

Zap

(lanceur d'applications développé par le Consortium Cocktail)



Zap ?

- Gestion centralisée des applications
- Des applications de type :
 - Web, WebStart ou Exécutable
- Une interface graphique dynamique et personnalisable
- Utilise le SSO (Single Sign-On)

✓ *lanceur multiplateformes (Java 1.4)*

SSO (Single Sign-On)

- Le but est de centraliser l'authentification des utilisateurs
- Il permet à l'utilisateur d'accéder à toutes les ressources auxquels il est autorisé d'accéder, en s'authentifiant une seule fois
- CAS propose ce service

Quel CAS ?

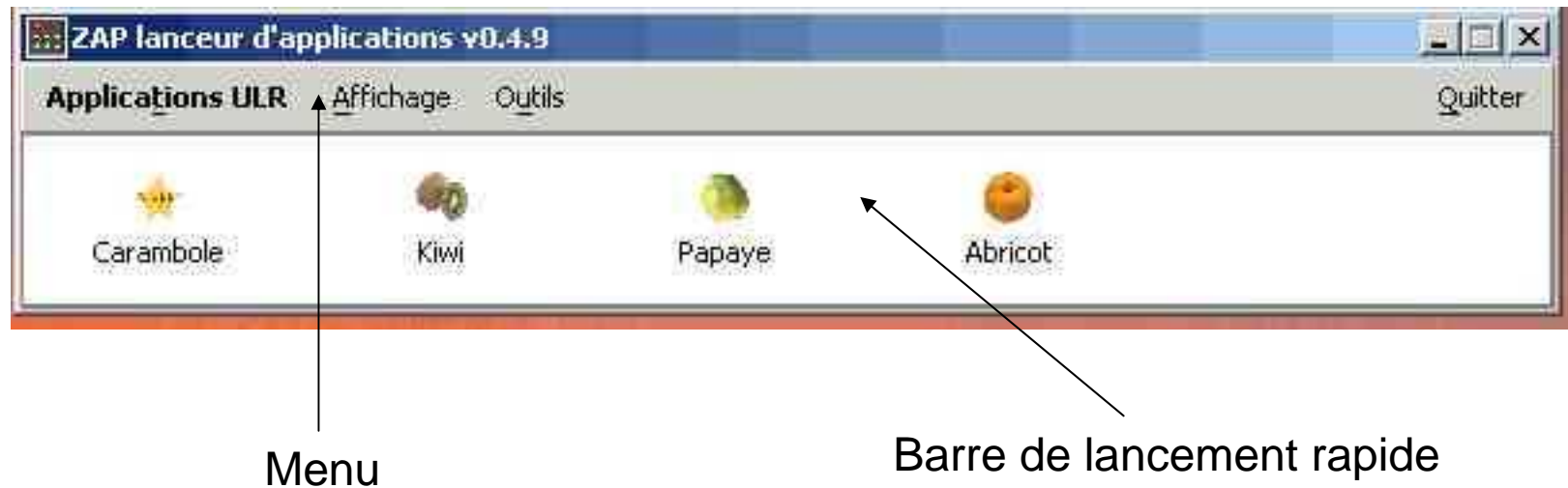
- CAS Generic Handler (esup-portail)
 - Utilise le SSO (Single Sign-On)
 - Et un plug-in permettant d'authentifier les utilisateurs avec des méthodes différentes (LDAP, database, files, NIS, ...)

