Manuel pGina

http://pgina.xpasystems.com

http://www.xpasystems.com

Introduction

pGina est, en résumé, une méthode alternative à l'authentification par domaine dans une environnement Windows. pGina, au travers de l'utilisation de technique de plug-in, permets à l'administrateur de choisir la méthode et source d'authentification qu'il préfère. Et si la méthode n'existe pas encore ou qu'il veut en étendre les possibilités, il a la possibilité d'écrire son propre plug-in en s'inspirant de l'exemple ou du plugin qui s'en rapproche le plus car pGina est fourni avec toutes les sources des programmes ainsi que toute la documentation sur les API.

pGina fonctionne en s'insérant dans le procéssus d'identification comme un GINA (Graphical Identification and Authentication). Sans pGina, quand un système Windows démarre, un procéssus appelé Winlogon charge le GINA Microsoft qui est chargé de gérer les évenements systèmes comme le CTRL+ALT+DEL, l'activation d'un économiseur d'écran, d'une tentative de logon, etc. Quand pGina est installé, il s'insère lui-même entre le processus Winlogon et le GINA Microsoft's, gère donc directement tous ces évenements (logon, vérouillage, etc) et passe tout le reste de manière transparente au module Microsoft.

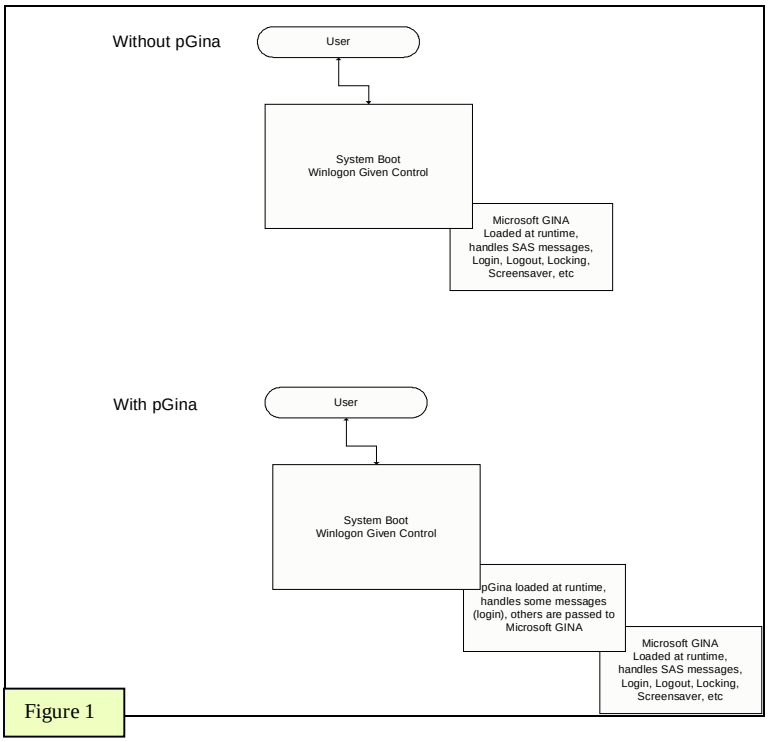


Figure 1

Quand Winlogon charge pGina, pGina charge a son tour un plug-in choisi par l'administrateur. Quand un utilisateur essaie de se logger, pGina utilise le plug-in sélectionné afin de déterminer s'il doit-être authentifié ou pas. Si le plug-in autorise l'utilisateur a poursuivre, pGina créera un compte utilisateur sur la machine locale, l'ajoutera dans les groupes spécifiés par le plug-in, mappera les disques réseau spécifiés aussi bien globalement que pour l'utilisateur et pourra faire encore bien d'autres choses selon la configuration et la personnalisation du plug-in.

