LanceENT
v 1.1

Introduction :

Cette application a été faite pour permettre le lancement automatique du navigateur Internet explorer, la connexion à une page précisée par l'administrateur et la saisie automatique dans les champs prévus a cet effet des identifiants et des mots de passe.

Elle est partagée en deux morceaux :

- une partie installée à un endroit commun à tous les utilisateurs (qui contiendra l'application en elle même).
- une partie générée lors de l'utilisation dans le répertoire de l'utilisateur contenant ses identifiants et mots de passe (cryptés bien sûr).

L'utilisation :

- Lors de la première utilisation, l'utilisateur renseignera son identifiant et son mot de passe permettant de générer un fichier dans son répertoire personnel (lance.vbe).
- Ensuite il n'aura qu'a demander la connexion pour que celle ci s'effectue de manière automatique.
- En cas de changement de mot de passe ou d'erreur de saisie de ses identifiants, l'application prévoie la possibilité de saisir à nouveau son identifiant et son mot de passe.

Paramétrages :

La connexion s’effectuera dans ce cadre à l'URL choisie par l'administrateur et le fichier comportant ses informations d'authentification seront stockées a un endroit également choisi par l'administrateur du réseau.

Ces paramètres de configuration changeront donc pour permettre d'adapter l’application a la structure du réseau sur lequel on l'installe. Vous trouverez ci dessous les procédures d'installation pour chaque cas (réseau pédagogique, réseau administratif, poste utilisateur).

INSTALLATION ET PARAMETRAGES :

Installation sur le réseau Pédagogique :

- Dézipez l'archive zip et copiez les fichiers contenus dans l'archive dans un répertoire du winappli, **le nom de ce répertoire ne doit pas contenir d'espaces.** Exemple : LanceurENT.

- Editez le fichier config.txt et modifiez le en fonction de vos besoins :

  URL
  La donnée **url** détermine la page web sur laquelle se déroulera l'authentification, en l'occurrence pour le collège Gambetta ce sera :
  url = "https://cas.entmip.fr/login?service=http%3A%2F%2Fgambetta.entmip.fr%2Fsg.do%3FPROC%3DIDENTIFICATION_FRONT"

  Pour récupérer cette adresse sans risque de mauvaise saisie, allez sur votre ENT, cliquez sur le lien « Se connecter » en haut à gauche de la page. L'adresse qui s'affiche dans votre barre d'adresse une fois que la page d'authentification est chargée est l'url qui nous concerne. Vous pouvez la sélectionner, la copier et la coller dans votre fichier config.txt entre les guillemets du paramètre url= " ".

  formID et formPswd
  Quand on regarde le code source de la page on peut voir sur la page d'authentification de l'ENT, le champ où l'on renseigne son identifiant porte le nom de username, on le mentionne grâce à la ligne suivante :
  formID = "username"
  de la même manière, le mot de passe est déposé dans le champ de formulaire qui porte le nom password :
  formPswd = "password"

  FICHIERVBS
  Cette dernière information détermine où l'on ira écrire le fichier qui contiendra les informations de connexion de chaque utilisateur :
  fichierVBS = "\\serveur01\%username%\lance.vbs"

Ce qui nous donne pour un serveur01 classique le fichier de configuration suivant pour l'ent de gambetta:

```
url = "https://cas.entmip.fr/login?service=http%3A%2F%2Fgambetta.entmip.fr%2Fsg.do%3FPROC%3DIDENTIFICATION_FRONT"
formID = "username"
formPswd = "password"
fichierVBS = "\\serveur01\%username%\lance.vbs"
```

• Il ne vous reste plus qu'à faire un raccourci sur le fichier « lanceur.jar » que vous pourrez placer dans le modèle des enseignants comme des élèves. Pour améliorer l'apparence, vous pouvez "Agrémenter le lanceur " comme décrit un peu plus bas.

Installation sur le réseau Administratif :

• décompactez l'archive zip et copiez les fichiers contenus dans l'archive dans un des répertoires du lecteur « L » dit « libre » (c'est le répertoire accessible de tous les utilisateurs) à nouveau, il faut éviter les noms comportant des espaces dans les noms des répertoires.

• le fichier de configuration sera sensiblement le même que pour le réseau pédagogique, a une exception près, la localisation du fichierVBS. On pourra le mettre dans le répertoire personnel de l'utilisateur comme par exemple « U » ou répertoire personnel. Soit :
fichierVBS = "U:\lance.vbs".

• Il ne reste plus qu'a faire un raccourci du fichier « Lanceur.jar » et le placer sur le bureau de chaque utilisateur du réseau administratif.

Installation sur un poste personnel:

• décompactez l'archive zip et copiez les fichiers contenus dans l'archive dans un des répertoires du lecteur « C » , par exmeple dans « C:\authentification\ » à nouveau, il faut éviter les noms comportant des espaces dans les noms des répertoires.

• le fichier de configuration sera sensiblement le même que pour le réseau pédagogique, à une exception près, la localisation du fichierVBS. On pourra le mettre dans le même répertoire que l'application (ou ailleurs au choix, mais toujours sans espaces pour les noms des répertoires). Soit :
fichierVBS = "C:\authentification\lance.vbs".

• Il ne reste plus qu'a faire un raccourci du fichier « Lanceur.jar » et le placer sur le bureau.

Agrémenter le lanceur :

• Est livré avec le lanceur un icône qui permet de représenter l'ENT et qui peux donner une meilleure apparence du raccourci sur le bureau de chaque utilisateur.

• Vous pouvez personnaliser les fenêtres de dialogue en enregistrant le bandeau de votre ent dans les fichiers de l'application sous le nom de « bandeau.png » et ce même si c'est du jpg. Les fenêtres de dialogues représenteront alors les questions sous le bandeau que vous aurez fourni.

