Aloaha Smartlogin

Mit Aloaha Smartlogin koennen Sie sich mit Ihrer Chipkarte, PKCS #11 Token oder einem USB Speicherstick an Ihr Windows System anmelden.

Auch einfache Karten wie MIFARE, I2C oder Kreditkarten werden unterstuetzt.

Sie koennen sich mit Aloaha weiterhin an Remote Desktops, Hyper-V Sessions oder Laufwerksfreigaben anmelden.

Aloaha unterstuetzt Domaenen und lokale Logons.

Contents

Features 3

Systemanforderungen 3

Installation 4

Logon Typen 4

- Chip Karte mit beliebigen Zertifikat 5
  - Automatisches Update der Softtoken bei Passwort Aenderung 7
  - Teilen der Softtoken via Netzkwerkfreigabe 7
  - Teilen der Softtoken via Active Directory 8
- MIFARE and Keycard 9
  - UserPass.ini Einstellungen 9
- PKCS #11 Token 10
- Einfacher USB Speicherstick 11

UserPass.ini Einstellungen 12

- Benutzername Feld ausblenden 12
- Aloaha Credential Provider Filter 12
- Aktion beim Entfernen der Karte 13
- ForceCRLChecks 13
- Notfall Anmeldung 13

Registry Einstellungen 13

- Sperrlistenabfragen konfigurieren 14
  - Aktivieren/de-aktivieren der Sperrlistenabfragen 14
  - Konfiguration der Sperrlistenabfrage 14

Windows XP/2003 and GINA (nicht mehr unterstuetzt) 15

SSO fuer standard Windows Anwendungen 15
Single Sign-On fuer Web Anwendungen 15
Andere nuetzliche Anwendungen 16
AloahaZIP 16
Zertifikate erstellen 16
Laufwerk mit einem Zertifikat verschluesseln: 16

Eine aktuelle Version finden Sie immer hier:
http://www.aloaha.com/handbuecher/AloahaSmartlogin_de.docx
http://www.aloaha.com/handbuecher/AloahaSmartlogin_de.pdf

Die englische Version finden Sie auf:
http://www.aloaha.com/handbuecher/AloahaSmartlogin_en.docx
http://www.aloaha.com/handbuecher/AloahaSmartlogin_en.pdf

Aloaha Smartlogin Homepage:
http://www.aloaha.com/smart-card-applications/aloaha-smart-login/

Features

- Unterstuetzt Kerberos Authentifizierung (Active Directory erforderlich).
- Chipkarten Logon auch OHNE Active Directory moeglich.
- Keine speziellen Anforderungen an das Logon Zertifikat.
- **Kartenanmeldung auch ohne Zertifikat moeglich (KeyCard).**
- Zusaetzlich zu Chip Karten koennen auch USB Speichersticks, PKCS #11[1] Token, MIFARE, Proximity Cards oder Speicherkarten als Logon Token benutzt werden.
- Logon auch an Netzwerkfreigaben, Remote Desktop Sessions, Hyper-V Konsolen, etc.
- Network Level Authentication (NLA) and Credential Security Support Provider (CredSSP) unterstuetzt.
- Chipkarten Logon auch fuer standard Windows Anwendungen (SSO)
- MSI basiertes Setup verfuegbar.

Systemanforderungen

- Windows XP (Anmeldung via GINA – mit dem Ende von XP nicht mehr unterstuetzt)
- Beliebiges 32/64 Bit Windows System ab Vista aufwaerts.
- .NET 3.5 Framework installiert.
- Active Directory wird unterstuetzt aber ist **NICHT ERFORDERLICH**
- Optional eine installierte Middleware[2] fuer benutzte Chip Karte

---

[1] Bitte stellen Sie sicher das die PKCS #11 Bibliothek Ihres Token installiert ist.

[2] Die Aloaha Middleware "Aloaha Cardconnector" unterstuetzt mehr als 45 verschiedene Chip Karten. Sollten Sie keine Middleware fuer Ihre Chip Karte besitzen koennen Sie den Aloaha Cardconnector von http://www.aloaha.com/download/cardconnector.zip installieren.

