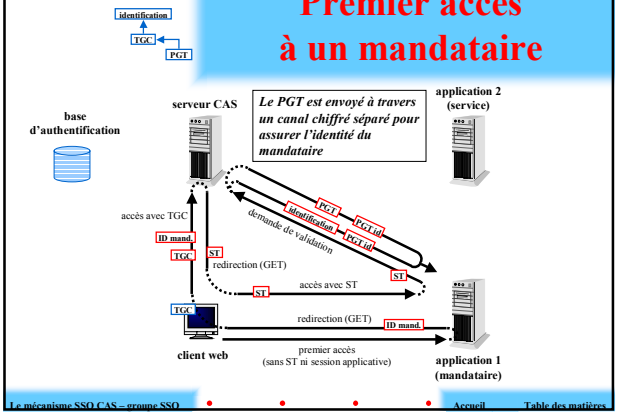
ESUP Portail

Premier accès à un mandataire



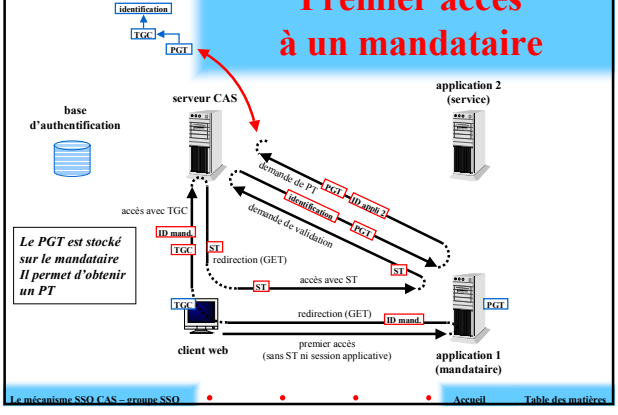
ESUP Portail

Premier accès à un mandataire



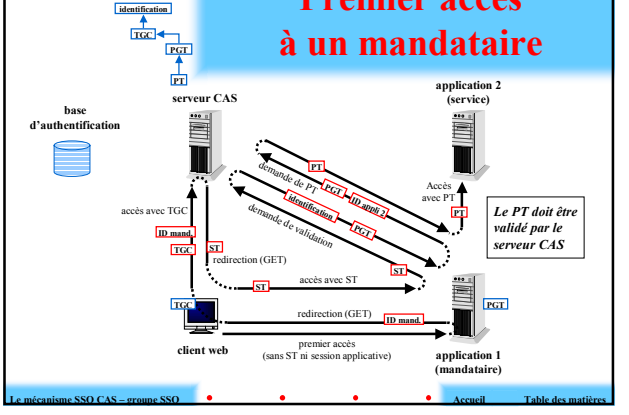
ESUP Portail

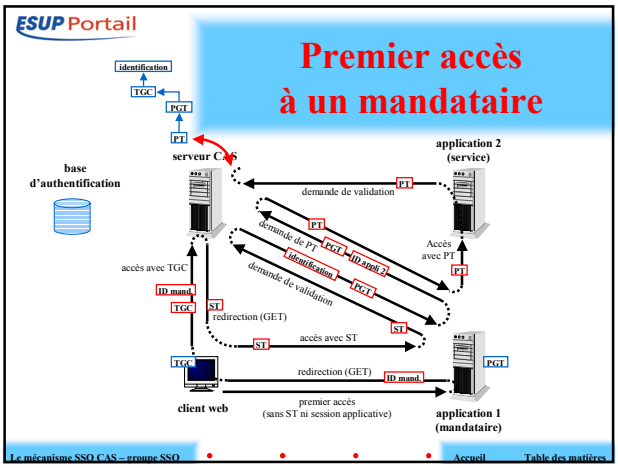
Premier accès à un mandataire

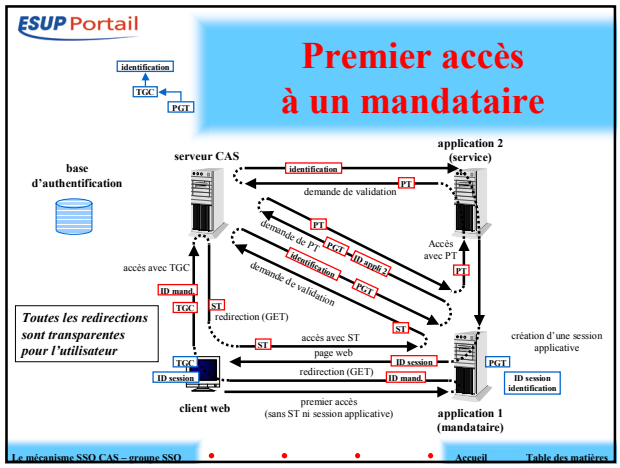


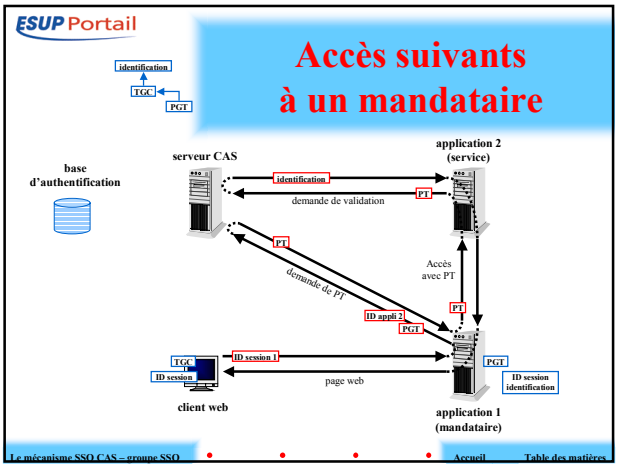
ESUP Portail

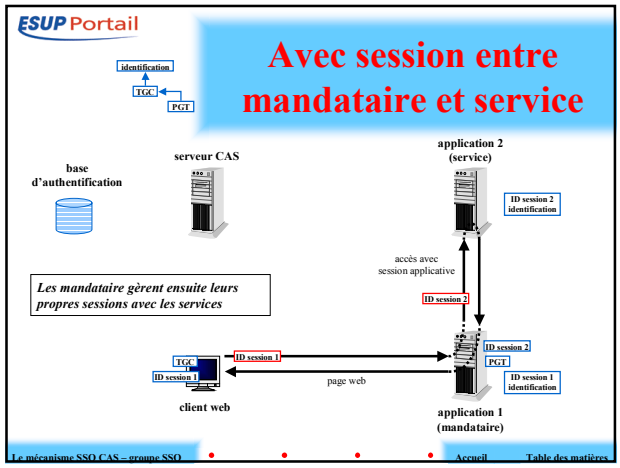
Premier accès à un mandataire




ESUP Portail
Premier accès
à un mandataire
identification
TGC
PGT
PT
serveur CAS
application 2
(service)
base
d'authentification
demande de validation
PT
demande de PT
PGT
ID appli 2
identification
Accès
avec PT
accès avec TGC
ID mand.
TGC
ST
redirection (GET)
accès avec ST
client web
premier accès
(sans ST ni session applicative)
application 1
(mandataire)
Le mécanisme SSO CAS – groupe SSO
Accueil
Table des matières


ESUP Portail
Premier accès
à un mandataire
identification
TGC
PGT
serveur CAS
application 2
(service)
base
d'authentification
demande de validation
PT
demande de PT
PGT
ID appli 2
identification
Accès
avec PT
accès avec TGC
ID mand.
TGC
ST
redirection (GET)
accès avec ST
page web
ID session
redirection (GET)
ID mand.
création d'une session
applicative
ID session
identification
client web
premier accès
(sans ST ni session applicative)
application 1
(mandataire)
Toutes les redirections
sont transparentes
pour l'utilisateur
Le mécanisme SSO CAS – groupe SSO
Accueil
Table des matières


ESUP Portail
Accès suivants
à un mandataire
identification
TGC
PGT
serveur CAS
application 2
(service)
base
d'authentification
identification
demande de validation
PT
demande de PT
Accès
avec PT
ID appli 2
PGT
TGC
ID session
ID session 1
page web
PGT
ID session
identification
client web
application 1
(mandataire)
Le mécanisme SSO CAS – groupe SSO
Accueil
Table des matières


ESUP Portail
Avec session entre
mandataire et service
identification
TGC
PGT
serveur CAS
application 2
(service)
base
d'authentification
ID session 2
identification
accès avec
session applicative
ID session 2
Les mandataire gèrent ensuite leurs
propres sessions avec les services
TGC
ID session 1
ID session 2
PGT
ID session 1
identification
ID session 1
page web
client web
application 1
(mandataire)
Le mécanisme SSO CAS – groupe SSO
Accueil
Table des matières