✓ *Nous avons choisi la méthode database.*

Zap pour l'utilisateur

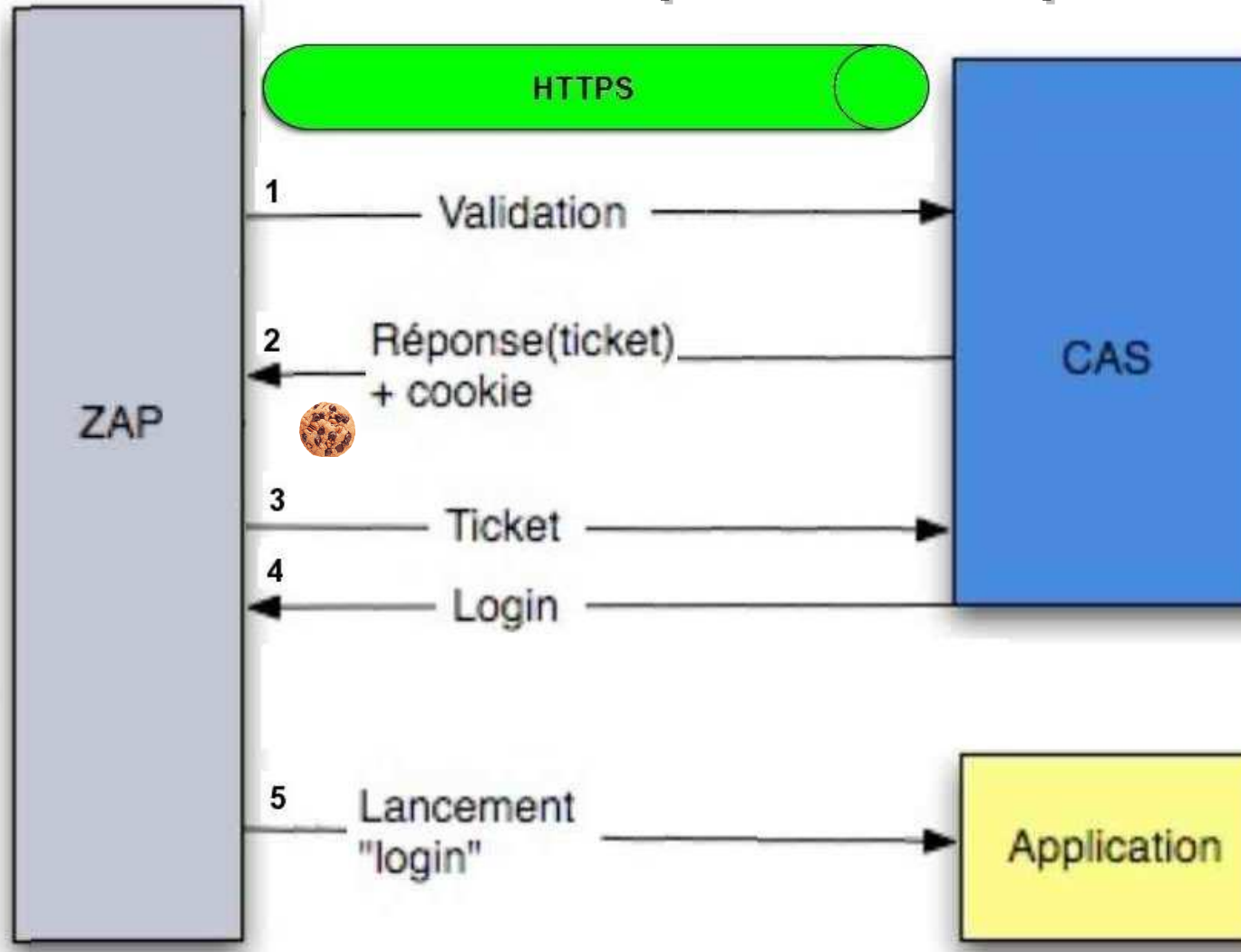
- Il s'authentifie une seule fois
 - au lancement de la première application
- Il peut ensuite lancer toutes les applications sans saisir à nouveau son login et mot de passe

Démonstration



- apps\documentation\zap\Zap_viewlet_swf.html

Principe de Zap



Zap se fait passer pour une appli Web auprès de CAS

Zap demande une authentification à l'utilisateur (login + mot de passe)