Installation

Den Installer koennen Sie von http://www.aloaha.com/download/smartlogin.zip starten. Auf Anfrage stellen wir auch gerne das komplette MSI Setup Paket zur Verfuegung.

Sollten Sie keine gueltige Lizenz besitzen fordern Sie bitte eine Testlizenz von info@aloaha.com an.

Falls Sie Zertifikate benutzen moechten muessen sicherstellen das Sie den Treiber bzw. die Middleware fuer Ihre Chipkarte installiert haben. Sollten Sie keine Middleware bzw. Treiber fuer Ihre Chipkarte besitzen oder aber die Aloaha Karte benutzen sollten Sie die Aloaha Middleware Aloaha Cardconnector benutzen. Der Cardconnector kann von http://www.aloaha.com/download/cardconnector.zip installiert werden.

Logon Typen

Die folgenden Logon Token werden unterstuetzt:

1. Chip Karte mit beliebigen Zertifikat.
   Diese Konfiguration wird von den meisten Kunden bevorzugt da keine Notwendigkeit besteht das das Zertifikat von einer Domain CA stammt. Weiterhin ist kein Active Directory zwingend erforderlich.
   http://www.win-logon.com/smartcard-based-windows-logon-with-any-certificate/

2. PKCS #11 Token
   http://www.win-logon.com/pkcs-11-logon/

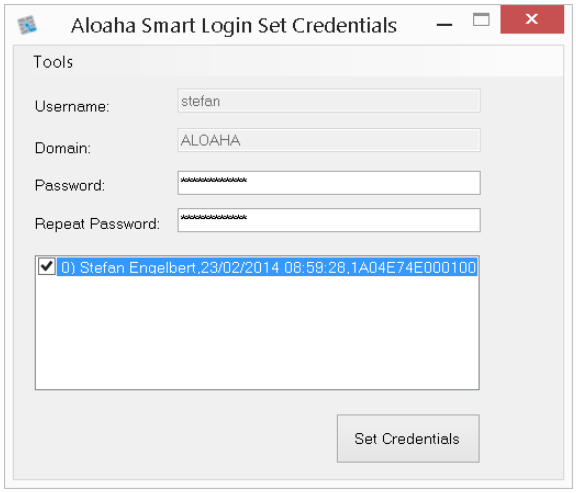
3. Einfacher USB Speicherstick
   http://www.win-logon.com/windows-logon-with-plain-usb-memory-stick/

4. Kerberos

5. MIFARE/Desfire/KeyCard
   Sie koennen Ihre Anmeldedaten direkt verschluesselt auf einer MIFARE Karte speichern.
   http://www.win-logon.com/logon-via-keycards-such-as-nfcmifaredesfire/

Chip Karte mit beliebigen Zertifikat

Um eine beliebige Chip Karte fuer das Logon zu benutzen muessen Sie zuerst die Chip Karte mit den Benutzerkennungen bekannt machen. Starten Sie dazu bitte „Encrypt Credentials“ vom Windows Startmenu oder „Card Credentials“ aus dem Aloaha System Tray. Sie sehen dann den folgenden Dialog:



Sie muessen hier Ihr Windows Passwort eintragen und das Chipkarten Zertifikat auswaehlen. Danach klicken Sie bitte „Set Credentials“.

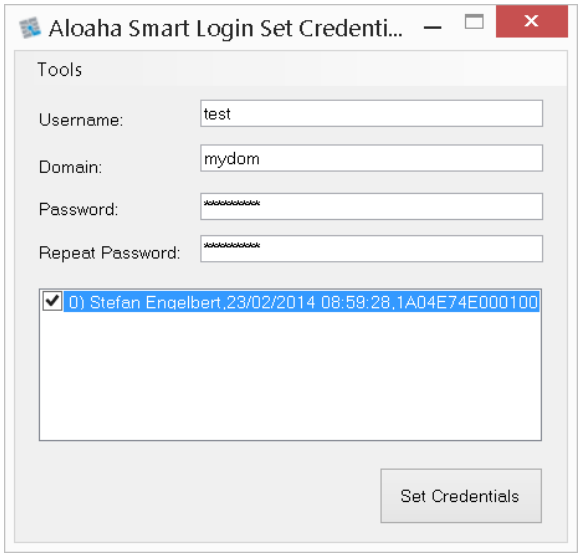
Ein Softtoken wurde nun generiert und in <Installdir>\CredentialStore abgelegt. Es enthaelt diverse Einstellungen, den oeffentlichen Teil des Zertifikates und ein verschluesseltes Geheimnis.