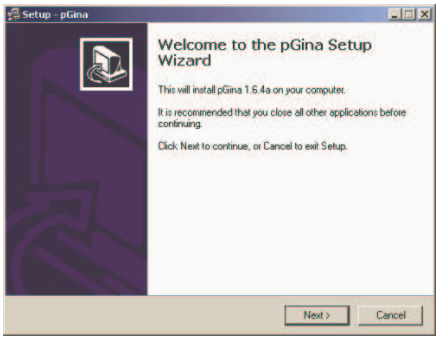
Pour aider à comprendre comment pGina peut aider quelqu'un, regardons l'exemple générique d'un administrateur nommé 'Pierre'. Pierre est responsable d'un parc de machines Windows 2000 et de quelques machines Linux. Actuellement Pierre est obligé de maintenir en double les comptes utilisateurs et mot de passe a la fois sur le système Windows que sur les machines Unix. En plus de cela le serveur Unix est également le serveur de fichiers, donc tout ce que fait le serveur Windows est d'authentifier les utilisateurs. Actuellement ses clients Linux utilisent le protocole LDAP. Pierre peut juste utiliser pGina pour authentifier tous ses utilisateurs depuis le même serveur Unix en installant simplement pGina et le plugin LDAP pour pGina. Maintenant Pierre a simplement a administrer une ressource unique contenant les noms et mots de passe, il n'a plus besoin de son serveur Windows. Cela lui libère une grande partie de

son temps qu'il pourra consacrer à d'autres tâches, et réduit le coût de fonctionnement en supprimant les licences Windows (clients et serveur).

Installation

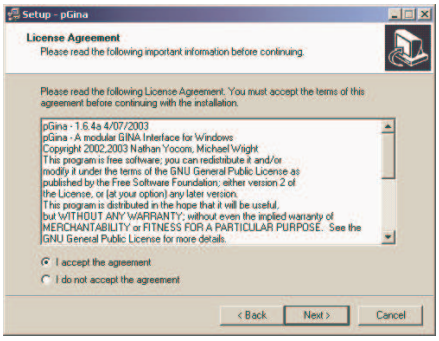
L'installation de pGina est très simple et ressemble à l'installation de beaucoup d'autres logiciels Windows. ***Merci de noter que si l'installation de pGina devait, pour une quelconque raison, crasher, votre système peut devenir inutilisable. Pour cette raison, il est important de savoir re-démarrer en mode sans échec et d'avoir une disquette de réparation ou d'être familier avec les techniques de modification du registre a distance..***

Première étape: Vous devrez télécharger le dernier programme d'installation depuis le site web situé à http://pgina.xpasystems.com. Après avoir téléchargé, soyez sûr d'avoir les privilèges administrateur local, que votre machine de fait PAS partie d'un domaine Windows (sans que vous utilisiez un pluggin qui le permette) et démarrez l'installation. Confirmez que vous voulez installer pGina et vous devez obtenir l'écran présenté en Figure 2.



Là, vous devez sélectionner l'endroit où vous voulez que pGina s'installe. Vous pouvez utiliser les valeurs par défaut qui sont recommandées (et qui seront utilisées tout au long de ce manuel).

Après avoir sélectionné l'emplacement souhaité, cliquez sur le bouton Next pour continuer à la Figure 3.



Cette boite de dialogue vous affiche une copie de la license Publique 'Gnu'. Merci de la lire attentivement afin de comprendre et accepter son contenu puis choisissez l'option "I accept the agreement",et cliquez sur "Next" pour continuer à la Figure 4.

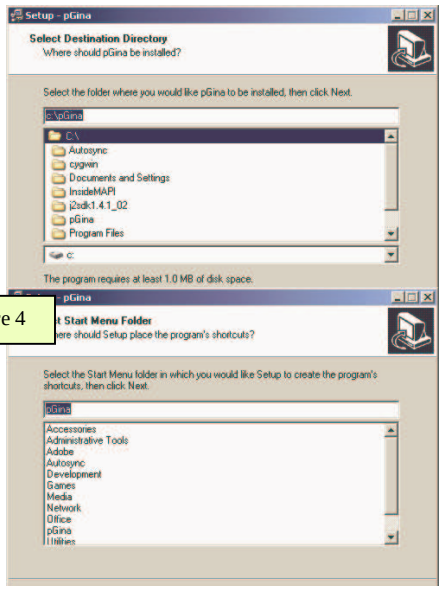


Figure 4

Vous allez, maintenant pouvoir choir dans quel répertoire vous souhaitez installer pGina. Selectionnez un répertoire dans le disque choisi et cliquez sur "Next" pour continuer à la Figure 5.

Vous pouvez maintenant sélectionner où pGina sera créé dans le menu démarrage des utilisateurs. Après avoir choisi, cliquez sur “Next” afin de continuer à la Figure 6.