1. Elle est transmise au serveur CAS pour validation

Vérification authentification à l'aide d'une base de données ou LDAP

2. Si Validation de CAS : Zap reçoit un Ticket (ST : Service Ticket) et un Cookie (TGC : Ticket Granting Cookie)

3. 4. Ticket utilisable 1 fois pour récupérer l'identifiant validé (le login)

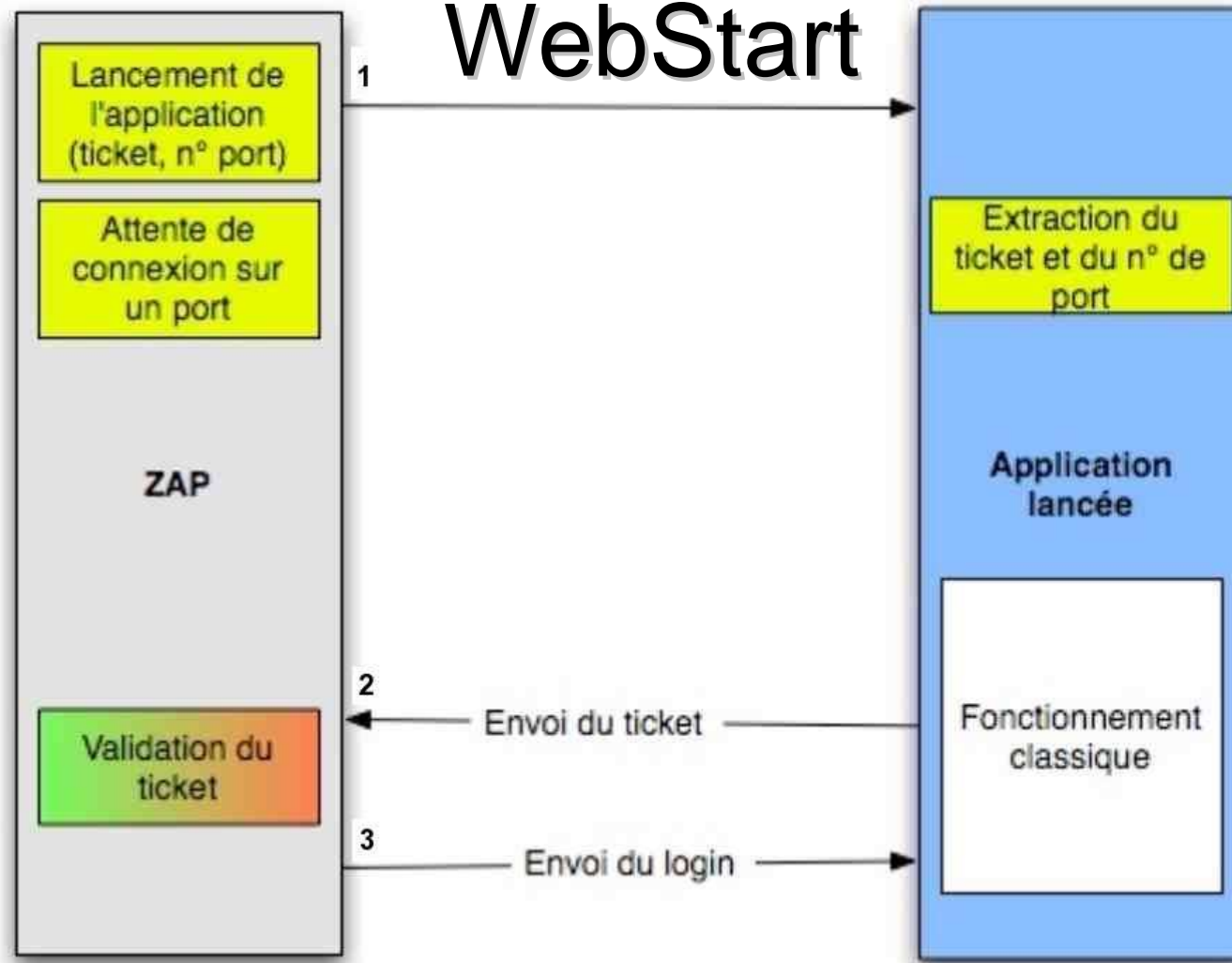
5. Lancer l'appli en lui transmettant le login utilisateur

Le Cookie TGC est mémorisé par Zap pour futures requêtes auprès de CAS.