NUR der private Key der Karte kann dieses Geheimnis entschluesseln!

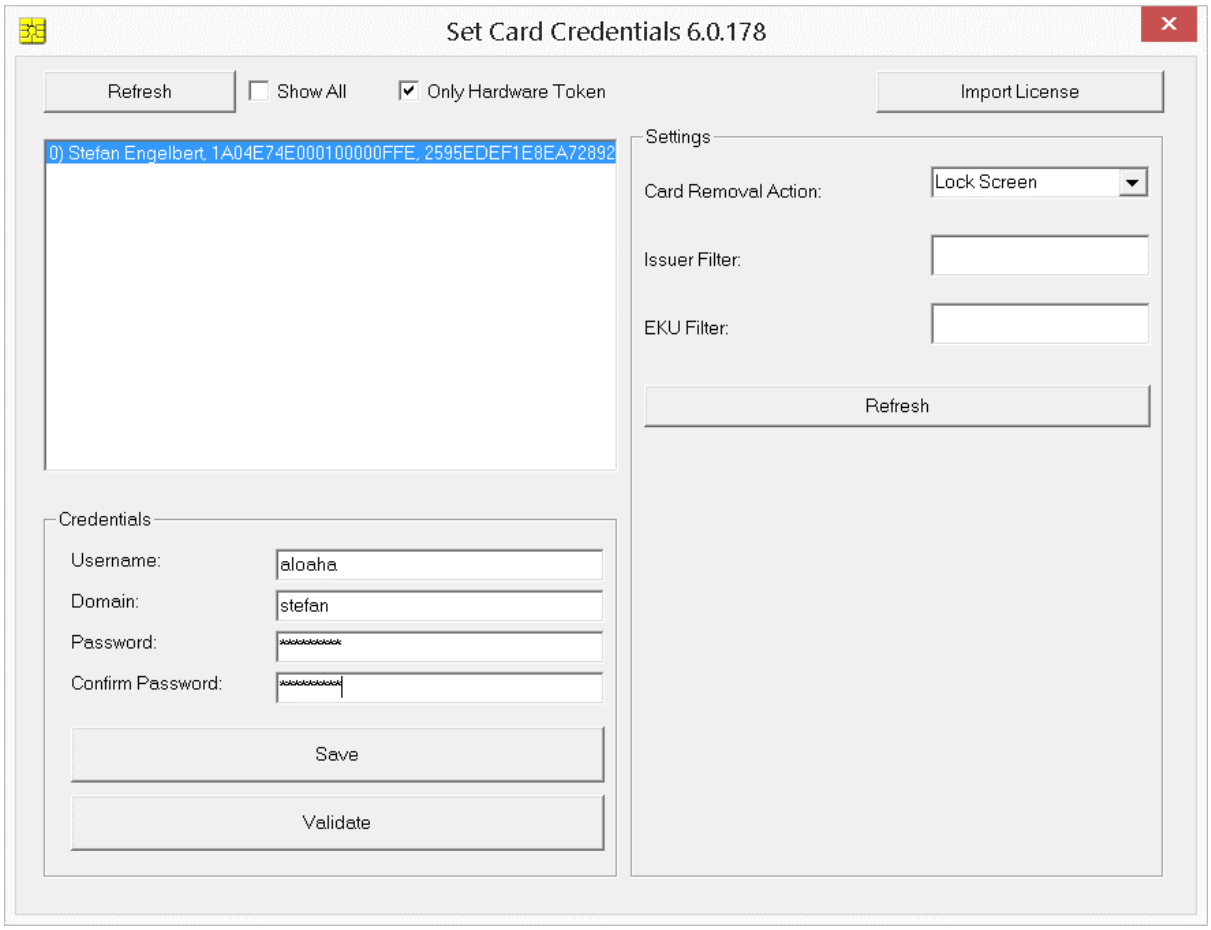
Es ist moeglich die Softtoken eines Rechners mit anderen Rechnern zu teilen. Das geht entweder via Active Directory oder Netzwerkfreigaben. Es wird in einem spaeteren Kapitel beschrieben.

