

L'architecture du gestionnaire de profils

Groupe 1B – version 2.5 – 12 décembre 2003

[Table des matières](#)

[Statut de ce document](#)

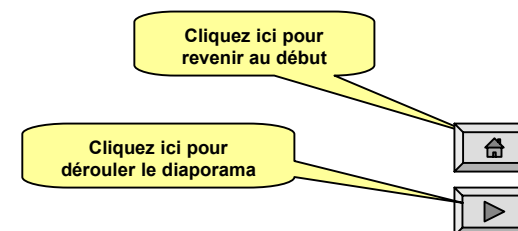


Table des matières

- [Besoins des librairies clientes](#)
 - [API des librairies clientes](#)
- [Spécification des groupes](#)
- [Architecture logicielle](#)
 - [Schéma complet](#)
- [Librairies clientes](#)
- [Architecture logicielle](#)
- [Versions prévues](#)



Statut de ce document

- **Historique**

- 2003-12-12 – version 2.5
 - Précisions sur la définition et la gestion des groupes (P. Aubry, J.-G. Avelin, R. Bourges, P. Gambarotto, J. Marchal, V. Mathieu, S. Qiang, B. Sor)
- 2003-11-26 – version 2.4
 - Ajout des groupes collaboratifs (V. Mathieu).
- 2003-11-26 – version 2.3
 - Intégration des remarques de R. Bourges.
- 2003-11-24 – version 2.2
 - Adoption de la dénomination des groupes officiels/personnels.
- 2003-11-23 – version 2.1
 - Intégration des remarques de V. Mathieu
 - PA : sauf le changement de groupes « partagés » en « globaux » que je préférerais voir discuté au sein de esup-dev.
- 2003-11-21 – version 2
 - Intégration des discussions de JRES (J.-M. Antoine, P. Aubry, J.-G. Avelin, R. Bourges, P. Gambarotto, J. Marchal, V. Mathieu, S. Montel, B. Sor, S. Zimmermann)
- 2003-11-14 – version 1 (P. Aubry)

- **Validation du document**

- au plus tard le vendredi 19 décembre 2003
- La version 2.5 est la dernière avant la spécification des APIs



Besoins des librairies clientes

- **Besoins des applications**
 - Pour un utilisateur
 - À quels groupes l'utilisateur U appartient-il ?
 - L'utilisateur U appartient-il au groupe G ?
 - L'utilisateur U appartient-il à (au moins) un des groupes G1, ..., Gn
 - Que vaut l'attribut A de l'utilisateur U (mono et multi-valués) ?

 - Pour un groupe
 - Quels utilisateurs sont membres du groupe G ?
 - Quelle est la description du groupe G ?

 - Quelle est la liste des groupes (et leurs description) ?

- **Besoins spécifiques à WebDAV**
 - Pour un groupe ou un utilisateur
 - À quels groupes {l'utilisateur U | le groupe G} appartient-il directement ?

 - Pour un groupe
 - Quels sont les membres du groupe G ?



API des librairies clientes (en Java)

- **Nom du package : org.esup.profiling.client**
- **Les classes visibles**
 - class Principal; // un acteur, utilisateur ou groupe
 - class User extends Principal; // un utilisateur
 - class Group extends Principal; // un groupe



API des librairies clientes (en Java)

- **La classe Principal**

- Construction `Principal(String pName);`
- Recherche des groupes d'appartenance directe `List Principal.getDirectMembership();`
- Recherche des groupes d'appartenance `List Principal.getMembership();`

- **La classe User**

- Construction `User(String uName);`
- Recherche des groupes privés `List User.getPrivateGroups();`
- Appartenance à un ou des groupes (directe ou indirecte) `boolean User.isFromGroup(Group g);`
`boolean User.isFromGroupSet(List groups);`
- Recherche d'attributs `List User.getAttr(String AttrName);`

- **La classe Group**

- Construction `Group(String gName);`
- Type de groupe `boolean Group.isShared();`
`boolean Group.isPrivate();`
- Recherche des membres directs `List Group.getDirectMembers();`
- Recherche des utilisateurs membres (indirects) `List Group.getUsers();`
- Recherche de la description `String Group.toString();`

- **La classe (abstraite) Profiling**

- Version `String Profiling.getVersion();`
- Recherche de tous les groupes partagés `List Profiling.getSharedGroups();`



Spécification des groupes de ESUP-Portail

	Officiels	Collaboratifs	Personnels
Visibilité	Tous les utilisateurs		Le propriétaire du groupe seulement
Spécification	Requêtes sur le SI	Liste d'utilisateurs et/ou de groupes	
Modification	Aucune	Manuelle	
Mode de modification	Fichier de configuration, Puis application CGI	Application CGI, WebDAV	
Mode d'accès	Web Service, puis RMI, puis SAML		



Les groupes officiels

- **Ils sont basés sur des requêtes sur le SI**
 - Requêtes (LDAP, SQL, fichiers, NIS, ...) sur des back-ends du SI
- **Ils sont utilisables par tous les utilisateurs**
- **Ils sont gérés par les administrateurs de l'ENT**
 - Déclarés et spécifiés par les administrateurs
 - Leur déclaration est faite dans un premier temps directement dans le gestionnaire de profils (grâce à un fichier de configuration), puis dans un deuxième temps par une application web dédiée, point d'accès privilégié à l'espace de stockage, s'appuyant sur le SSO
- **Seule leur déclaration (requête(s) de construction) est modifiable (pas leur contenu)**



Les groupes collaboratifs

- **Un groupe collaboratif est une liste d'utilisateurs et/ou de groupes**
 - Les groupes membres peuvent être officiels ou collaboratifs
- **Ils sont utilisables par tous les utilisateurs**
 - Exactement comme les groupes officiels
- **Ils sont gérés (créés, modifiés, supprimés) par des utilisateurs particuliers, désignés par les administrateurs de l'ENT**
 - À l'aide d'une application web dédiée, s'appuyant sur le SSO
 - Directement à l'aide du protocole WebDAV (ACP)
- **Ils sont physiquement stockés dans un back-end, dans la pratique probablement une base de données.**

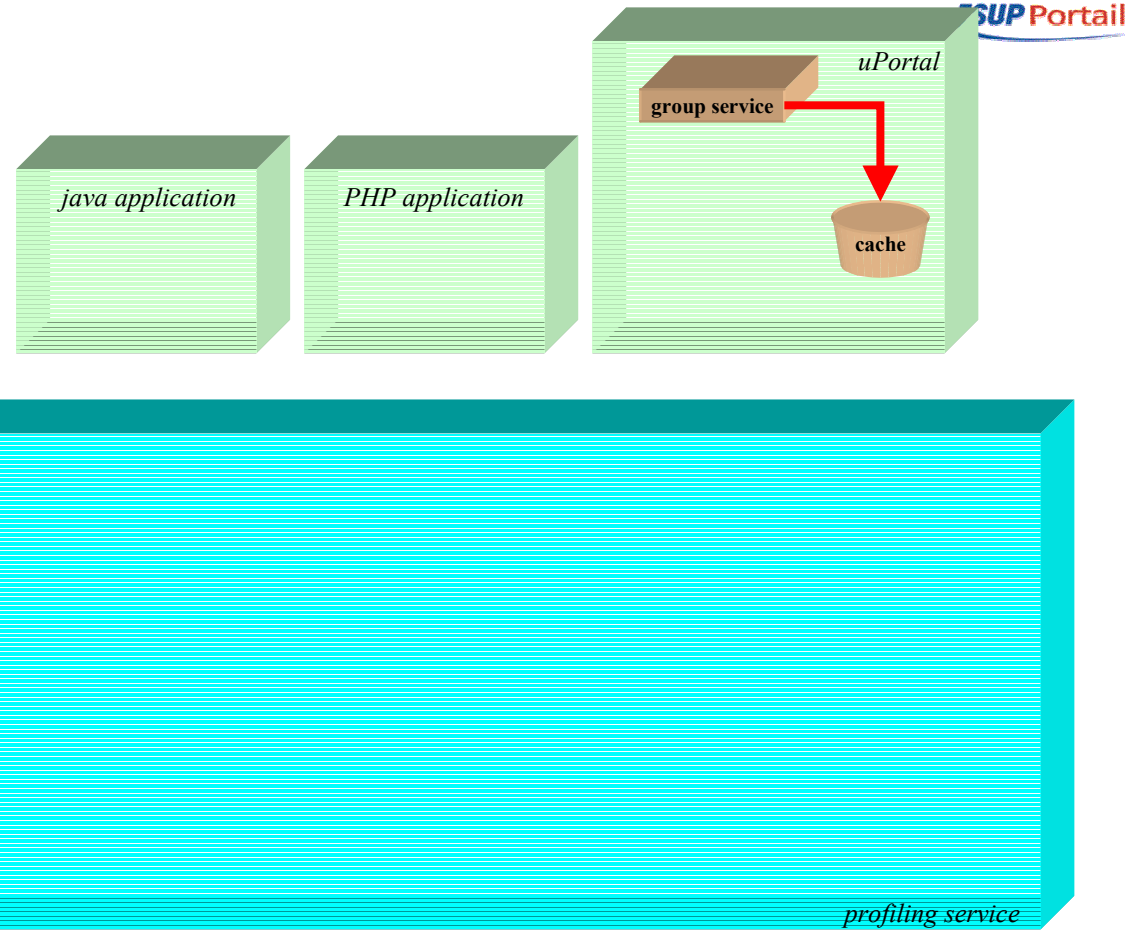


Les groupes personnels

- **Un groupe personnel est une liste d'utilisateurs et/ou de groupes**
 - Les groupes membres peuvent être personnels, collaboratifs ou officiels
- **Ils sont personnels**
 - Ils ne sont utilisables que par l'utilisateur auquel ils appartiennent
 - Pour positionner une ACL par exemple
 - Ils sont invisibles des autres utilisateurs
 - Mais sont pris en compte s'ils conditionnent l'accès à une ressource
- **Ils sont gérés (créés, modifiés, supprimés) par les utilisateurs.**
 - À l'aide d'une application web dédiée, s'appuyant sur le SSO
 - Directement à l'aide du protocole WebDAV (ACP)
- **Ils sont physiquement stockés dans un back-end**
 - Dans la pratique probablement une base de données ou l'annuaire LDAP
 - Le stockage dans l'annuaire LDAP permet l'interrogation par les applications non intégrées à l'ENT, mais pouvant s'appuyer sur LDAP
 - Note : dans la suite de ce document, les groupes personnels et collaboratifs sont stockés dans un seul back-end, accessibles seulement par les interfaces du gestionnaire de profils. Dans la pratique, les back-ends des groupes pourront être séparés, par exemple :
 - Un annuaire LDAP (externe) pour les groupes collaboratifs
 - Une base de données (interne) pour les groupes personnels