Il permet de ré-authentifier l'utilisateur auprès de CAS sans re-saisir ses identifiants (login + mot de passe)

A chaque lancement d'appli, on revalide l'authentification (ZAP rejoue le ticket pour en vérifier la validité)

Applications Exécutable ou WebStart



(Ticket ZAP : équivalent du ST de CAS)

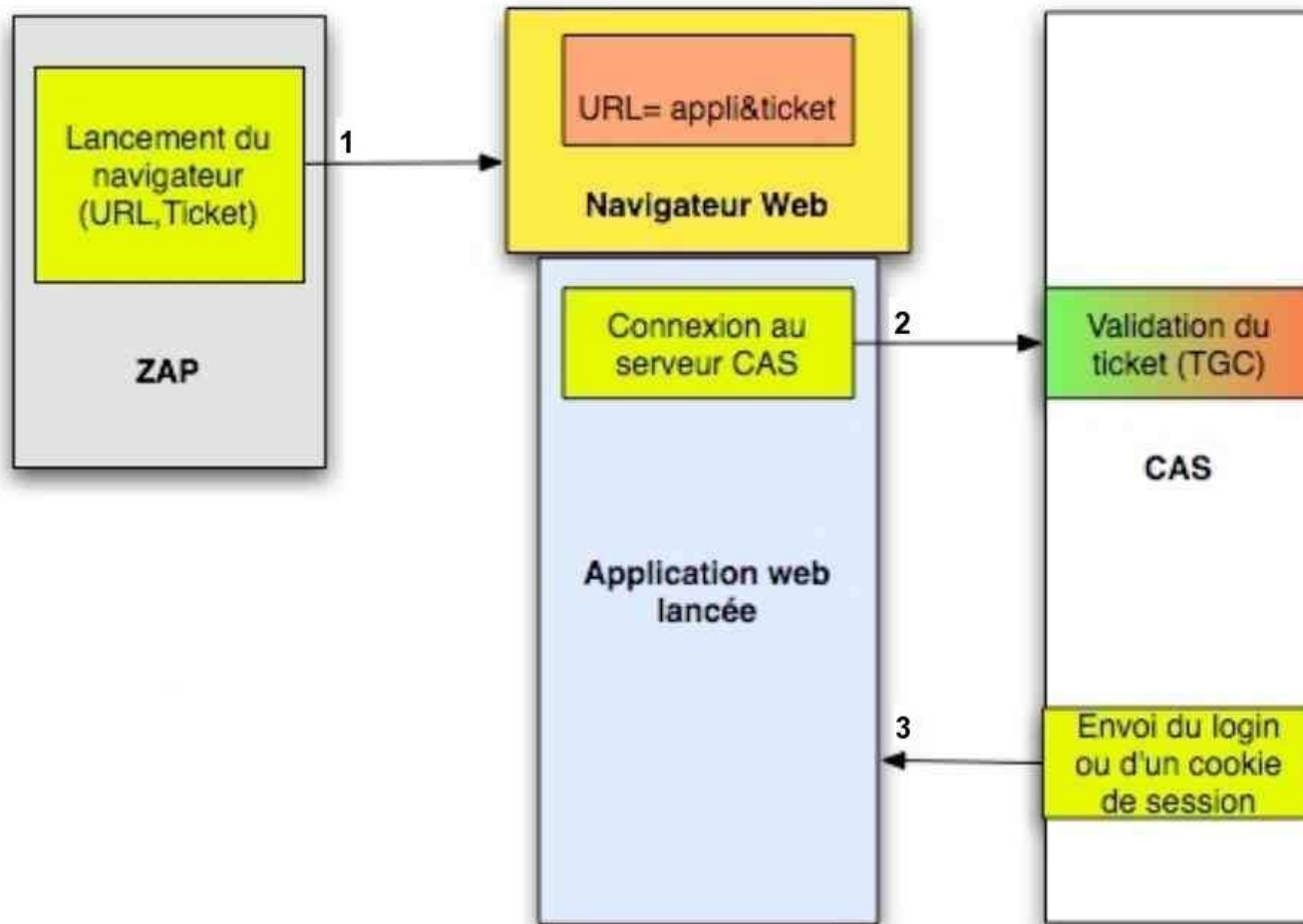
1. ZAP lance l'appli et transmet un ticket et le n° de port TCP