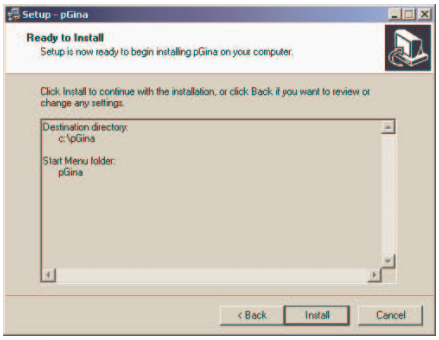


Figure 6

Cet écran vous permet de confirmer les choix que vous avez fait précédemment. Utilisez le bouton Back pour revenir sur vous choix et les modifier si besoin. Après avoir sélectionné “Install”, tous les fichiers seront installés sur votre système à l’endroit indiqué.

L’installation par défaut doit fonctionner sans avoir besoin d’être configurée, cependant il n’est pas recommandé de rebooter sans avoir vérifié cette étape. La Figure 7 montre la boite de dialogue finale de la procédure d’installation.

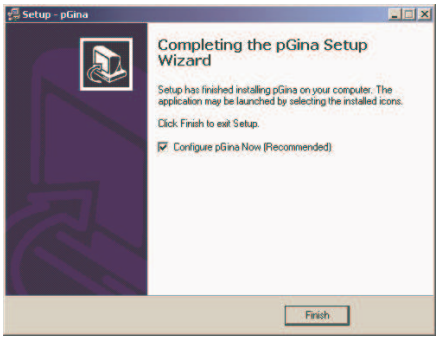


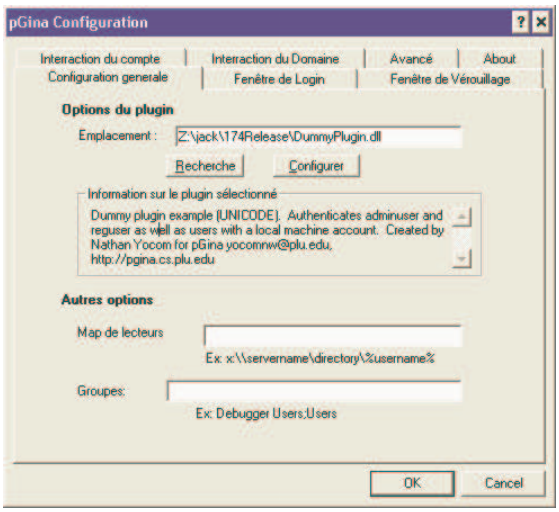
Figure 7

Pour sauter l’étape de configuration, décochez la boite “Configure pGina Now” et sélectionnez “Finish”. Autrement sélectionnez “Finish” pour quitter le programme d’installation et démarrer le programme de configuration.

Configurer pGina

Pour configurer pGina, a nouveau soyez sûr d'être loggé comme administrateur ou avec les privilèges administrateur, puis démarrez le programme de configuration en cliquant sur 'Démarrer->Programmes->pGina->Configure pGina" . Après un bref écran de présentation, l'écran de configuration apparaît. C'est à travers cet écran que vous pouvez changer les paramètres de fonctionnement de pGina et de ses dépendances. Regardons les options individuelles et leurs effets sur pGina.

CONFIGURATION GENERALE



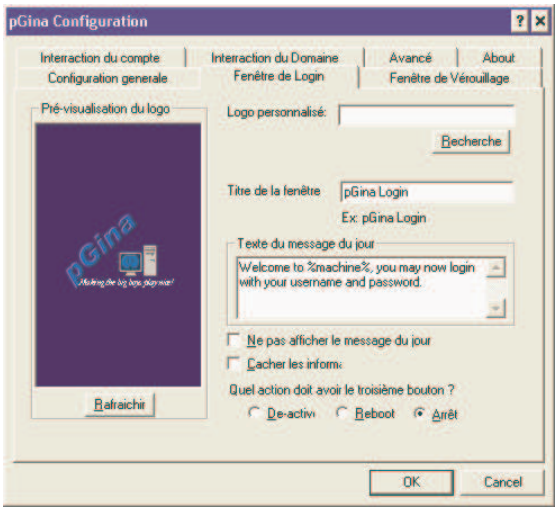
Les options les plus communement utilisées sont sur l'onglet 'General'. Cela inclus le plugin que pGina devra utiliser pour l'authentification et le mapping de lecteurs disques qui doivent être faits pour chaque utilisateur.