Architecture logicielle

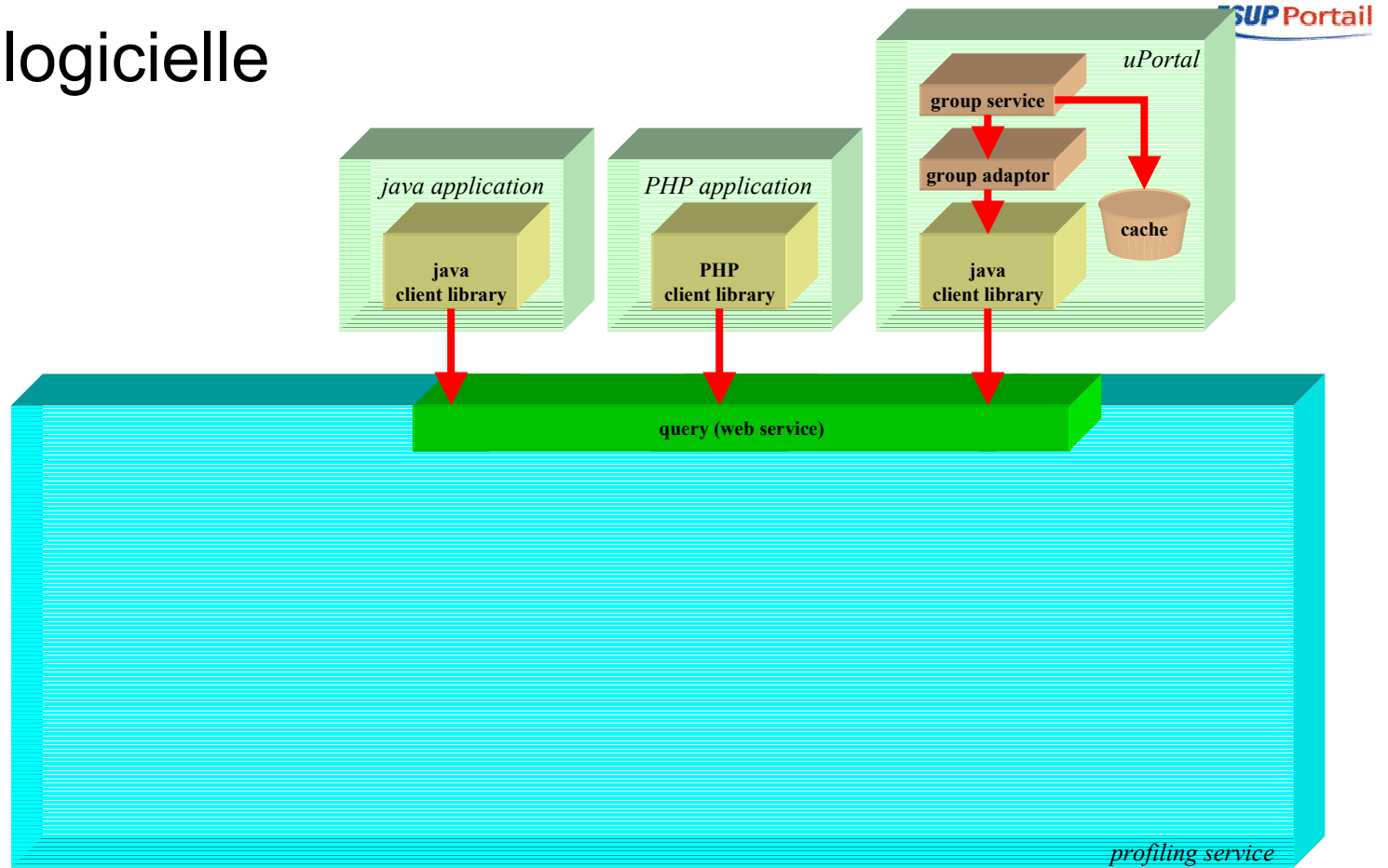


- **Clients du gestionnaire de profils**

- Le gestionnaire de profils (*profiling service*) est interrogé par des applications Java, PHP, ..., dont uPortal, qui possède son propre gestionnaire de groupes intégré.



Architecture logicielle

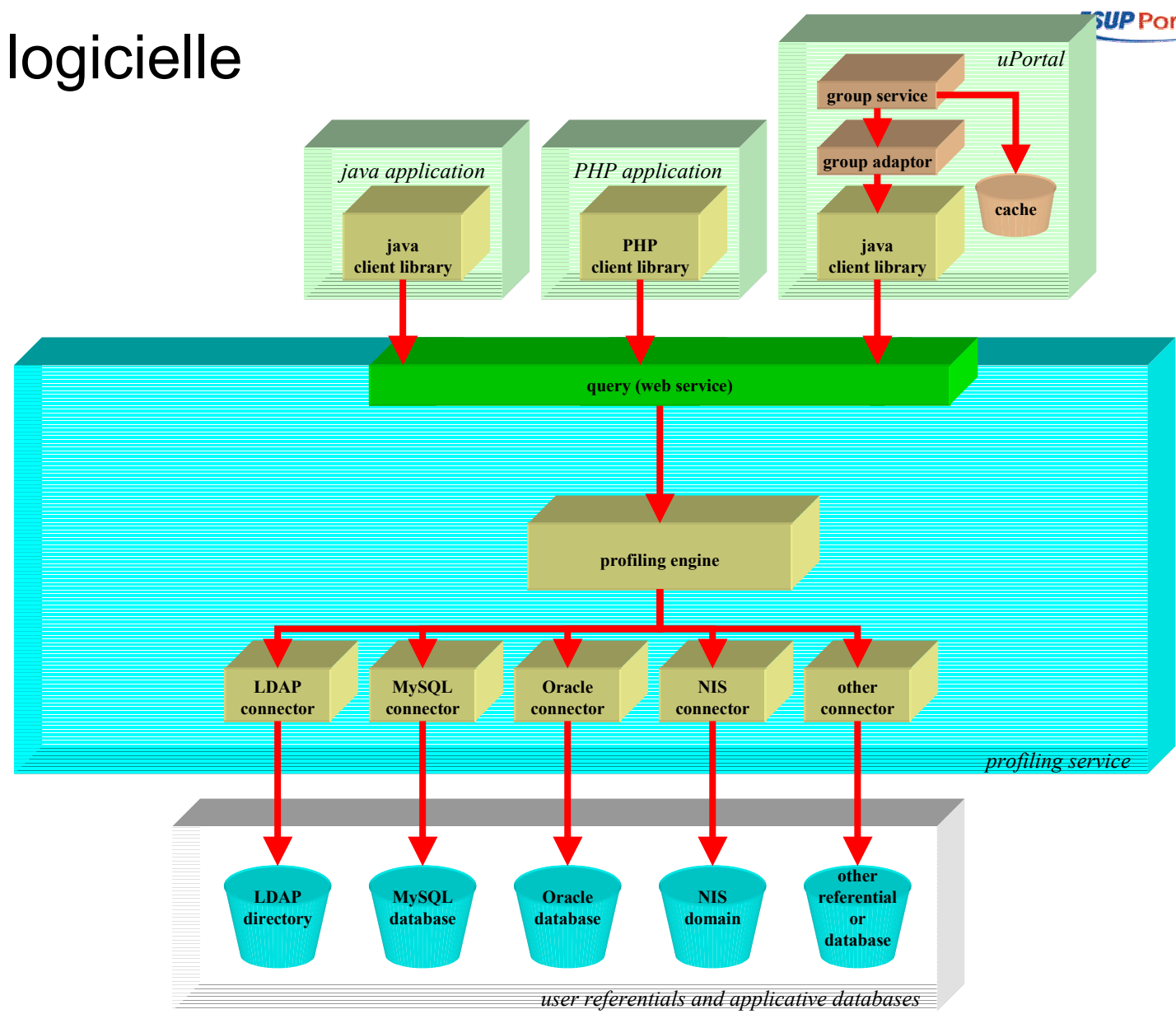


- **Interrogation du gestionnaire de profils**

- Elle est faite à l'aide de librairie clientes installées dans les applications, à travers l'appel d'un *web service*.

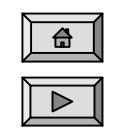


Architecture logicielle

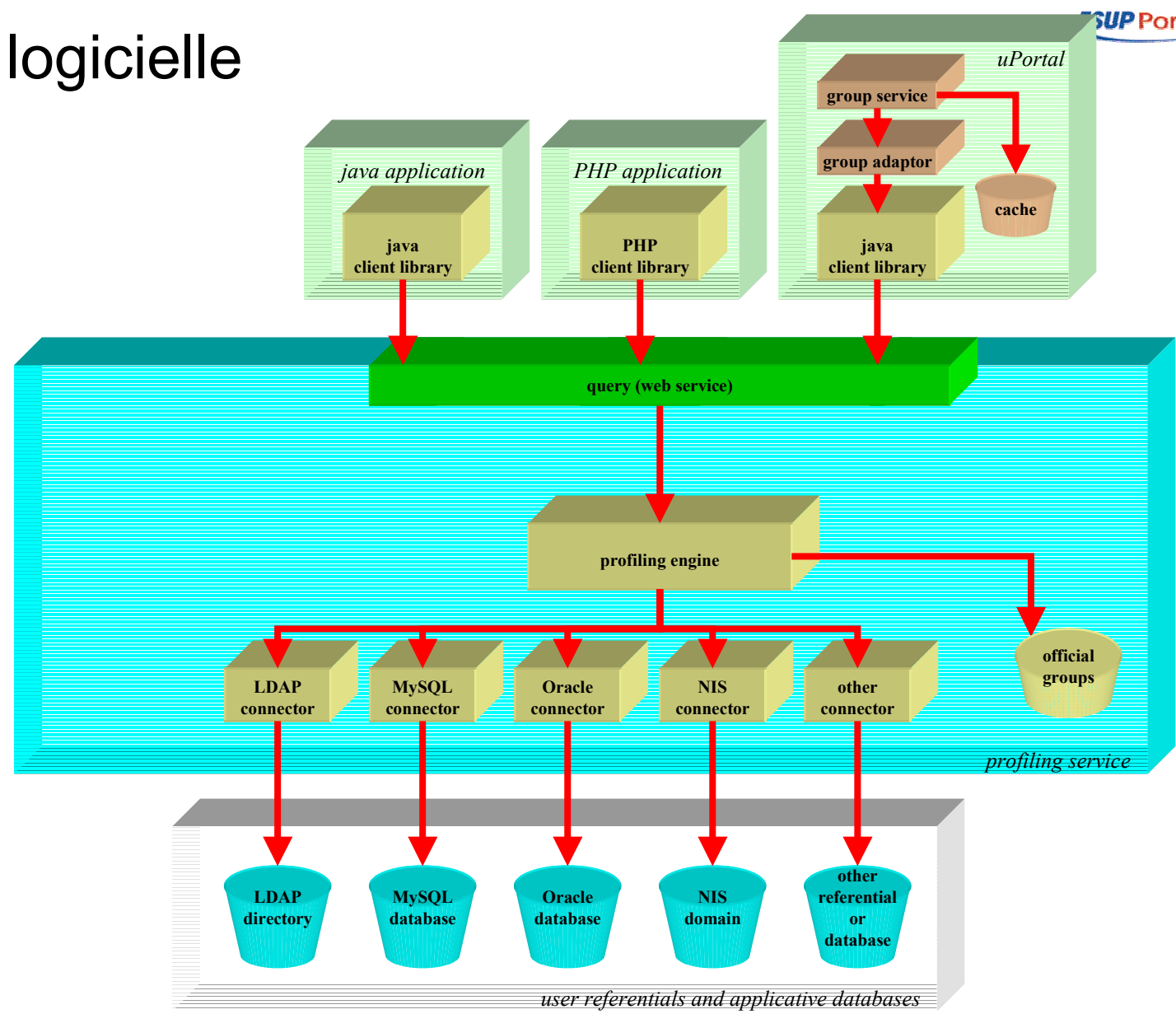


- **Groupes « officiels »**

- Le moteur de profils s'appuie sur des connecteurs accédant à des bases de données applicatives et des référentiels utilisateurs. Les groupes « officiels » issus des requêtes à ces données sont globaux et partagés (utilisables par tous les utilisateurs de l'ENT).