2. L'application contacte ZAP sur ce port et lui renvoie le ticket

ZAP vérifie le ticket. (Utilisable 1 seule fois)

3. S'il est valide, l'identifiant de l'utilisateur (login) est transmis à l'application

Applications Web



1. ZAP lance le navigateur Web avec URL contenant une action ZAP (avec le paramètre: cookie TGC)

L'appli extrait le Cookie.

Elle ajoute le cookie TGC comme cookie de session du Navigateur.

Elle redigire le navigateur vers la page d'accueil de l'appli.

2. Authentification classique CAS pour récupérer LE LOGIN :

Si cookie reconnu, pas besoin de re-saisir login+passwd

Sinon, formulaire d'authentification

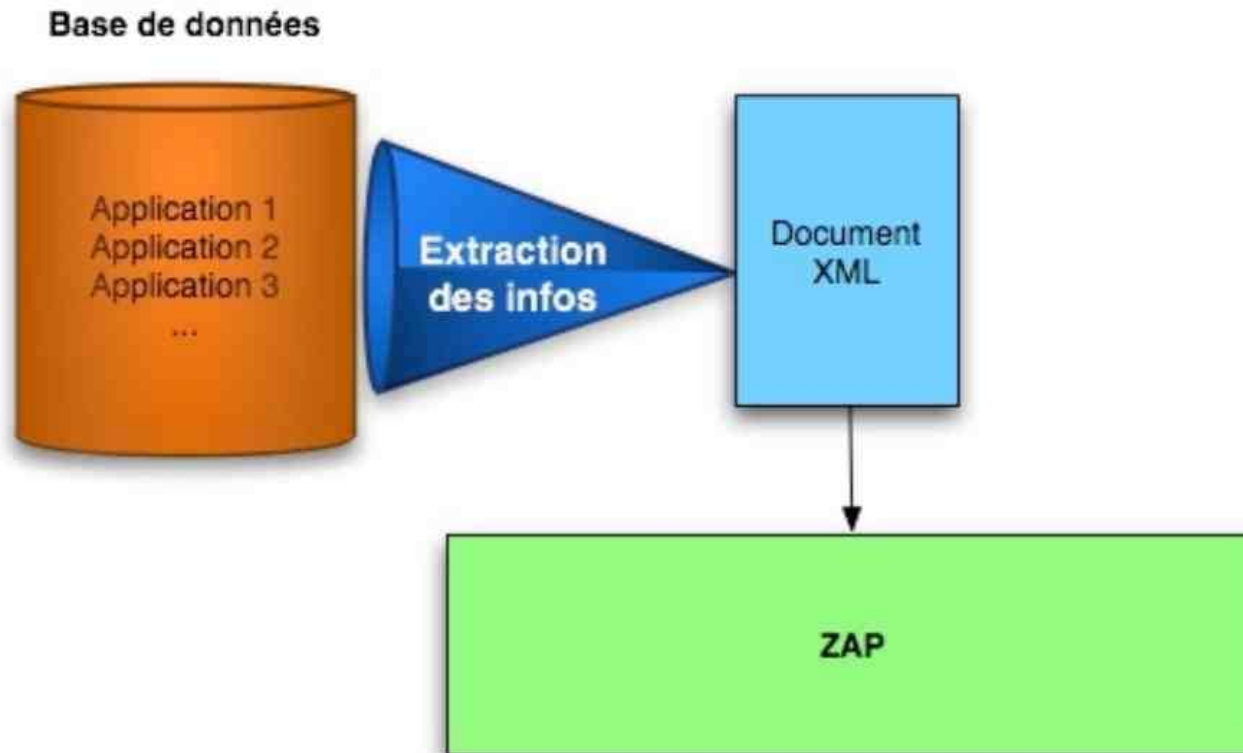
Niveaux d'authentification

- «none» : aucune authentification
- «login» : login et mot de passe (CAS)
- «certificat» : certificat et code PIN (token de sécurité USB avec certificat personnel : norme PKCS11)
- «login+certificat» : les 2 mon capitaine

✓ *Nous avons choisi le niveau «login»*

Sources XML

- Statique : fichiers XML sur un site web
- Dynamique : dans une base de données



Fonctionne avec le serveur d'authentification Cocktail : (il génère dynamiquement les fichiers XML pour ZAP grâce à une URL)

Au lancement, ZAP télécharge la liste des applis et construit l'interface Graphique (menu)

Barre de lancement rapide est stockée dans le « home » de l'utilisateur

L'utilisateur peut à tout moment rafraîchir le contenu de ZAP

Déploiement

Gestion du contenu de ZAP

(avec un formulaire Web)

La définition d'un theme

Jefyco
Missions
Prestations
Conventions
Inventaire

Nom* Jefyco

Commentaire Gestion Financiere et Comptable

UP DOWN

Supprimer

Valider (*Champ obligatoire)

La définition d'une application

Corossol-Inventaire
Abricot-Bordereaux
Carambole-Bon de commandes
Bibasse-Budget
Situations

Nom (long)* Abricot-Bordereaux

Nom (court)* Abricot