Options de PlugIn
Pour sélectionner ou changer de plugin, cliquez sur Browse afin de trouver le plugin recherché. Des informations sur le plugin choisi apparaîtront alors dans la zone "Selected Plugin Information" box. Si un plugin permet une configuration, un click sur le bouton Configure vous conduira à la boite de dialogue de configuration du plugin.

Autres Options
Egalement disponible sur l'onglet General, l'option de mapping de disques réseau : Si sélectionnée, tous les disques listés seront mappés pour tout les utilisateurs qui auront été loggés. Les disques sont spécifiés par DRIVE:UNC-PATH. Par exemple, pour mapper le disque J sur \\serveur\partage il faut saisir J:\\serveur\partage. De multiples disques réseau peuvent être spécifiés sur la même ligne par l'ajout du caractère ';' entre chaque entrée.

De la même manière, vous pouvez spécifier une liste de groupes auquels l'utilisateur doit faire partie. Cette liste doit avoir la même présentation ; c'est à dire une liste de valeurs séparées par le caractère ';'. Par exemple si vous voulez qu'un utilisateur fasse partie à la fois du groupe 'Utilisateurs' et du groupe 'Utilisateurs avec pouvoir', vous devez entrer la ligne suivante :"Utilisateurs;Utilisateurs avec pouvoir" , sans les parenthèses.

PERSONNALISATION DE LA FENÊTRE DE LOGIN



En cliquant sur l'onglet Logon Window, vous avez accés a toutes les options qui affectent l'aspect de la fenêtre de login.

Vous pouvez utiliser le bouton Browse pour trouver l'image bitmap qui sera utilisée comme logo. Dès sa sélection, si l'image est valide, elle sera affichée dans la zone de prévisualisation sur la gauche de la fenêtre. Son apparence sera la même lors de l'affichage dans la fenêtre de login. Comme référence, l'image par défaut a une dimension de 100x146 pixels, une résolution de 300x300 en 24bits (65536 couleurs). Seules les images bitmap sont utilisables.

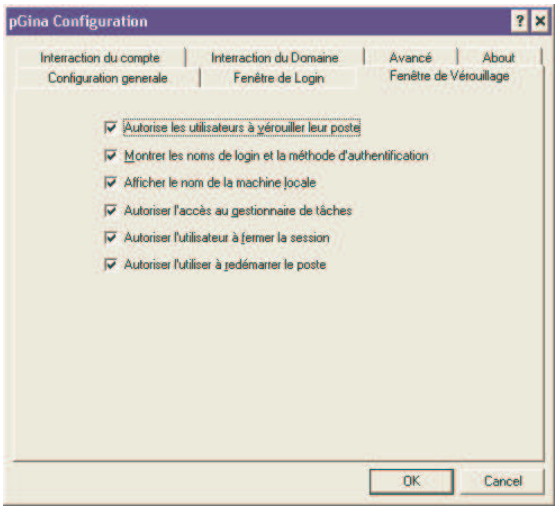
Le titre de la fenêtre est personnalisable.

Le “Message of the day” est affiché avant la zone utilisateur et mot de passe quand la fenêtre de login est affichée. Pour plus de facilité, le texte %machine% est remplacé au démarrage par le nom de la machine (sans son suffixe DNS). Si vous choisissez de cacher ce message, vous ne serez pas capable de modifier le texte du message (puisqu’il ne sera pas affiché de toutes façons).

Les informations de plugin (comme ce qui est présent dans l’onglet General) sont affichées après les zones utilisateur et mot de passe. Si vous ne voulez cependant pas que cette information s’affiche, cliquez simplement sur la boite “Hide Plugin Info”.

Le troisième bouton disponible lors du démarrage est paramètrable. Il peut être dé-activé ou alors permettre un re-démarrage ou un arrêt du système.

PERSONNALISATION DU VÉROUILLAGE



La fenêtre affichée lors de l’appui sur la séquence de touches CTRL+ALT+DEL pendant une session est également paramètrable.

L’option “Allow users to lock their desktop” permet ou non d’interdire à l’utilisateur de vérouiller son poste de travail.