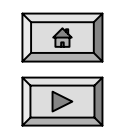


Architecture logicielle

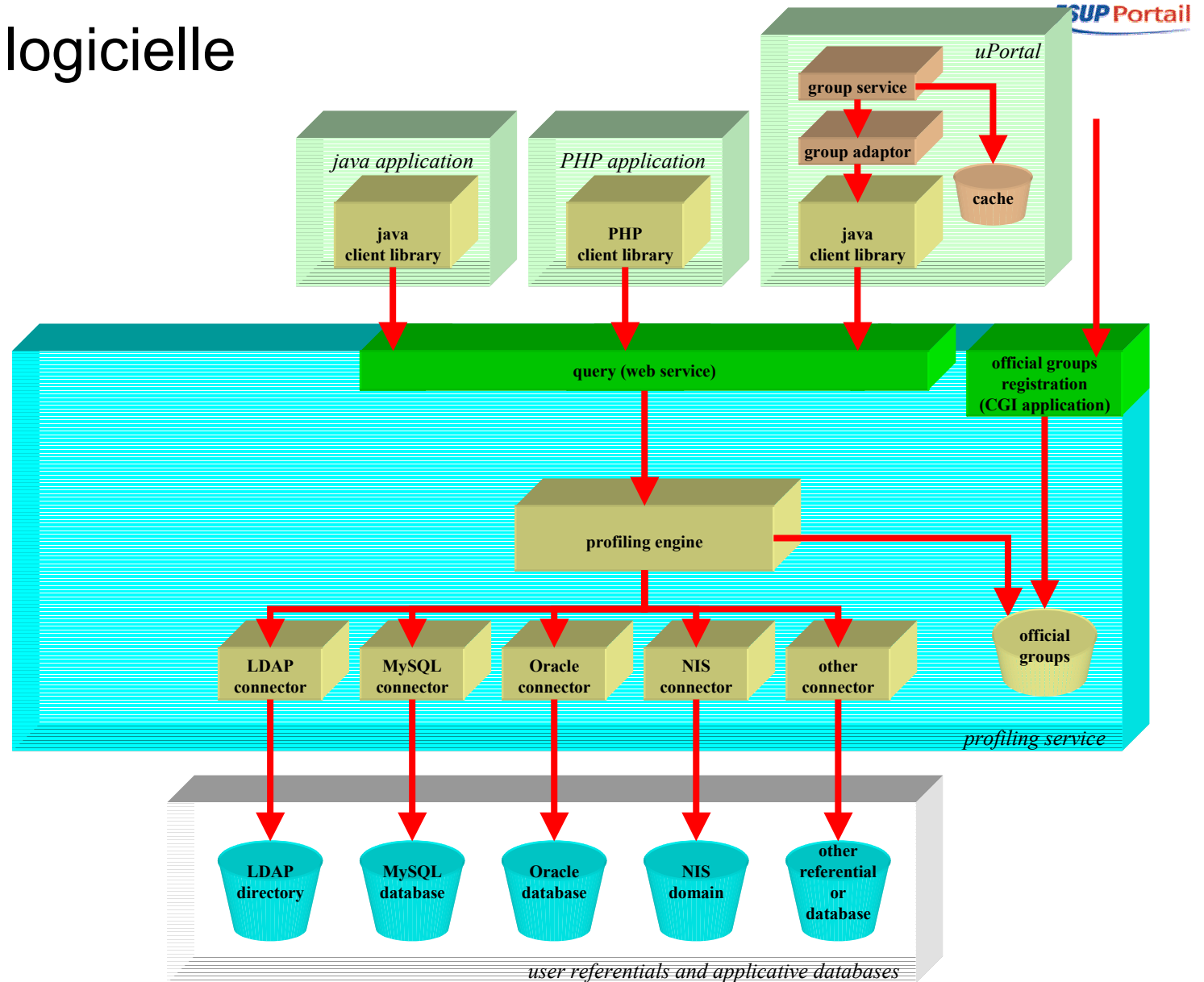


- **Déclaration des groupes officiels**

- Pour être connus du moteur de profils, les groupes officiels doivent être déclarés dans le gestionnaire (pour que le moteur de profil sache quelles requêtes effectuer).



Architecture logicielle

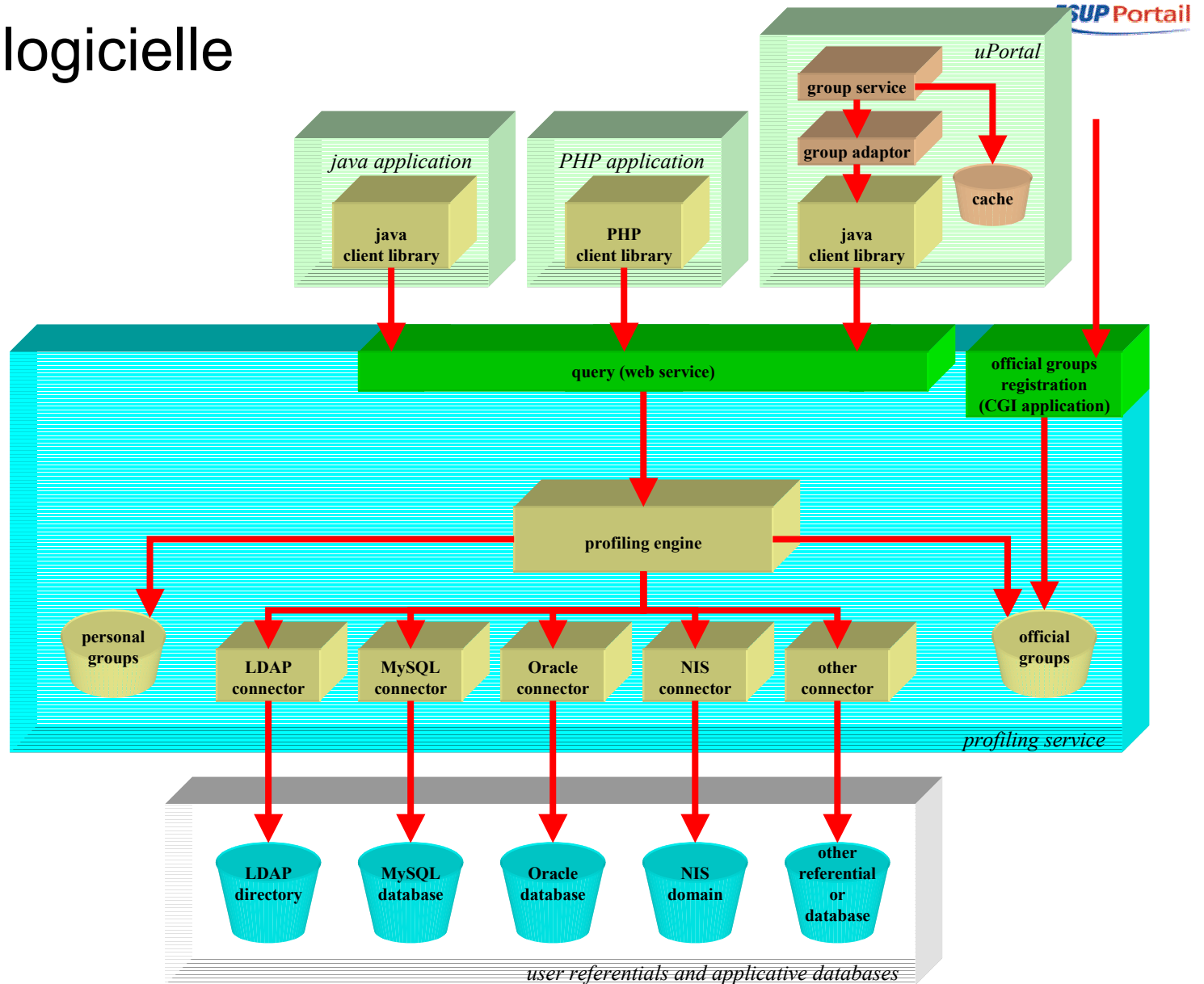


- **Enregistrement des groupes officiels**

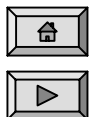
- Les groupes officiels sont enregistrés par une application CGI, accessible seulement aux administrateurs de l'ENT.



