Description fonctionnelle des applications

Application Esup Activ FO

Page d'accueil de l'application

L'utilisateur est accueilli sur une page l'invitant à choisir quelle procédure il souhaite réaliser.

La liste des procédures accessibles diffère selon le fait que l'utilisateur est authentifié ou non. Si l'utilisateur choisi la procédure d'activation ou de réinitialisation de son compte, il devra par ailleurs définir son statut au sein de l'établissement. Un bouton "Confirmer" lui permettra ensuite de débuter la procédure.

Déroulement de la procédure d'activation de son compte informatique

Etape 1 : Identification

Durant cette étape l'utilisateur saisira les informations permettant de l'identifier. Dans le cas d'un étudiant par exemple, l'utilisateur devra saisir son numéro d'étudiant ainsi que sa date de naissance (configuration par défaut). Une fois collectées ces informations seront transmises au Back-Office via l'API SOAP pour identification de la personne. Si celle-ci est authentifiée le Back-Office (BO) fournira au Front-Office (FO) les informations de l'utilisateur récupérées du LDAP ainsi qu'un code unique d'identification utilisable entre le FO et le BO pour la session de cet utilisateur. Le FO vérifiera que le compte de l'utilisateur n'est pas déjà activé (en vérifiant que l'attribut *shadowlastchange* n'est pas défini) et redirigera alors la personne à l'étape 2. Si le compte est déjà activé, un message d'erreur lui signifiera et l'invitera si nécessaire à utiliser la procédure de récupération de son mot de passe.

Etape 2 : Informations personnelles

Durant cette étape l'utilisateur a la possibilité de mettre à jour ses données personnelles. Celles-ci lui sont affichées dans un formulaire éditable pré-remplit à partir de données déjà présentes dans l'annuaire LDAP. A la validation du formulaire les informations seront validées (et éventuellement converties) en fonction du paramétrage et, si elles sont valides, seront transmises au BO pour modification. Le FO fournira également l'identifiant de l'utilisateur ainsi que le code unique d'identification de la session.

⚠ **Note importante :** l'identifiant fournit correspond à un attribut LDAP configurable dans le FO via le paramètre *account.key.id* (fichier *properties /config.properties*). Il doit correspondre à l'identifiant utilisé côté BO configurable dans son paramètre *ldap.attribute.login* (fichier *properties /config.properties*).

Etape 3 : Acceptation de la charte informatique

Durant cette étape, il est demandé à l'utilisateur d'accepter la charte informatique de l'établissement en cochant une case et en cliquant sur un bouton pour valider. Un lien vers le texte de la charte informatique est fourni pour permettre à l'utilisateur d'en prendre connaissance. Si celui-ci valide sans cocher la case un message d'erreur lui précisera que cette opération est obligatoire pour pouvoir continuer. Une fois la case cochée et le formulaire validé le FO permettra l'accès à l'étape suivante.

Note : Le fait d'accepter la charte n'est pas à proprement dit stocké dans l'annuaire actuellement. Cela fait cependant partie d'une évolution actuellement en cours de recette.

Etape 4 : Choix du mot de passe

Note : Cette description fonctionnelle décrit un cas d'usage d'un stockage du mot de passe dans l'annuaire LDAP.

Durant cette étape, l'utilisateur devra choisir son mot de passe. Ce mot de passe devra respecter la politique de sécurité de l'établissement. Une indication visuelle lui permettra d'observer le niveau de sécurité de son mot de passe. L'utilisateur devra saisir deux fois son mot de passe puis valider. Le FO validera alors que les deux saisis du mot de passe sont bien identiques et que ce dernier respecte bien la politique de sécurité. Si c'est le cas, le FO fera appel à la procédure de changement du mot de passe de l'API du BO toujours avec le code unique de session de l'utilisateur. Le BO hachera alors le mot de passe (*SSHA* par défaut) et le modifiera dans l'annuaire LDAP. L'attribut *shadowlastchange* sera également défini. Le FO affichera alors un message à l'utilisateur l'informant que son compte a été activé et qu'il peut dès à présent accéder aux ressources informatiques offertes par l'établissement. Par défaut un lien vers le portail ENT lui sera fourni.

Déroulement de la procédure de modification de son mot de passe

Etape 1 : Identification

Durant cette étape l'utilisateur doit saisir son login et son mot de passe actuel pour permettre son identification. Une fois le formulaire validé les informations seront transmises au Back-Office via l'API SOAP pour identification de la personne. Si celle-ci est authentifiée le Back-Office (BO) fournira au Front-Office (FO) les informations de l'utilisateur récupérées du LDAP ainsi qu'un code unique d'identification utilisable entre le FO et le BO pour la session de cet utilisateur. Le FO vérifiera que le compte de l'utilisateur est bien déjà activé (en vérifiant que l'attribut shadowlastchange est bien défini) et redirigera alors la personne à l'étape 2. Si le compte n'est pas encore activé un message d'erreur expliquera à l'utilisateur qu'il doit activer son compte et l'invitera à utiliser la procédure d'activation.