URL de lancement* http://hevea.inp-toulouse.fr/cgi-bin/WebObjects/Abricc

Type* WebStart

Authentification* login

Commentaire

URL de l'icone http://hevea/apache2-default/apps/zap/icones/logo_e

Theme(s) associé(s)* Jefyco
Missions
Prestations
Conventions
Inventaire

Sélection multiple possible

UP DOWN

Ajouter un séparateur

Supprimer

Valider (*Champ obligatoire)

Avantages de ZAP

- **Accès et lancement des applications simplifié**
 - authentification unique
 - plus de soucis de mode de lancement, d'emplacement
- **Déploiement simplifié**
 - une application Web permet d'administrer l'accès aux applications

Installation à l'INPT

- Pré-requis :
 - JRE 1.4, ANT
 - CAS Generic Handler, avec :
 - jdbc Oracle
 - certificat «tomcat» (si serveur d'application et CAS sur des machines différentes)
 - configuration pour nom d'utilisateur sur plus de 8 caractères
- Installation et configuration ZAP, avec :
 - signature des JAR client avec un certificat «cocktail»
 - obligatoire pour le téléchargement des JAR

Ce qui reste à faire à l'INPT ...

- Mettre ZAP sur un serveur Web
 - déploiement plus facile
- Installer un certificat du CRU :
 - certificat reconnu automatiquement par les navigateurs
- Utiliser le LDAP :
 - l'annuaire de l'établissement
- Coder les mots de passe des utilisateurs dans la base :
 - plus de sécurité

Premier bilan à l'INPT

- Un des premiers établissements du consortium Cocktail à utiliser ZAP
- Retour positif des utilisateurs
- Déployé sur ~ 30 postes (site Labège)
- Déploiement prévu sur ~ 150 postes d'ici la fin de l'année

Pour en savoir plus ...

- Application Open-Source Java
- Evolution du produit :
 - Maintenu mais aucune évolution depuis décembre 2005
 - Ajouter les droits d'utilisation des applications
- Bibliographie :
 - <http://www.univ-lr.fr/apps/support/zap/>
 - Article lors des JRES 2005