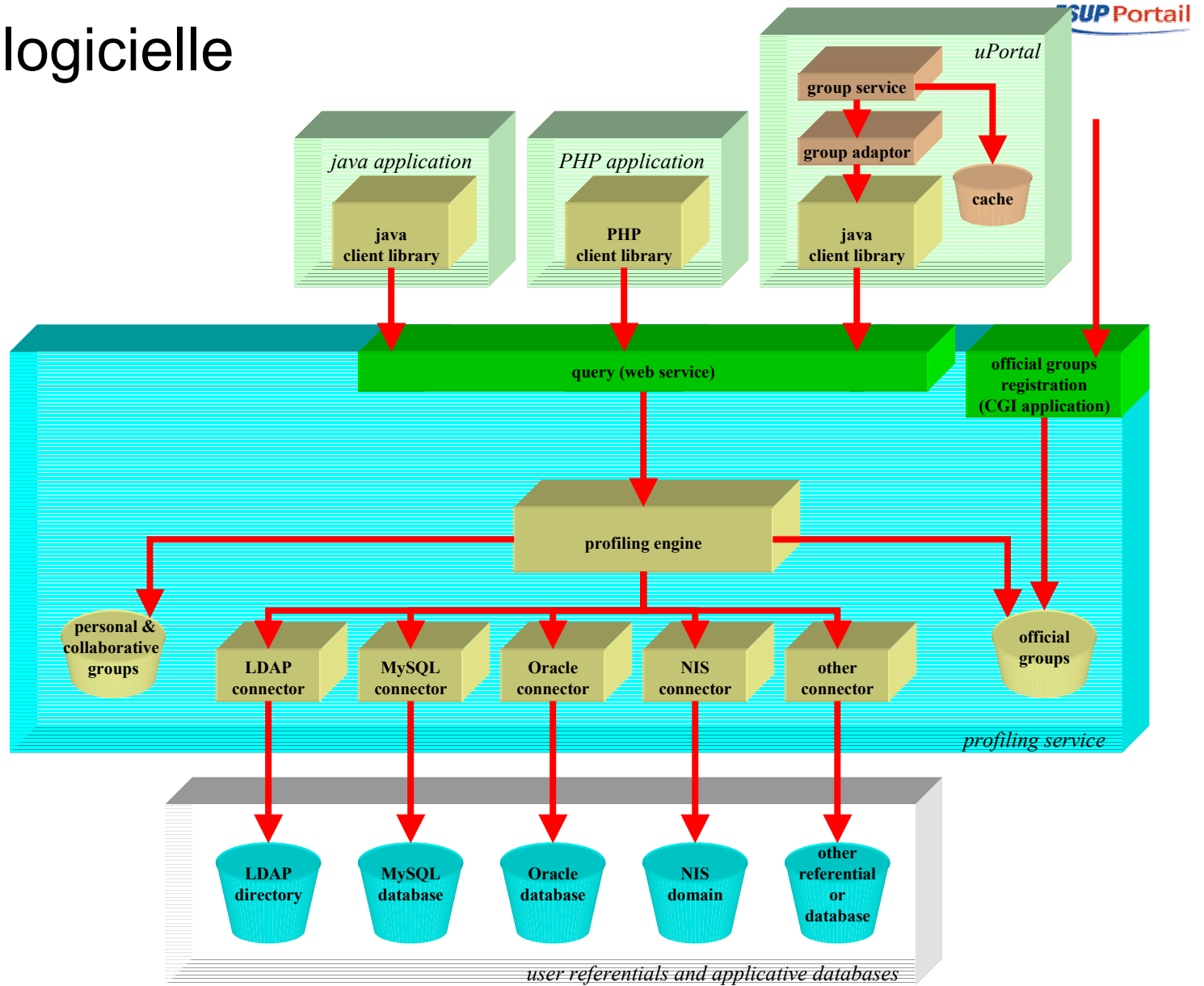
Architecture logicielle



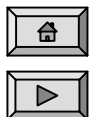
- **Groupes personnels**



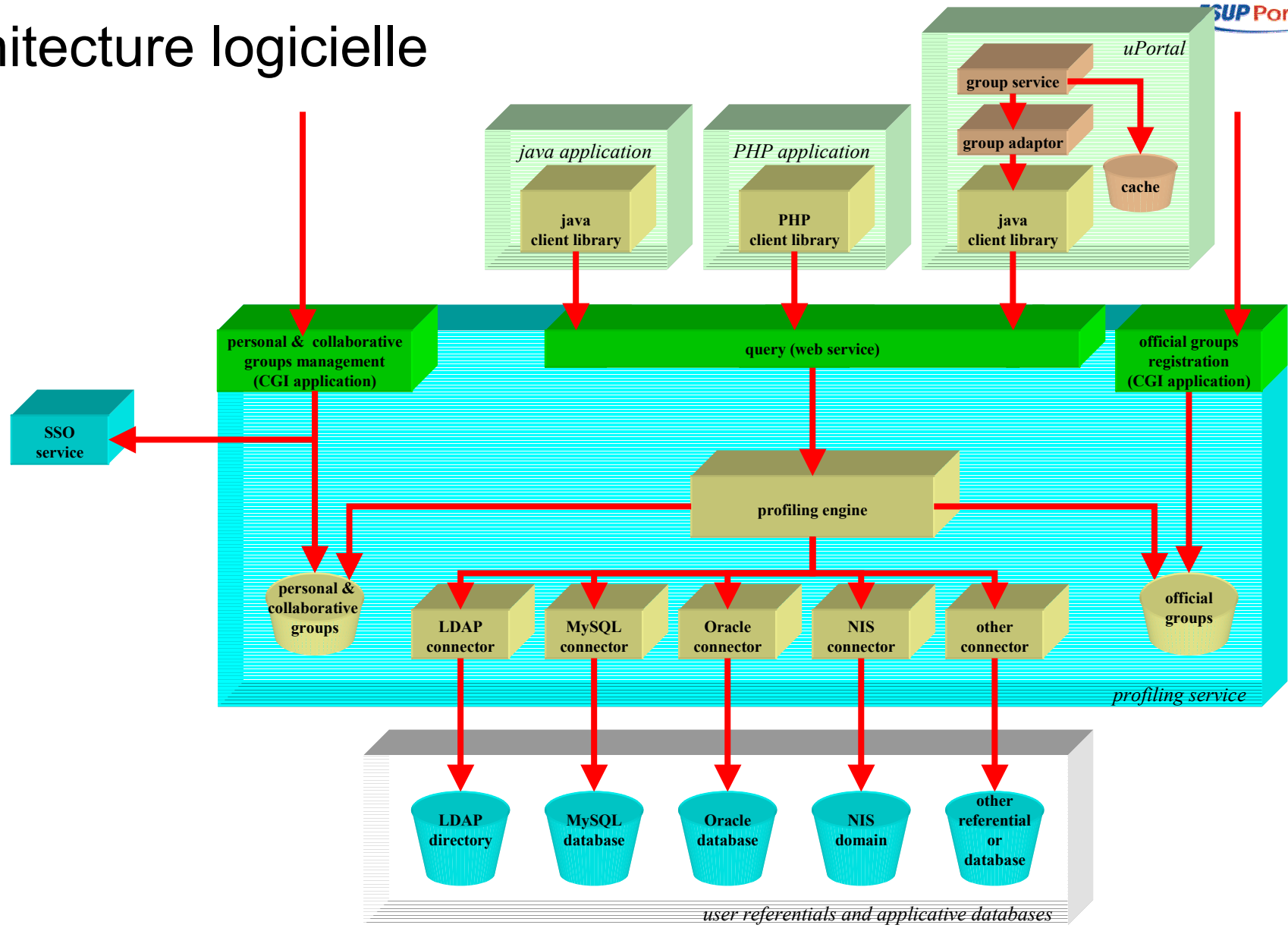
Architecture logicielle



- **Groupes collaboratifs**

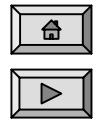


Architecture logicielle

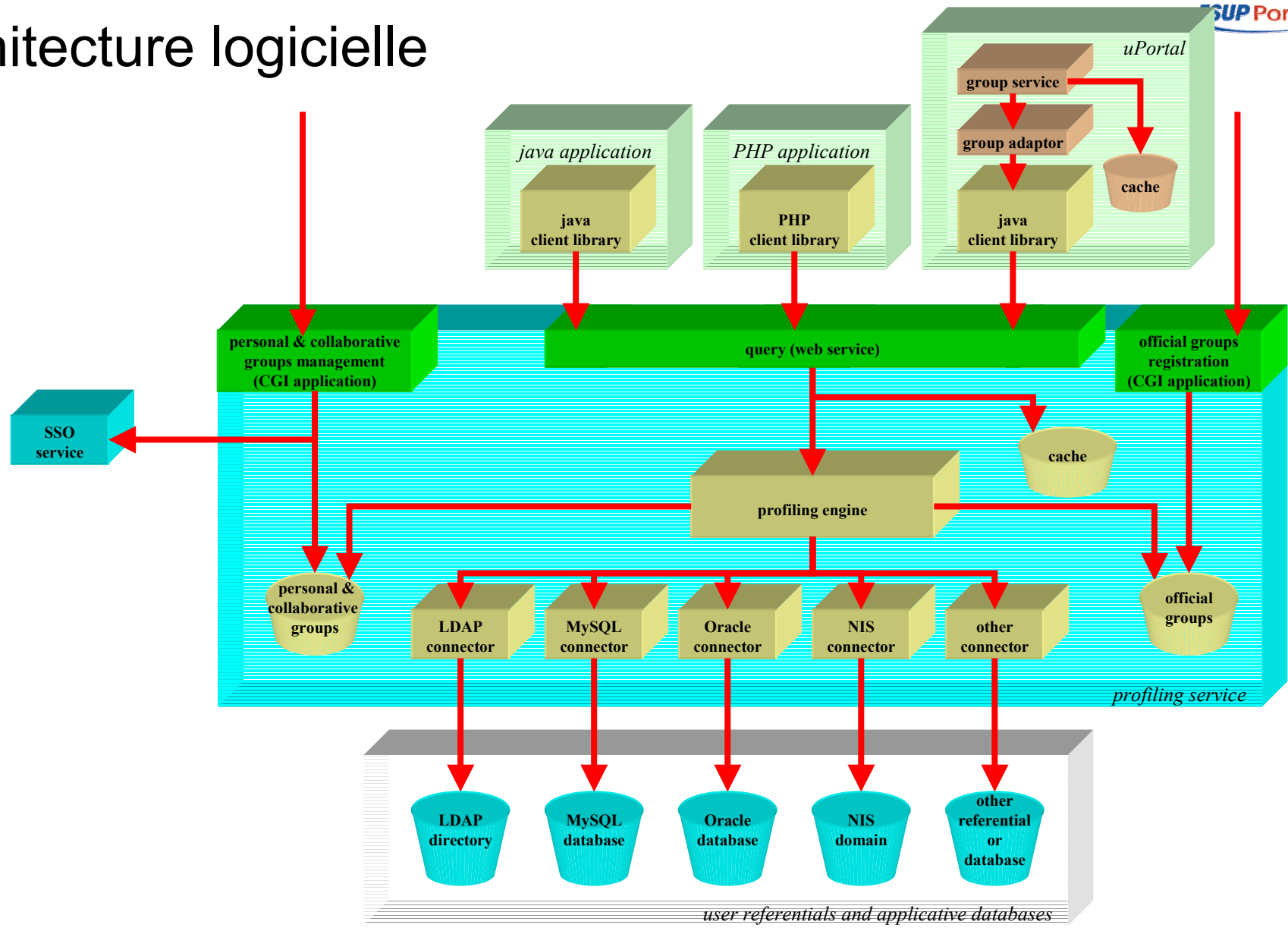


- **Gestion des groupes personnels et collaboratifs**

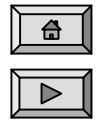
- Les utilisateurs gèrent leurs groupes personnels à travers une application CGI dédiée, qui s'appuie sur le service de Single Sign-On.