Etape 2 : Informations personnelles

Durant cette étape l'utilisateur à la possibilité de mettre à jour ses données personnelles. Cette étape est identique à celle de la procédure d'activation du compte.

Etape 3 : Choix du mot de passe

Durant cette étape l'utilisateur devra choisir son nouveau mot de passe. Cette étape est également identique à celle de la procédure d'activation du compte mis à part le fait que les différents messages sont adaptés à la situation.

Déroulement de la procédure de réinitialisation de son mot de passe

Etape 1 : Identification

Durant cette étape l'utilisateur saisira les informations permettant de l'identifier (mêmes informations qu'en cas d'activation d'un compte). Les informations seront transmises au Back-Office via l'API SOAP pour identification de la personne. Si celle-ci est authentifiée le Back-Office (BO) fournira au Front-Office (FO) les informations de l'utilisateur récupérées du LDAP ainsi qu'un code unique d'identification utilisable entre le FO et le BO pour la session de cet utilisateur. Le FO vérifiera que le compte de l'utilisateur est bien déjà activé (en vérifiant que l'attribut *shadowlastchange* est bien défini) et redirigera alors la personne à l'étape 2. Si le compte n'est pas encore activé un message d'erreur expliquera à l'utilisateur qu'il doit activer son compte et l'invitera à utiliser la procédure d'activation.

Etape 2 : Choix du mode d'obtention du code de réinitialisation

Durant cette étape l'utilisateur devra choisir par quel circuit il souhaite obtenir le code de réinitialisation de son mot de passe. Il aura le choix entre :

- **un envoi du code par email** sur son adresse mail alternative. Ce choix lui sera proposé uniquement si son mail alternatif est renseigné dans l'annuaire LDAP
- **un envoi du code par SMS** sur son numéro de mobile. Ce choix lui sera proposé uniquement si son numéro de mobile est renseigné dans l'annuaire LDAP. L'établissement devra par ailleurs avoir une solution d'envoi de SMS (plateforme esup-sms-u, back-office à minima)
- **récupérer le code via le service d'assistance** de l'établissement. S'il choisit ce mode d'obtention le code sera envoyé par mail au service d'assistance, l'utilisateur devra contacter ce service afin que son code lui soit communiqué.

Un choix ***"J'ai un code"*** lui est également proposé. Cette option permet de traiter tous les autres cas possibles où l'utilisateur dispose déjà d'un code.

Pour l'envoi du code, le Front-Office fera appel à la méthode du Back-Office d'un code via son API SOAP en lui spécifiant le mode d'obtention choisi par l'utilisateur. Le Back-Office générera alors un code de validation et l'enverra à l'utilisateur. Ce code à une durée de validité limitée et est stocké par le Back-Office dans le fichier *userData.txt*. Cette durée pourra être différente pour chacune des méthodes d'obtentions possibles.

L'utilisateur accédera ensuite à l'étape 3.

Etape 3 : Saisi du code de réinitialisation

Durant cette étape l'utilisateur doit saisir le code de réinitialisation. Si un code lui a été envoyé durant l'étape précédente, un message le lui précisera.

Une fois le code saisi l'utilisateur doit cliquer sur un bouton pour soumettre son code.

Une vérification syntaxique du code sera faite et si celui-ci est invalide un message d'erreur sera affiché à l'utilisateur.

Si le code est syntaxiquement valide le Front-Office le soumettra pour validation au Back-Office via son API SOAP. Si le code est valide l'utilisateur accédera à l'étape 4, sinon un message d'erreur s'affichera. Après X tentatives erronées (3 par défaut), l'utilisateur sera bloqué et devra attendre X secondes (30 par défaut) avant de pouvoir soumettre à nouveau un code.

FIXME : Il serait bien de commenter ici le fonctionnement et l'utilité de la boucle de déblocage.

Etape 4 : Informations personnelles

Durant cette étape l'utilisateur à la possibilité de mettre à jour ses données personnelles. Cette étape est identique à celle de la procédure d'activation du compte.

Etape 5 : Choix du mot de passe

Durant cette étape l'utilisateur devra choisir son nouveau mot de passe. Cette étape est également identique à celle de la procédure d'activation du compte mis à part le fait que les différents messages sont adaptés à la situation.