Sie koennen sich nun bereits mit der Karte an das System anmelden.

In manchen Faellen ist es erforderlich das Sie verschiedene oder andere Benutzer einer Karte zuweisen. In dem Fall starten Sie bitte das Tool **SmartLogin_SetCredentials.exe** mit dem Parameter **/e** aus dem Installationsordner. Das Tool erlaubt Ihnen dann jedes Feld zu editieren:



Als eine Alternative koennen Sie auch das Tool **SetCredentials.exe** aus dem Installationsordner benutzen. Das Tool erlaubt es auch eine Benutzerzuweisung zu testen:



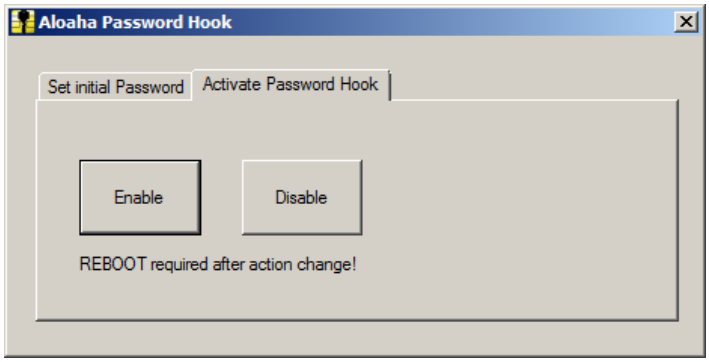
Automatisches Update der Softtoken bei Passwort Aenderung

Ein Softtoken muss upgedated werden sobald ein Benutzer sein Passwort aendert. Mit dem **Password Hook** kann man diese Updates automatisieren.

Der Password Hook muss auf dem System aktiviert werden auf dem die Benutzerpasswoerter gespeichert werden. In einer Domain ist das der Domain Controller. Lokale Benutzer werden immer auf der lokalen Maschine gespeichert.

Um den Password Hook zu installieren muss Smartlogin installiert sein. Sie finden dann das Tool **PasswdHK.exe in <InstallDir>\PasswdHK.exe**.

Rufen Sie das Tool mit einem rechten Mausklick -> „Als Administrator ausfuehren“ auf. Dann waehlen Sie den Tab „Activate Password Hook“ wie im Screenshot gezeigt:



Nun koennen Sie mit einem Klick auf „Enable“ und einen Neustart den Hook aktivieren.

Teilen der Softtoken via Netzkwerkfreigabe

Per Default werden dieSofttoken in <Installdir>\CredentialStore gespeichert. Sie koennen natuerlich den Ordner umdefinieren oder sogar ein Netzwerk Share angeben. Dazu aendern Sie bitte den Wert in **HKLM\SOFTWARE\<Wow6432Node>\Aloaha\CSP\CredentialStore** entsprechend.

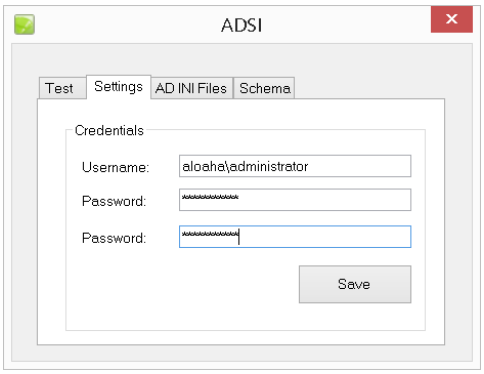
Beachten Sie aber bitte das der Logon Prozess als „Local System“ laeuft und Sie deshalb sicherstellen muessen das die Netzwerkfreigabe diesem Benutzer auch die entsprechenden Rechte einraeumt.