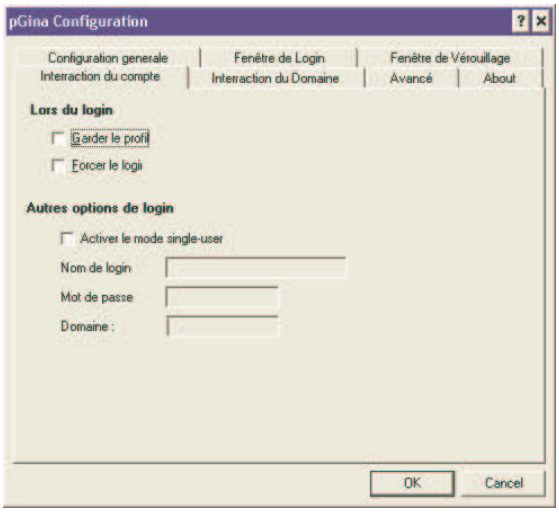
Si la seconde option est cochée la méthode d’authentification sera affichée (Plugin, Local, Domain).

Si la troisième option est cochée, le nom de la mchine sera affiché.

Si la quatrième option n’est pas cochée, le bouton du gestionnaire de tâches sera dé-activé (Cela ne dé-active pas les autres raccourcis comme CTRL+SHIFT+ESC).

Les deux dernières options controlent la possibilité de re-démarrer ou arréter le poste de travail.

INTERACTION DE COMPTE



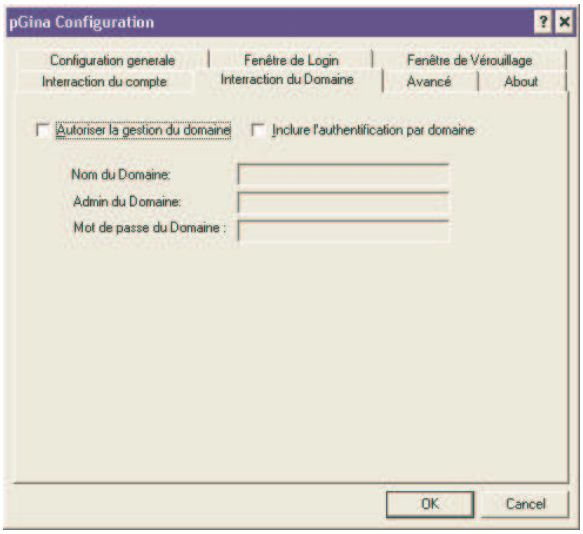
Dans des circonstances normales, pGina gère les logins avec les informations transmisent par le plugin qui a authentifié l’utilisateur. Cela se traduit, si besoin, par la création de comptes locaux qui correspondent aux informations fournies par celui-ci. Un profil sera donc créé (en accord avec les eventuelles restrictions de machine). La gestion ce ce processus est possible par l’onglet ‘Account Interaction’.

Quand l’option ‘Keep Profiles’ est cochée, le profil stocké sur le disque n’est pas détruit lors du logout de l’utilisateur. Cela signifie que le profil est gardé entre deux logins.

Quand l'option 'Keep Profiles' est active, il est possible que le mot de passe d'un utilisateur aie changé ailleur (sur l'annuaire LDAP par exemple) et que dans ce cas le mot de passe du compte local n'ayant pas changé, les mots de passes ne soient plus cohérents. L'option 'Force Login' permets d'éliminer ce dysfonctionnement en resynchronisant le mot de passe local a chaque login avec celui qui a été utilisé par le plugin.

L'option 'Single User Logon' est également disponible. Quand elle est activée, les noms d'utilisateur et mot de passe (et domaine Windows si fourni, autrement un login sur la machine locale est supposé) sont utilisés pour se logger sur la machine au lieu du nom et mot de passe fournis par le plugin. Cela permet l'utilisation d'un compte unique que si l'on a été authentifié par un autre compte. Quand cette option est utilisée, les options 'Keep Profiles' et 'Force Login' n'ont pas d'effets.