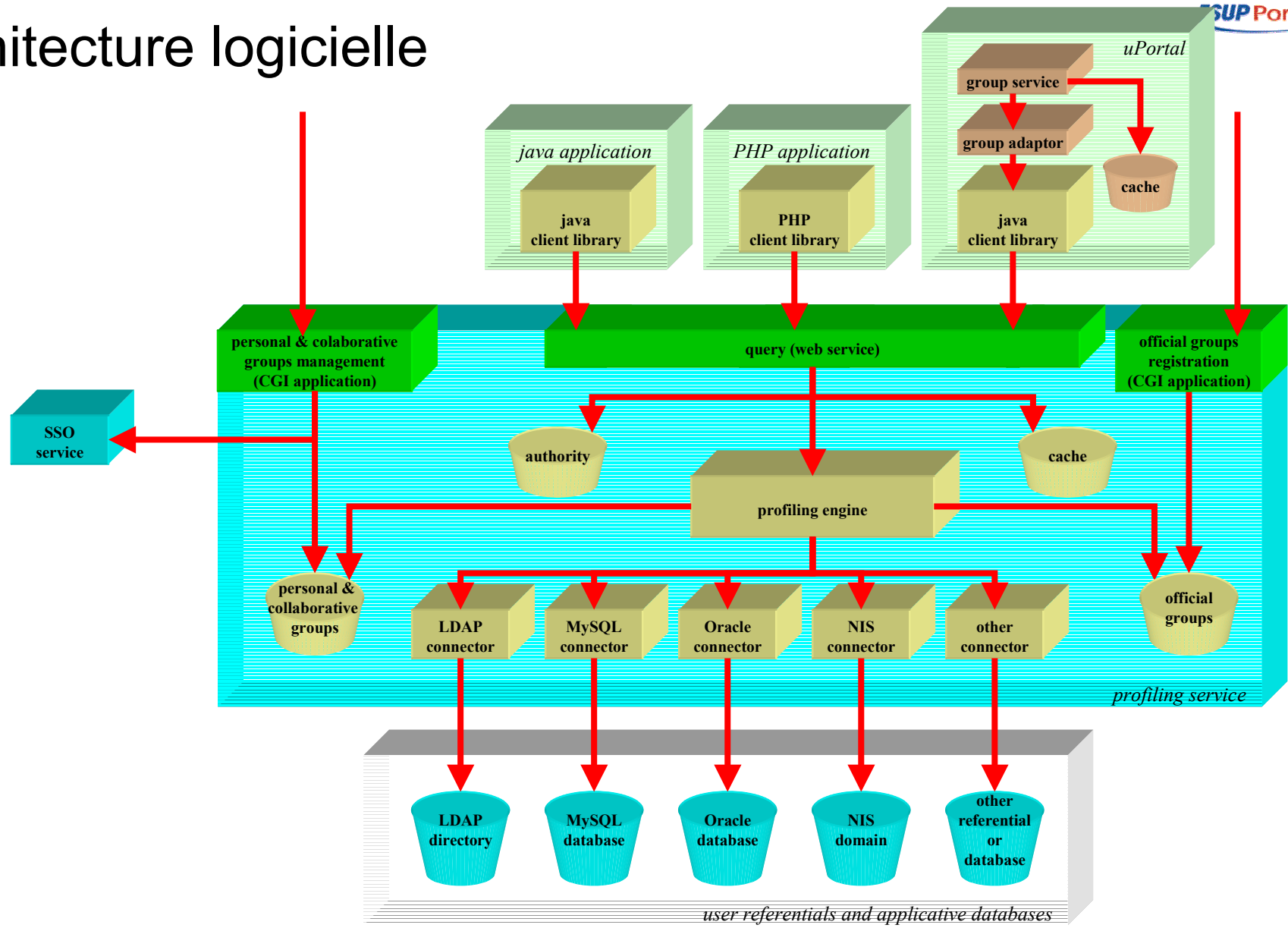
Architecture logicielle



- **Cache des requêtes**
 - Un cache permet de limiter la sollicitation des back-ends.

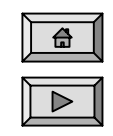


Architecture logicielle

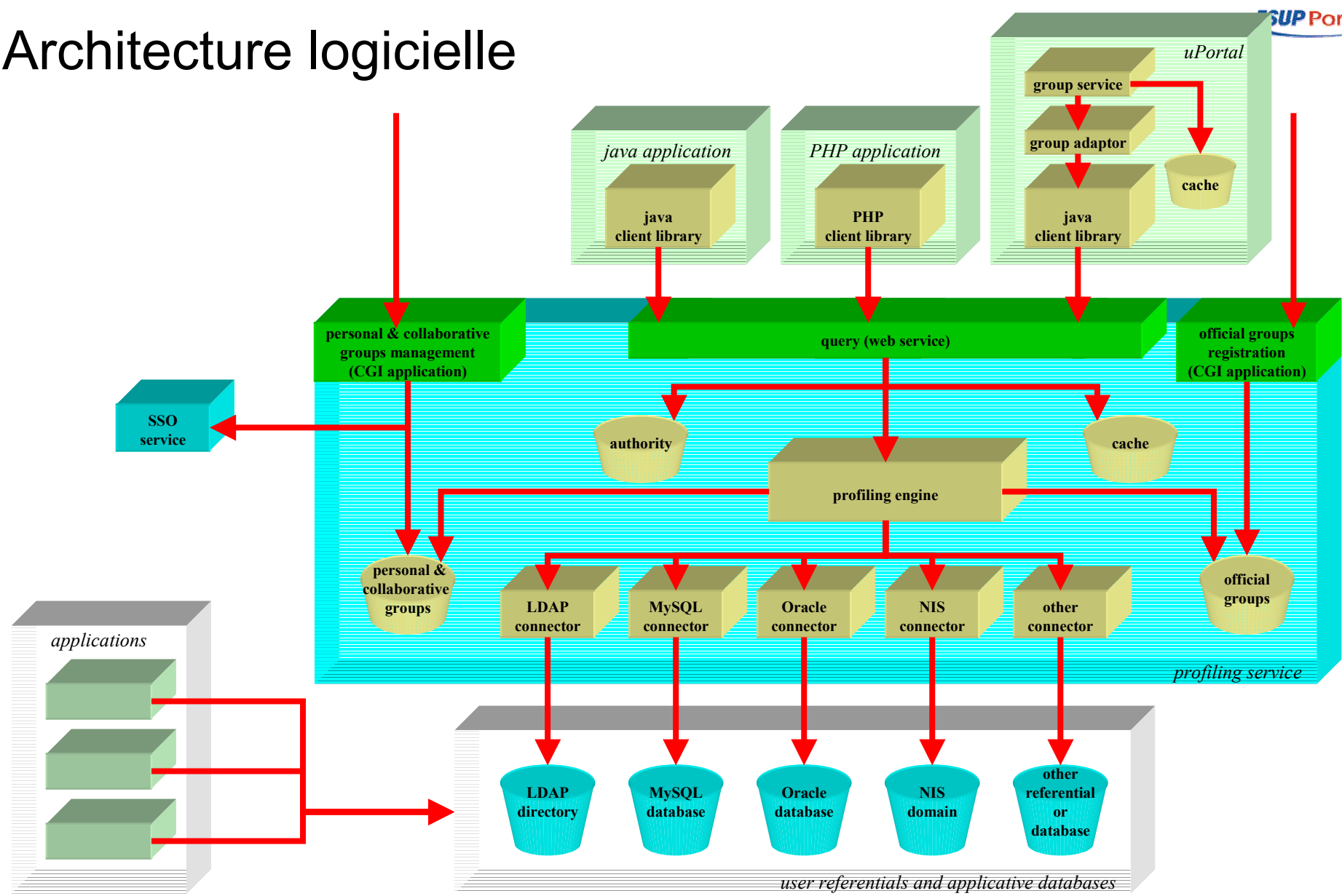


- **Autorité de distribution**

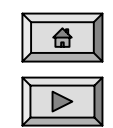
- Une autorité de distribution limite les attributs des utilisateurs qui peuvent être renvoyés aux applications.



Architecture logicielle



- **Modification des référentiels utilisateurs et des bases de données applicatives**
 - Le gestionnaire de profils ne fait qu'interroger les référentiels utilisateurs et des bases de données applicatives. Ce données sont modifiées par des applications tierces, à charge des établissements.



Versions prévues

- **Version 1 (maquette)**
 - Doit être rapidement utilisable et assez riche pour satisfaire les applications s'appuyant sur la notion de groupe (uPortal).
 - Version 1.0
 - Les librairies clientes implémentent la logique applicative.
 - Les groupes officiels sont construits uniquement sur les attributs LDAP.
 - Version 1.1
 - Les groupes officiels peuvent être construits sur les groupes LDAP.
- **Version 2 (diffusion)**
 - Version 2.0
 - La logique est déplacée dans le gestionnaire de profil, interrogeable par *web service*
 - Version 2.1
 - Cache des requêtes d'interrogation
 - Version 2.2
 - Introduction de nouveaux providers
 - Version 2.3
 - Remontée des attributs
 - Version 2.4
 - Ajout des groupes privés et collaboratifs
 - Version 2.5
 - Ajout de l'autorité de distribution
 - Version 2.6
 - Ajout de l'application CGI de gestion des groupes officiels
- **Version 3 (maturation)**
 - Conformité SAML



Version 1.0 (maquette)

- **Fonctionnalités**

- Librairies clientes
 - Ce sont elles qui implémentent toute la logique de *profiling*.
 - Leur API est définitive (pourra être étendue mais pas modifiée).
- Gestionnaire de profil
 - Il n'existe pas dans cette version.
- Référentiel utilisateur
 - Le seul référentiel utilisable est l'annuaire LDAP.
 - Les groupes sont tous officiels et construits en fonction des attributs des utilisateurs dans l'annuaire LDAP.

- **Travail à réaliser**

- Valider l'API
- Étudier les possibilités d'intégration de la librairie cliente dans uPortal
- Développer la recherche de groupes sur attributs dans un annuaire LDAP
 - Ce travail pourra être récupéré en version 2.
- Note : le développement d'une librairie autre que Java (PHP par ex.) ne pourra pas être récupéré dans les versions ultérieures.

- **Remarque**

- Les interactions entre le gestionnaire de profils et uPortal doit être abordée de manière concrète. Julien Marchal et Jean-Guy Avelin sont chargés de regarder la faisabilité de l'interaction.