Teilen der Softtoken via Active Directory

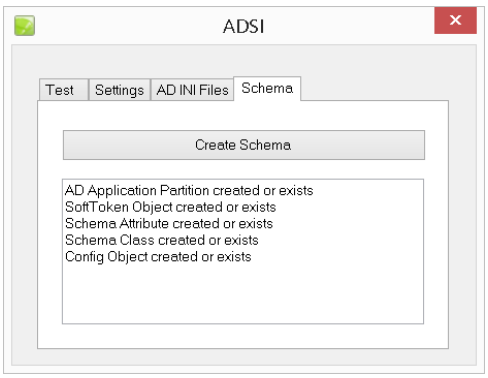
Sollte Ihre Maschine Mitglied in einer Domain sein koennen Sie die Softtoken auch ueber das Active Directory roamen.

Aloaha benutzt dazu eine dedizierte „Active Directory Application Partition“. Um diese Partition zu erstellen muessen Sie einmalig folgende Schritte ausfuehren:

1. Stellen Sie sicher das Sie mit einem Benutzer mit „Schema-Admin“ Rechten angemeldet sind.
2. Erstellen Sie den Wert **ForceCreate** in **HKLM\SOFTWARE\<Wow6432Node>\Aloaha\AD** und weisen Sie dem Wert die Nummer **1** zu.
3. Laden und starten Sie AloahaADSI von: http://23.102.21.128:8080/f/295da15224/
4. Waehlen Sie den **„Settings“** Tab und tragen Sie Benutzername und Password fuer den Schema-Admin ein. Sobald Sie die Credentials mit **„Save“** speichern werden die Passwort Felder geleert.



5. Nun oeffnen Sie bitte den **„Schema“** Tab und betatigen „Create Schema“. Im Ausgabefenster sollten Sie eine aehnliche Ausgabe wie im Screenshot sehen:

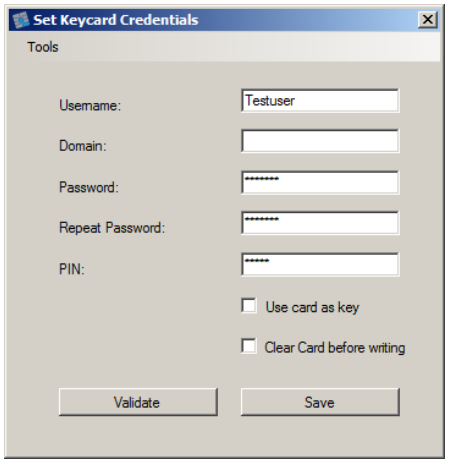


6. Nun koennen Sie das Tool beenden. Loeschen Sie **HKLM\SOFTWARE\<Wow6432Node>\Aloaha\AD\ForceCreate** um den Schema Tab zu verbergen.

Die noetige Partition ist nun fertig erstellt und kann von Smartlogin benutzt werden. Um das AD Roaming zu aktivieren setzen oder erstellen Sie bitte den Wert **enabled** in **HKLM\SOFTWARE\<Wow6432Node>\Aloaha\AD** auf **1**

MIFARE and Keycard

Unter MIFARE und Keycard Token fassen wir alle Token zusammen die nicht in eine der anderen Kategorien passen. Das sind zum Beispiel MIFARE Classic und Desfire, Zeitkontrol 3.14[3] Karten, Chipkarten ohne Zertifikat und auch Kreditkarten.



Bitte tragen Sie Ihren Benutzernamen, optional Ihre Domaene und natuerlich Ihr Passwort hier ein.

Fuer das PIN Feld muessen Sie sich Ihre eigene PIN ausdenken. **Es ist NICHT die PIN der Karte gemeint!**

Die PIN wird als Teil das Passwortes in die Verschluesselung der Daten einfliessen.

Sie muessen „Use card as key“ aktivieren!