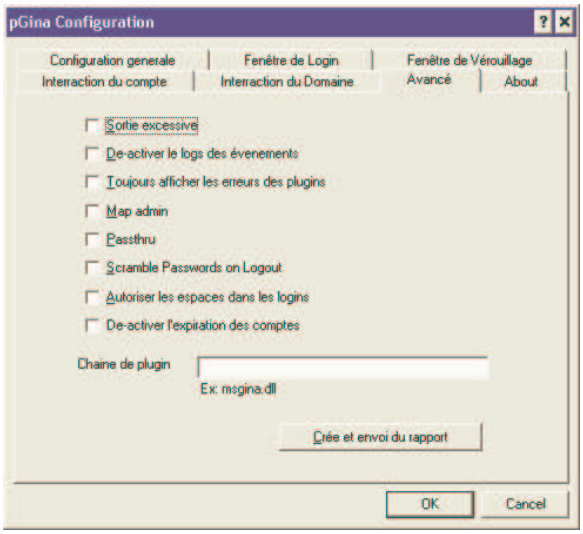
INTERACTION AVEC LES DOMAINES WINDOWS



pGina a aussi quelques option qui pemettent d'interagir avec les domaines Windows. Même si cela n'est pas l'objectif initial de pGina, celà est devenu un outil pratique et nécéssaire dans certaines circonstances. Quand l'option "Include Domain Authentication" est validée, le domaine fourni sera aussi utilisé dans la chaine d'authentification. Quand cela est le cas, pGina essaiera d'abord d'authentifier l(utilisateur via le plugin choisi puis, avec le domaine fourni, avec la machine locale.

Quand l'option 'Enable Domain Management' est cochée, pGina redirigera ses requêtes vers le domaine fourni. Cela siginfie que les comptes seront créés, effacés ou gérés comme pGina le ferais en local. Pour la version 1.7.4 cela requiert soit un serveur NT4 ou un serveur Active Directory fonctionnant en mode mixte (le support pure AD est prévu pour les prochaines versions). Un compte et mot de passe administrateur est nécéssaire afin que pGina puisse faire les changements nécéssaires.

OPTIONS AVANCÉES



La dernière option disponible est celle de l'onglet 'Advanced '.

La première option de cette fenêtre permet le log de nombreuses informations qui sont consultables par le gestionnaire d'évenements.

Si cette option est de-activée, le log se fera uniquement pour des informations normales.

Si l'option 'Always Display Plugin Errors' est active, cela resultera dans le log de toutes les erreur rencontrées par le plugin même si l'authetification a réussi avec un compte local ou de domaine. L'option de-activée, un log ne sera fait que si l'authentification a totalement échoué.

Par défaut, pGina ne mappe que les disques réseau décrits dans l'onglet 'General Configuration' pour les utilisateurs qui ont été authentifiés par le plugin choisi. L'option 'Map Admins' permets également aux comptes administrateurs locaux d'avoir ces disques réseau mappés.

L'option 'passthru' quand à elle permet de de-activer pGina en lui-même et donc de passer tout contrôle au GINA Microsoft d'origine sans avoir a de-installer pGina.

At times, la gestion des profils souhaitée est d'utiliser l'option 'Kepp Profile' dans l'onglet 'Account Interaction'. Cependant, le profil stocké sur le disque contient le mot de passe utilisé au moment du dernier login. Si la connection réseau est rompue ou que l'authentification par le plugin échoue mais que le nom et le mot de passe local sont utilisés, l'accés est autorisé. The Scramble Passwords on Logout allows for the retention of local accounts without also inherently providing local access by resetting the password of the local account to a random value. C'est très important que cet option soit activée SEULEMENT quand l'option 'Force Password' est aussi activée. Il est prévu que le non respect de celà entraine l'impossibilité d'accéder aux comptes locaux.

Quelques protocoles, comme LDAP, ignorent systématiquement les blancs dans les noms quand l'option "Allow Spaces in Usernames" n'est PAS selectionnée, pGina n'essaiera pas d'authentification si un nom d'utilisateur contient un blanc.

Autres Références

Article du support Microsoft sur "Setting up a custom default user profile":
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q305709

Autre documentation sur pGina
http://pgina.xpasystems.com

Forum de discussion 'Online'
http://forums.xpasystems.com/

Demandes professionnelles d'implémentations et de support
http://www.xpasystems.com

Mailing Lists:
General: http://lists.sourceforge.net/mailman/listinfo/pgina-general
Updates: http://lists.sourceforge.net/mailman/listinfo/pgina-updates
Developers: http://lists.sourceforge.net/mailman/listinfo/pgina-devel

Autres documentations sur les GINA
http://msdn.microsoft.com/library/en-us/security/security/winlogon_and_gina_start_page.asp