Version 1.1 (maquette)

- **Nouvelles fonctionnalités**

- Référentiel utilisateur

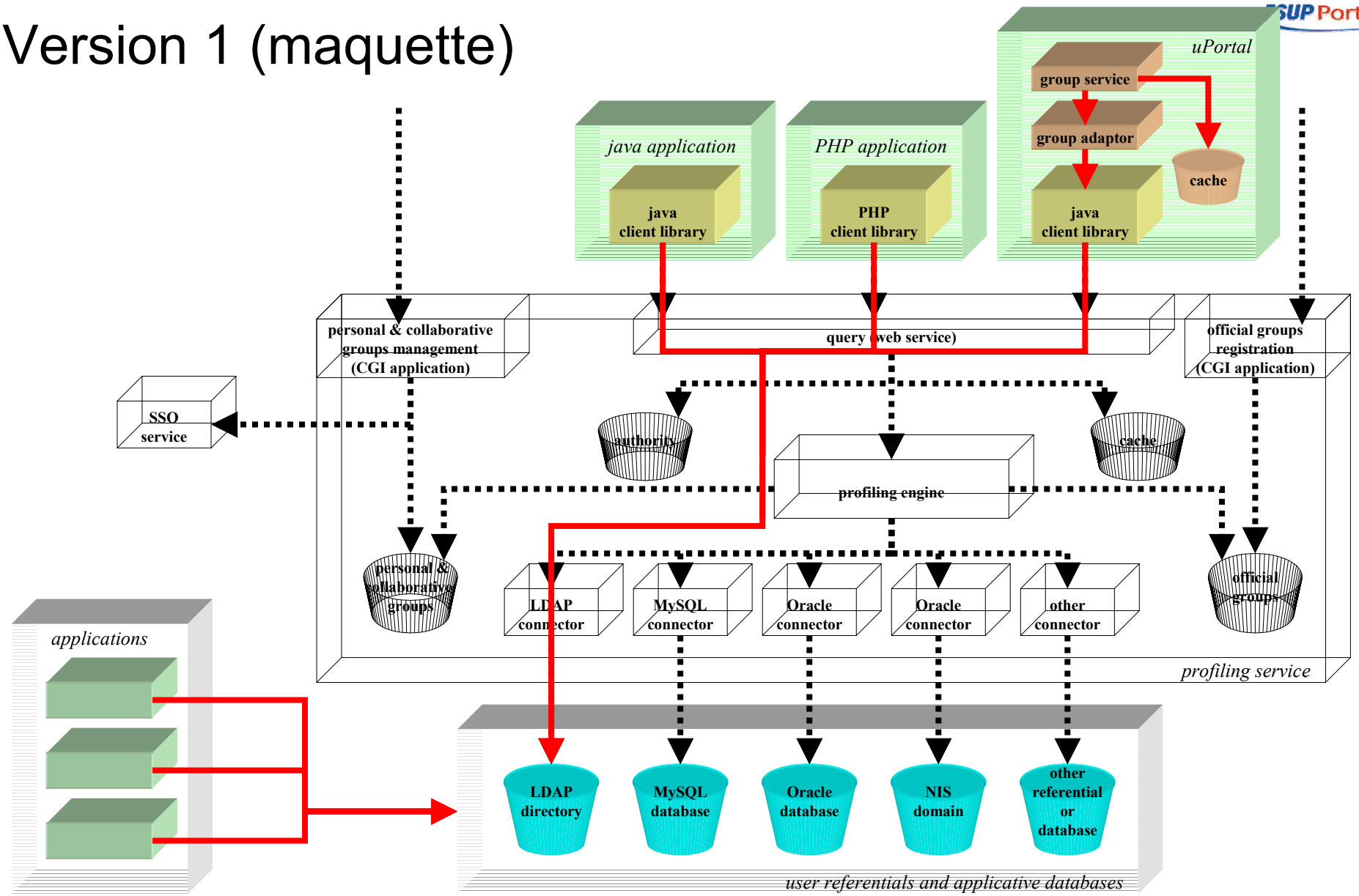
- Les groupes officiels sont construits non seulement sur les attributs, mais également sur les groupes LDAP.

- **Travail à réaliser**

- Écrire le bout de code qui va chercher dans les groupes LDAP.



Version 1 (maquette)



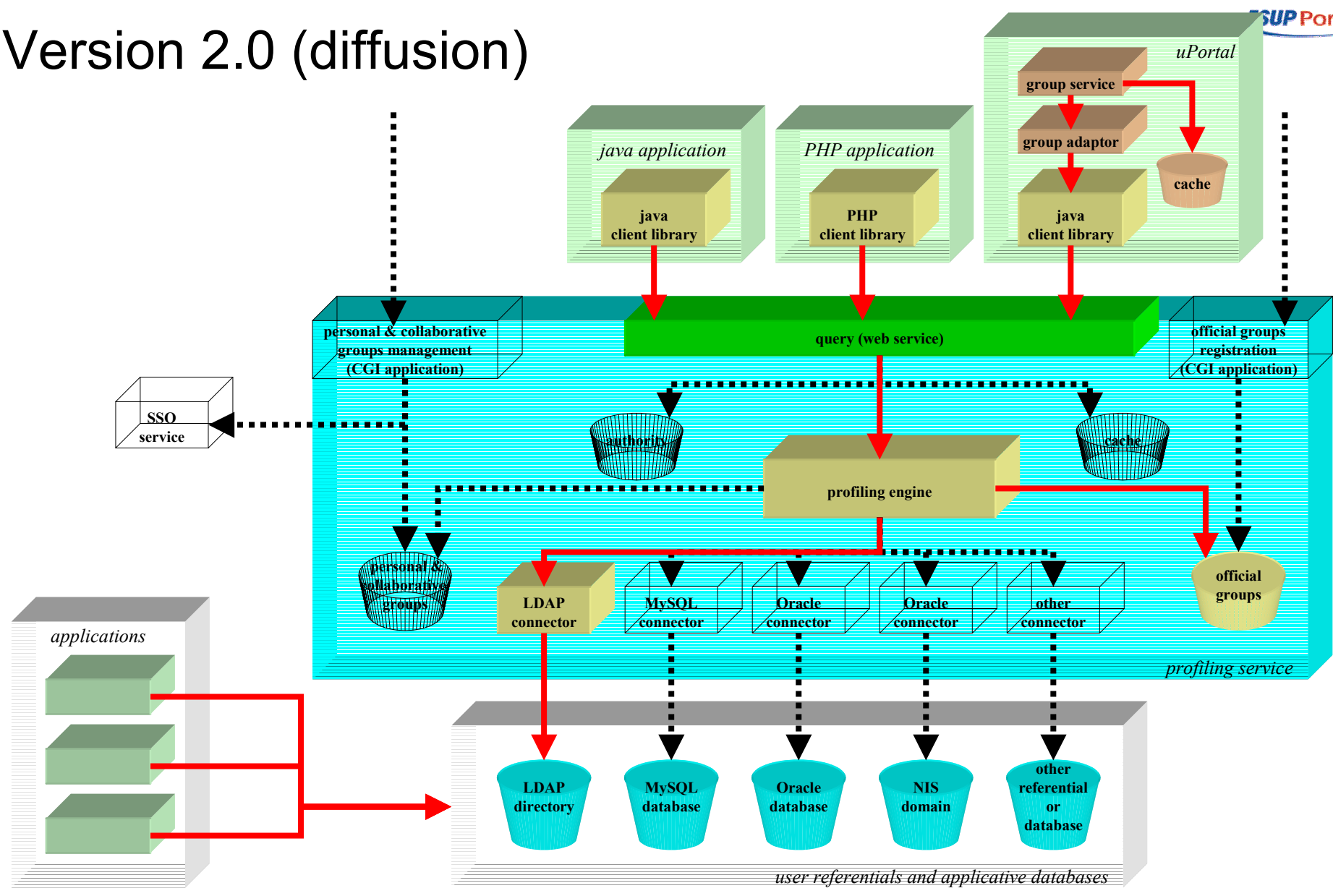
Version 2.0 (diffusion)

- **Nouvelles fonctionnalités**
 - La logique de *profiling* est déplacée dans le gestionnaire de profils.
 - Le gestionnaire de profils est interrogé via un *web service*.

- **Travail à réaliser**
 - Gestionnaire de profils
 - Récupérer la logique des librairies de la version 1.
 - Spécifier le stockage des groupes officiels.
 - En version 1, les groupes officiels pourront être stockés « en dur » (fichier XML par ex.).
 - Interfacer le moteur de profils avec les groupes officiels.
 - Transformer en *web service*.
 - Librairies clientes
 - Interfacer le *web service*.



Version 2.0 (diffusion)

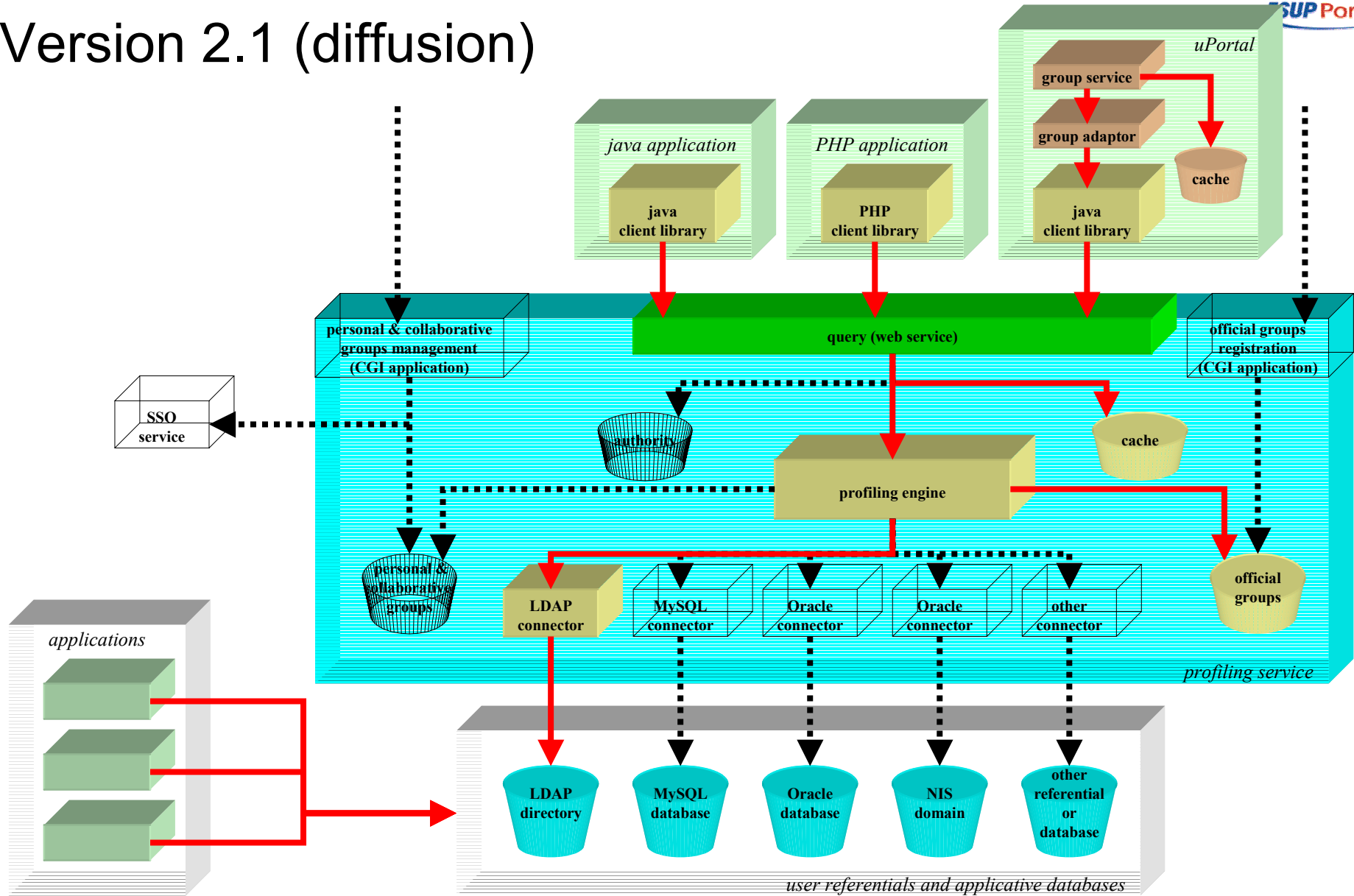


Version 2.1 (diffusion)

- **Nouvelles fonctionnalités**
 - Ajout du cache des requêtes du *web service*.
- **Travail à réaliser**
 - Spécifier et écrire le cache.