UserPass.ini Einstellungen

Um MIFARE oder Keycards benutzen zu koennen kann es sein das Sie einige Einstellungen in der UserPass.ini manuell vornehmen muessen. Sie finden diese Datei im Installationsordner.

```
[Generic]
AllowMIFARE=1
AllowVisa=1
AllowATR=0
ForceMonitorKeyCards=1
AllowPayFlex=1
AllowPGP=1
```

In jedem Fall muessen Sie **AllowMIFARE** auf 1 setzen. **Das gilt auch fuer nicht-MIFARE Karten!**

AllowVisa braucht nur dann auf 1 gesetzt werden wenn Sie planen Kreditkarten als Logon Token zuzulassen.

`AllowPayFlex` braucht nur dann auf 1 gesetzt werden wenn Sie planen `PayFlex Karten` als Logon Token zuzulassen.

`AllowPGP` braucht nur dann auf 1 gesetzt werden wenn Sie planen PGP Karten als Logon Token zuzulassen.

Bitte setzen Sie **AllowATR** nur dann auf 1 wenn Sie eine Karte oder Token benutzen die ihre eindeutige ID im ATR einbettet. Zum Beispiel HID Proximity Cards wie H10301.

---

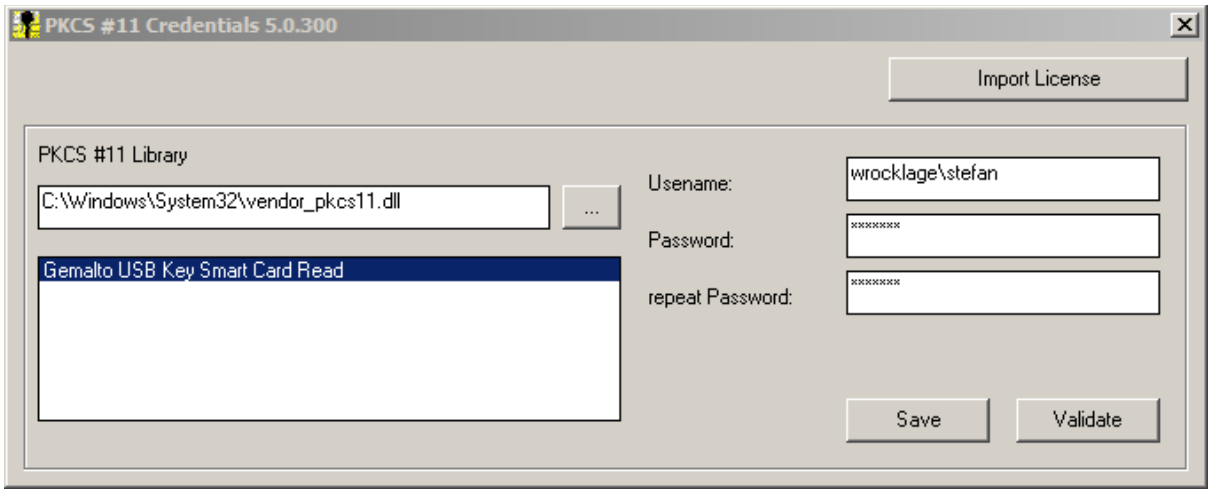
[3] Mit Aloaha Firmware

Wenn Sie **ForceMonitorKeyCards** auf 1 setzen wird die Karte konstant gepollt damit besser erkannt wird ob eine Karte entfernt wird.

PKCS #11 Token

Falls Sie sich mit einem PKCS #11 Token an das System anmelden moechten werden Ihre Credentials auf dem Token selbst verschluesselt gespeichert. Es ist wichtig das Sie Ihre PKCS #11 Bibliothek korrekt installiert haben.

Um Ihre Credentials auf dem Token zu speichern starten Sie bitte „PKCS #11 Credentials“ vom Windows Startmenu oder dem Aloaha System Tray.