Annexes

Bugs rencontrés et solutions trouvées :

Lors du lancement de l'application, c'est un logiciel comme winzip ou 7zip qui se lance, ce n'est pas le système de connexion automatique. (Merci aux personnes qui ont remonté ce problème : Muriel Dupont de Prayssac et Floreal Vaz de Cahors).

Le lanceur est un programme java sous forme d'archive **J**ava **Ar**chive (JAR) qui est une archive zip spécialisée. Certains logiciels de compression de fichier s'associent à ce suffixe « jar ». C'est assez rare mais cela empêche toute exécution du programme de connexion automatique. La solution est de modifier le raccourci pour préciser que l'on souhaite le lancer grâce à java et non pas via un autre programme. Pour se faire :

- Cliquez avec un clic droit sur le raccourci.
- Dans le menu contextuel sélectionnez « Propriétés ».
- Dans l'onglet raccourci, vous trouverez le chemin d'accès complet d'accès au lanceur.jar, par exemple sur mon ordinateur : C:\authentification\ent\Lanceur.jar
- Modifiez ce champ du raccourci (qui se nomme Cible sous W7) et faites précéder les informations déjà mentionnées de l'appel à java comme interpréteur : java -jar . Ce qui devrait vous donner au final « java -jar C:\authentification\ent\Lanceur.jar », (sans les guillemets et avec le chemin complet du lanceur.jar correspondant à votre configuration, pas nécessairement identique à C:\authentification\ent\).
- Dans la liste déroulante également présente, en face d'exécuter, choisissez « Réduite » à la place de « Fenêtre normale ».
- Cliquez sur OK.

Normalement, le raccourci présent sur votre bureau devrait devenir fonctionnel et vous permettre de vous connecter à l'ENT.

Le programme se lance, me propose de renseigner mon identifiant et mon mot de passe et m'envoie un message d'erreur quand je clique sur « enregistrer » précisant qu' « Pas d'extension pour le fichier... » (Merci à David Auffray de Saint Céré d'avoir remonté ce problème).

Cette erreur est déclenchée quand il y a au moins un espace dans les chemins d'accès utilisés. Vérifiez que vous avez déposé les fichiers de l'application dans une localisation ou aucun des noms de repertoire ne contient d'espaces et dans le fichier config.txt qu'il en va de même pour la valeur du paramètre fichierVBS.

Pourquoi utiliser cette technique de connexion ?

L'authentification à l'ENT et les programmes existants :

Depuis l'arrivée de l'ENT dans les établissements, il est devenu important pour en favoriser les usages de permettre aux utilisateurs une authentification la plus pratique et rapide possible.
Plusieurs outils ont été développés dans ce sens :
– Lanceur ENT fourni par M. BIANSAN
– Un lanceur intégré à Magret (merci au passage aux « papas de Magret », Thierry Chassain et Guy Picou).
Chacun de ces outils sont basés sur une technique qui s'appelle les « sendkeys ». Le programme qui gère l'authentification en effectuant les étapes qu'un utilisateur accomplirait pour s'authentifier en saisissant l'identifiant et le mot de passe comme si il le tapait au clavier. Le problème c'est que ce programme le fait « en aveugle » sans être certain qu'il tape les identifiants et mots de passe dans la bonne application et dans le bon champ (on a déjà vu des mots de passe saisis dans le champ nom et qui apparaissaient en clair sur l'écran, ce qui peut être gênant si l'écran est affiché via un vidéo projecteur). Ce sont ces inconvénients qui amènent la plupart des professionnels de la conception d'applications à ne pas utiliser la méthode des « sendkeys » en production. Néanmoins, cette méthode possède un avantage. Le programme ne sachant pas dans quels champs il tape l'identifiant et le mot de passe de l'utilisateur, n'a pas a être configuré sur ce point. Cela en fait une méthode très polyvalente. Chaque application d'authentification automatique déjà réalisée a donc été adaptée par ces concepteurs pour limiter au maximum ces problèmes (comme pour le Lanceur ENT de M. BIANSAN qui effectue sa saisie qu'une fois que l'utilisateur confirme que le navigateur internet est bien ouvert sur la bonne page).

Alternative à la méthode des « Sendkeys »:

L'alternative que j'utilise dans LanceENT est de déposer directement les informations d'authentification dans les champs identifiants et mots de passe tels que définis dans la page internet du site. Cela est beaucoup plus contraignant (il faut connaître les noms des champs du formulaire d'authentification) et ceux ci changeant d'un site a un autre, cela diminue la polyvalence et doit donc être configuré dans l'application. Deuxième inconvénient, c'est que c'est le navigateur internet lui même qui rempli les champs sur la page d'authentification, on se retrouve donc contraints a n'utiliser pour cette authentification qu'un seul navigateur, en l'occurrence Internet Explorer. En échange de ces contraintes, on obtient une authentification automatique beaucoup plus sure et plus rapide, bref qui favorise davantage les usages.

La connexion à l'ENT se fait pour tous les utilisateurs à la même adresse (URL) et ils ont a remplir leurs identifiants et leurs mots de passe dans les mêmes champs. Ces informations sont donc valables pour tous et il est préférable que l'administrateur du réseau concerné en garde le contrôle (fichier config.txt).
A l'opposé, les informations de connexion de chaque utilisateur (l'identifiant et le mot de passe) sont propre à l'utilisateur et doivent donc être stocké dans les informations de l'utilisateur, sous forme cryptée pour en garder la confidentialité.
Nous retrouveront donc deux fichiers qui permettent le fonctionnement de l'authentification, un fichier de configuration propre à l'administrateur et un fichier qui contiendra les identifiants et mots de passe de l'utilisateur qui sera placé dans un espace propre à l'utilisateur.