Version 2.1 (diffusion)

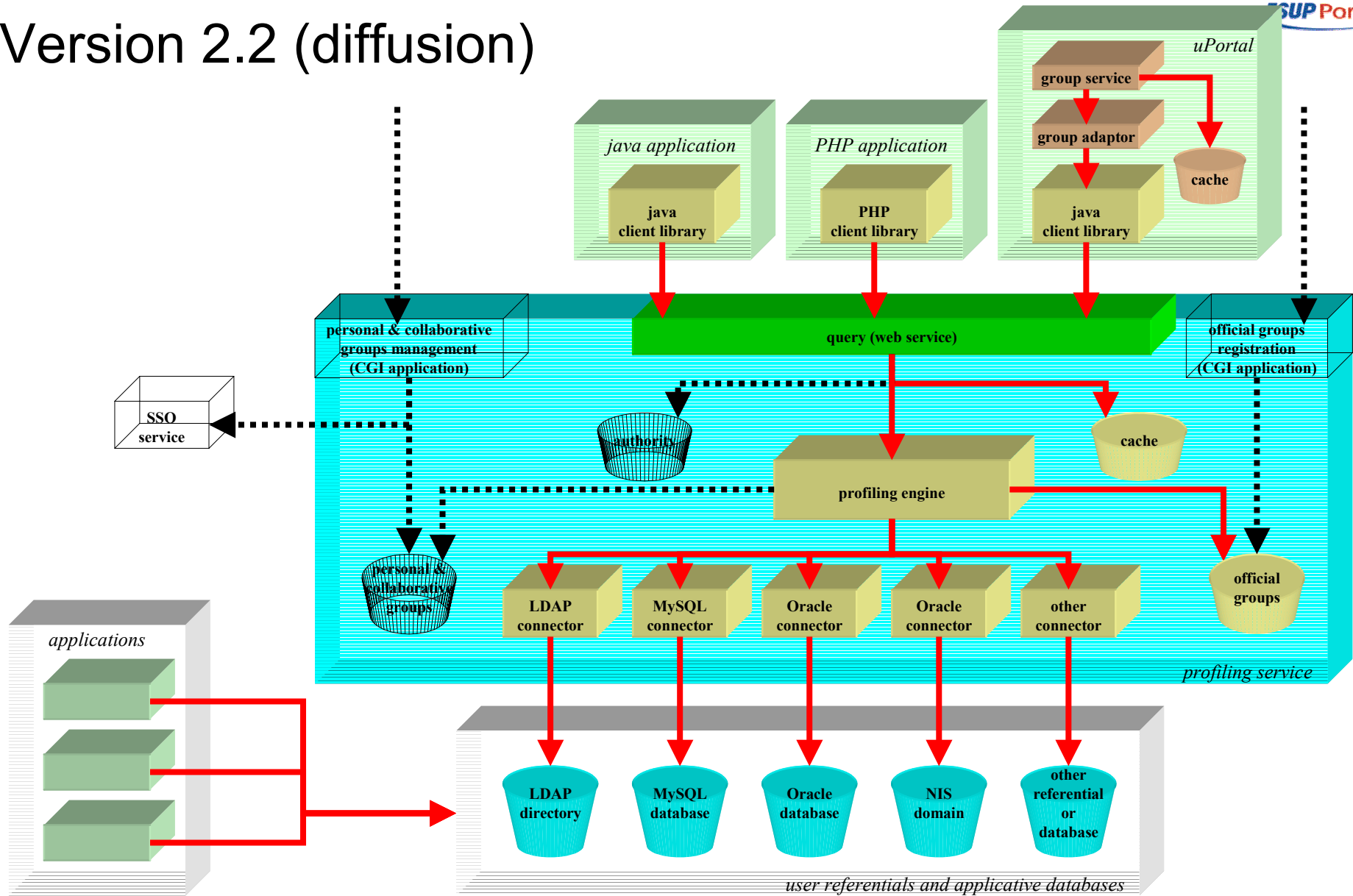


Version 2.2 (diffusion)

- **Nouvelles fonctionnalités**
 - Ajout de nouveaux *providers*
 - Par exemple des connecteurs Oracle, MySQL, NIS, ...
- **Travail à réaliser**
 - Développer les *providers*.



Version 2.2 (diffusion)



Version 2.3 (diffusion)

- **Nouvelles fonctionnalités**
 - Remontée des attributs
- **Travail à réaliser**
 - Remonter les attributs des référentiels vers l'API des applications

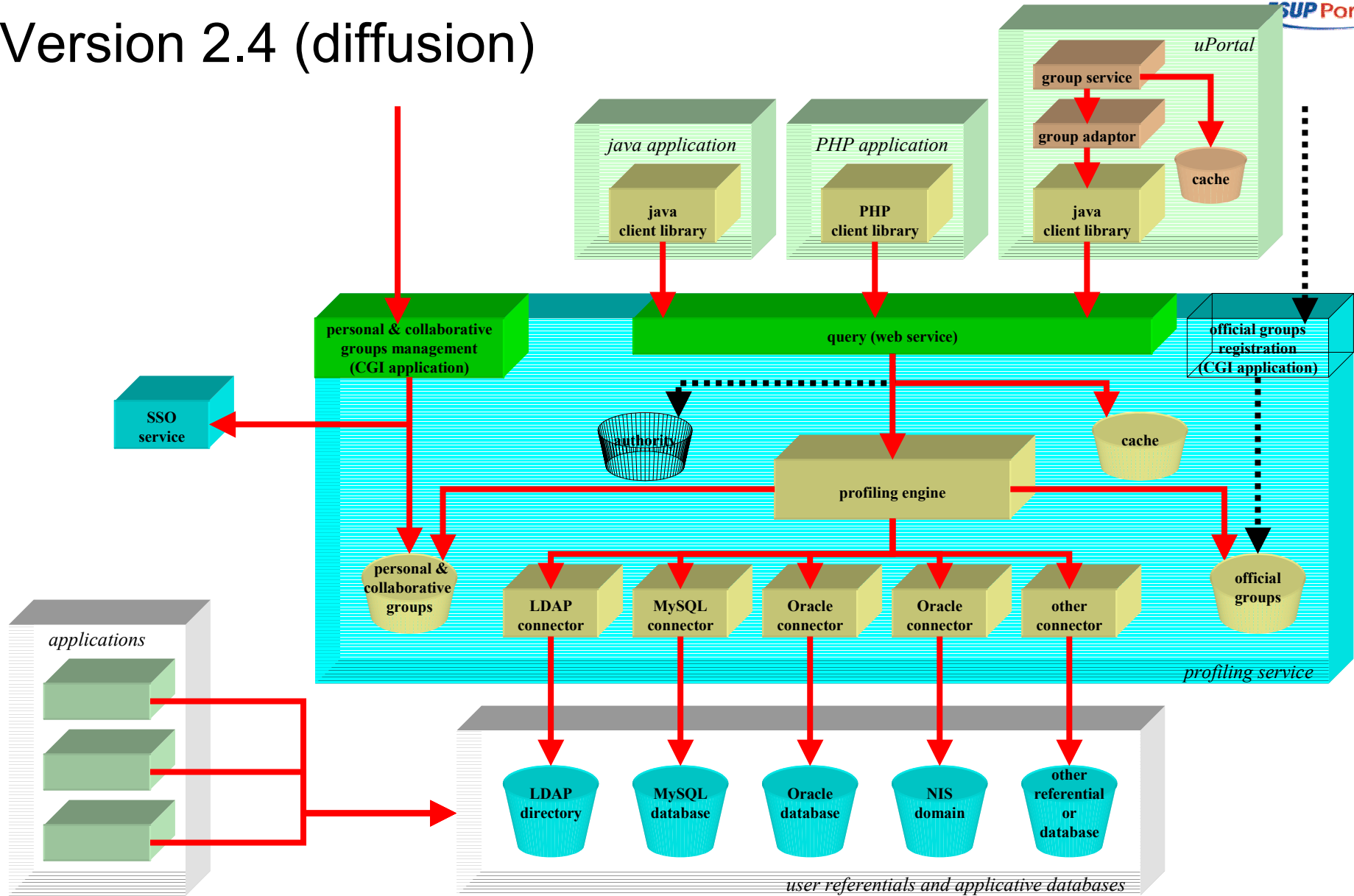


Version 2.4 (diffusion)

- **Nouvelles fonctionnalités**
 - Ajout des groupes personnels et collaboratifs
- **Travail à réaliser**
 - Spécifier le stockage des groupes personnels
 - Interfacier le moteur de profils avec les groupes personnels
 - Écrire une application CGI de gestion des groupes personnels



Version 2.4 (diffusion)