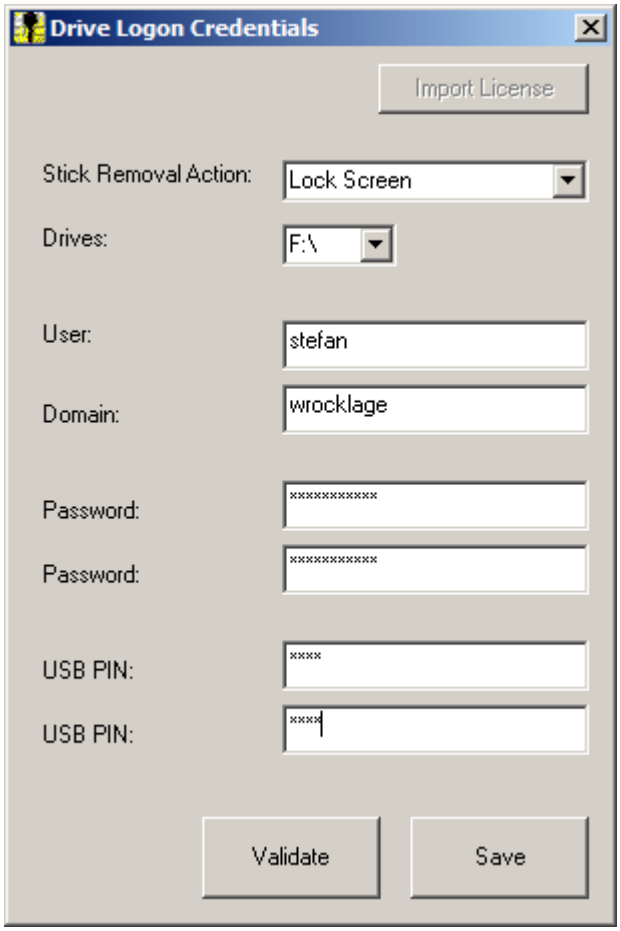


1. Waehlen und konfigurieren Sie Ihre PKCS #11 Bibliothek.
2. Ihr Token sollte nun in der Liste erscheinen. Waehlen Sie den zu benutzenden Token aus der Liste.
3. Geben Sie <domain>\Benutzerkennung und Ihr Passwort ein.
4. Speichern Sie mit einem Klick auf „Save“ Ihre verschluesselten Credentials auf Ihrem PKCS #11 Token. Mit „Validate“ koennen Sie ein Logon simulieren.

Einfacher USB Speicherstick

Es ist auch moeglich einen normalen USB Speicherstick als Logon Token zu benutzen. Ihre Credentials werden dabei verschluesselt auf dem Token selbst gespeichert.

Da USB Speichersticks keinerlei Crypto Prozessor haben ist diese Methode natuerlich weniger sicher als die Benutzung von echten Chip Karten!



In diesem Dialog muessen Sie den Laufwerksbuchsaben Ihres USB Sticks, Ihren Benutzernamen, optional den Domainnamen und Ihr Windows Passwort eintragen. Es ist sehr wichtig das Sie eine PIN spezifizieren. Diese PIN wird zur Verschluesselung der Credentials mit benutzt. Weiterhin benoetigen Sie spaeter diese PIN um sich am System anzumelden.

UserPass.ini Einstellungen

Benutzername Feld ausblenden

Der Bentzername kann beim Logon leer gelassen werden. Aloaha versucht dann, anhand des Kartenzertifikates, den richtigen Usernamen zu waehlen. Sie koennen das Username Feld auch komplett ausblenden:

<Installdir>UserPass.ini

[Generic]
DisableUserName=0
EnableUserName=1

[Generic]
DisableUserName=1
EnableUserName=0

Aloaha Credential Provider Filter

Mit dem Aloaha Credential Provider Filter ist est moeglich unerwuenschte Logon Tiles zu verbergen:

Manchmal ist es erwuenscht das nicht alle moeglichen Logon Tiles im Anmeldeschirm angezeigt werden. Wenn man diese per Group Policy oder Registry deaktiviert dann werden diese Logon Arten auch aus der Session selbst entfernt. Das ist jedoch keine gute Idee da man innerhalb der Session diese Mechanism noch benoetigt. Deshalb gibt es den Filter. Mit dem Filter werden die Tiles NUR vom Anmeldeschirm entfernt.