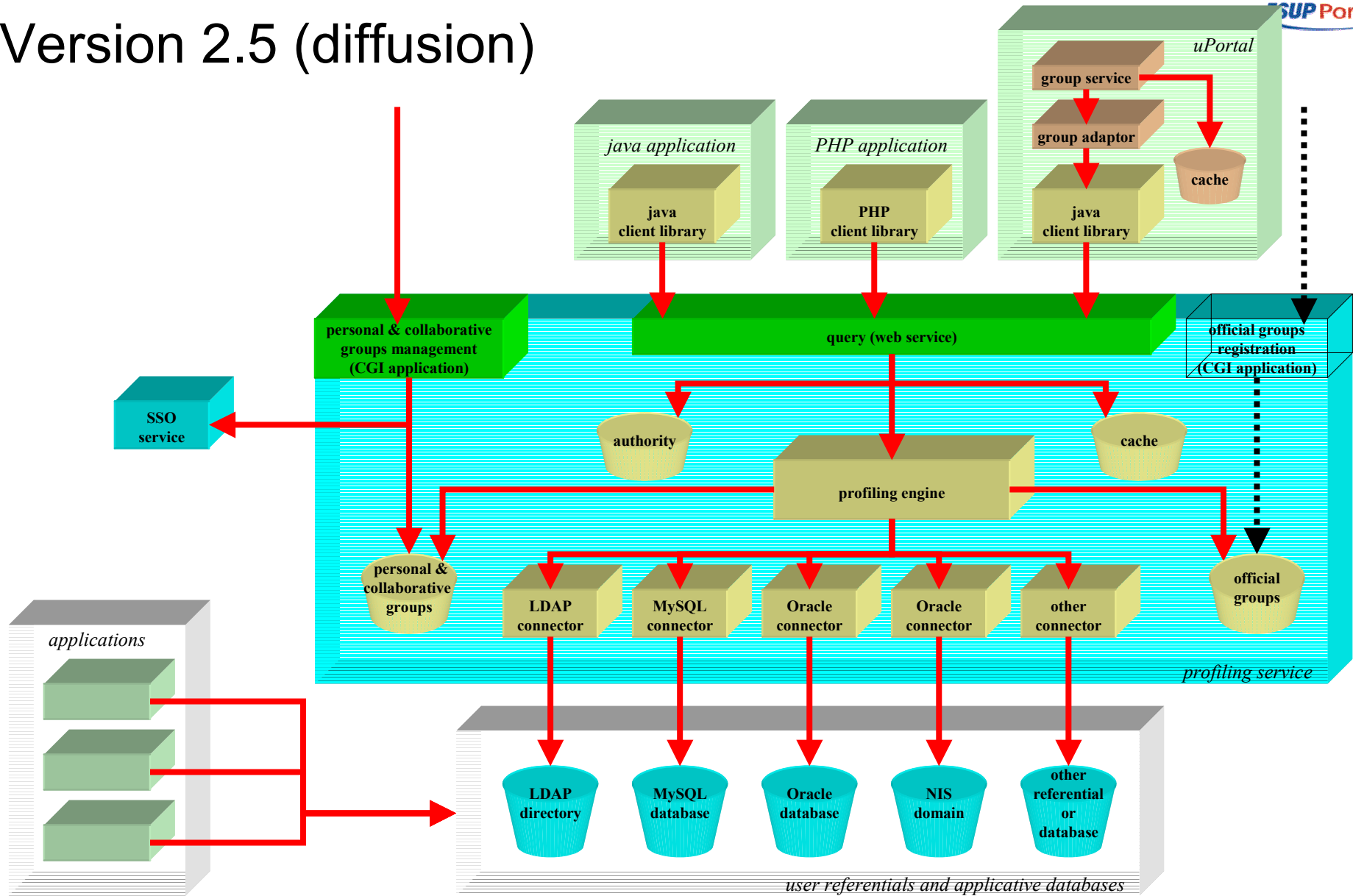


Version 2.5 (diffusion)

- **Nouvelles fonctionnalités**
 - Ajout de l'autorité de distribution.
- **Travail à réaliser**
 - Spécifier le stockage des règles de distribution
 - Interfacer le moteur de profils avec les règles de distribution



Version 2.5 (diffusion)

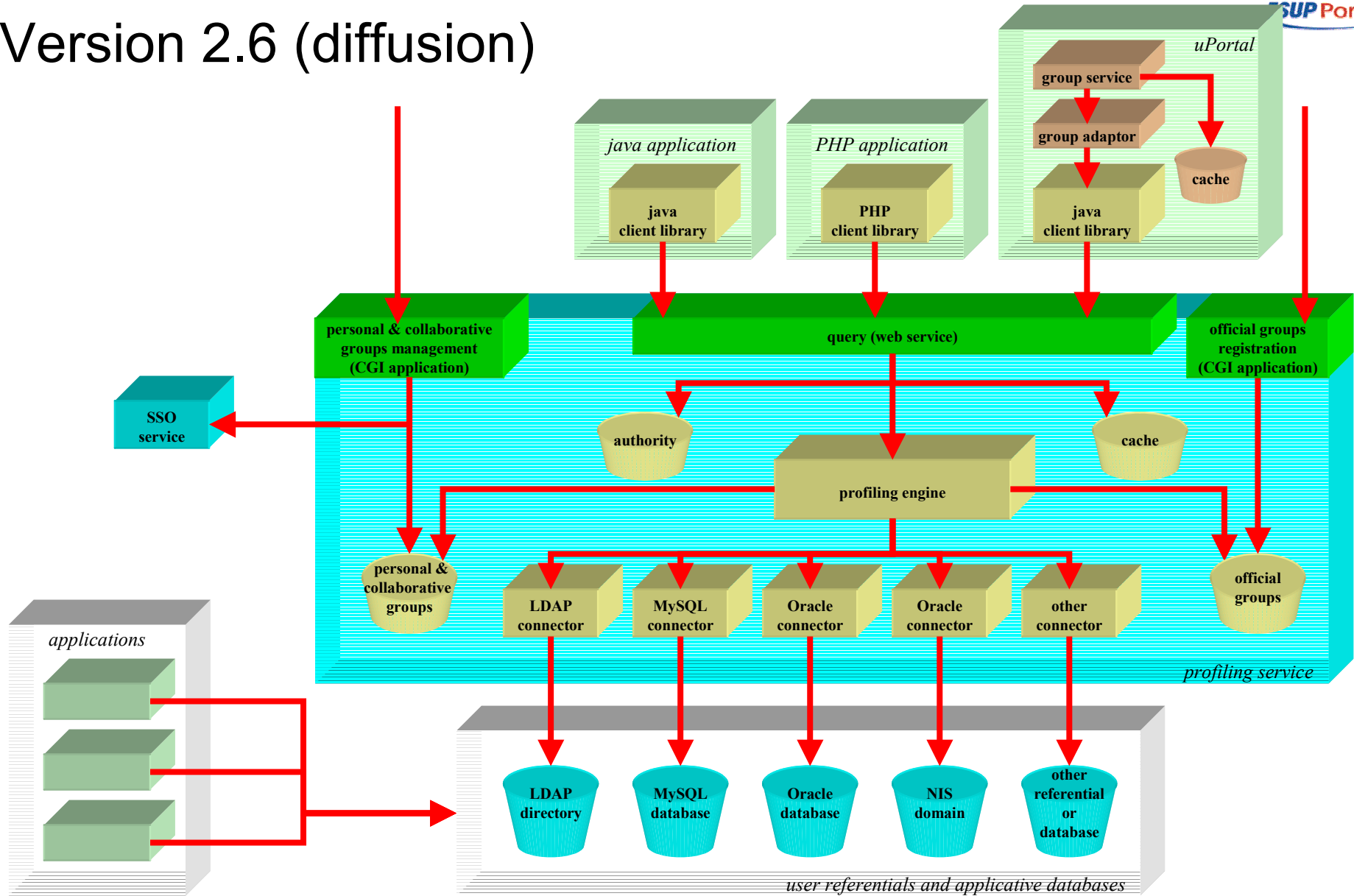


Version 2.6 (diffusion)

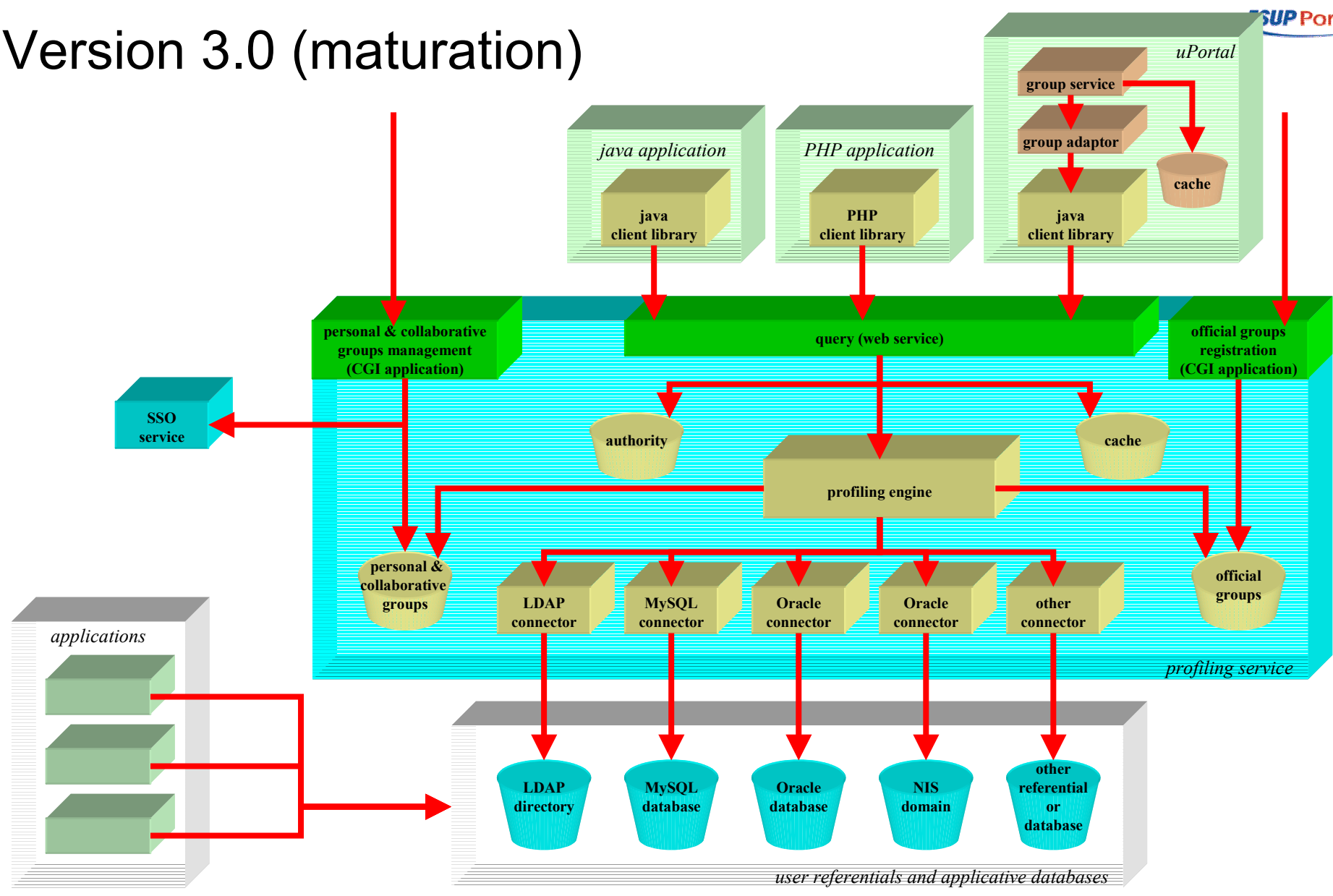
- **Nouvelles fonctionnalités**
 - Ajout de l'application CGI de gestion des groupes personnels
- **Travail à réaliser**
 - Développer l'application CGI



Version 2.6 (diffusion)



Version 3.0 (maturation)



Calendrier prévisionnel

- **À compléter**