Um den Filter zu aktivieren muessen Sie die UserPass.ini editieren. In der Sektion **CredentialProviders** koennen Sie fuer jedes Logon Tile einen entsprechenden Filter aktivieren. Im folgenden Beispiel werden ALLE nicht Aloaha Tiles verborgen.

```
[CredentialProviders]

25CBB996-92ED-457e-B28C-4774084BD562=1
3dd6bec0-8193-4ffe-ae25-e08e39ea4063=1
503739d0-4c5e-4cfd-b3ba-d881334f0df2=1
6f45dc1e-5384-457a-bc13-2cd81b0d28ed=1
8bf9a910-a8ff-457f-999f-a5ca10b4a885=1
94596c7e-3744-41ce-893e-bbf09122f76a=1
```

```
AC3AC249-E820-4343-A65B-377AC634DC09=1
e74e57b0-6c6d-44d5-9cda-fb2df5ed7435=1
F8A0B131-5F68-486c-8040-7E8FC3C85BB6=1
```

Aktion beim Entfernen der Karte

Standardmaessig benutzt Aloaha die Maschinen- oder Domain Einstellungen der Aktion beim Entfernen der Karte. Dieses Verhalten kann jedoch umdefiniert werden:

[AutoLock]
PolicyAction=1
RemoveActionM=1

Weiterhin muessen Sie noch folgenden Eintrag in der Registry anpassen:
HKLM\Software\<*Wow6432Node*\>Aloaha\CSP\RemoveAction=1

1 = Lock Screen, 2 = Lock Off, 3 = Reboot

ForceCRLChecks

```
[Generic]
ForceCRLChecks=1
```

Wenn dieser Wert auf 1 steht wird die Abfrage der Sperrlisten erzwungen. Keine andere Einstellung kann diese Einstellung deaktivieren.

Notfall Anmeldung

```
[Generic]
AllowUP=1
```

Solange AllowUP auf 1 gesetzt ist (Standard) kann sich der Benutzer im Notfall noch immer per Passwort anmelden. Er muss dann dem Usernamen ein up: voransetzen und anstelle der PIN sein Passwort eingeben. Also er tippt up:JohnDoe anstelle von JohnDoe in das Benutzernamen Feld und LetMeIn anstelle der PIN 0815.

Registry Einstellungen

Bild der Kachel aendern

Es ist moeglich das Bild der Logonkachel zu aendern. Dazu erstellen Sie bitte in HKLM\Software\Aloaha\CP den Schluessel tileImage und tragen dort den Pfad eines BMP Bildes ein.

Diese BMP Datei sollte im Format 480x480x32 sein.

Sperrlistenabfragen konfigurieren

Bei einem frisch installiertem Aloaha Smartlogin sind Sperrlistenabfragen nicht aktiviert. Dafuer gibt es verschiedene Gruende:

1. Waehrend der Testphase benutzen die meisten Kunden Testzertifikate um sich anzumelden. In den meisten Faellen gibt es fuer diese Testzertifikate keine funktionsfaehige CA und Sperrlistenabfragen wuerden fehlschlagen.
2. Falls ein Benutzer seine Karte als verloren oder gestohlen meldet reicht es vollkommen aus den Softtoken fuer die Karte zu loeschen ODER das Passwort des Benutzers zu aendern. Die verlorene Karte hat dann keine Chance mehr sich anzumelden. Mit einer neuen Karte und einem neuen Zertifikat kann sich der Benutzer aber weiterhin anmelden.

Der zweite Punkt zeigt das Sperrlistenabfragen eine zusaetzliche Sicherheitschicht darstellen. Aber auch ohne diese Schicht kann man sicher arbeiten und Karten sperren.

Aktivieren/de-aktivieren der Sperrlistenabfragen

Die Abfragen koennen mit HKLM\SOFTWARE\<Wow6432Node>\Aloaha\CSP\CertificateAlwaysValid aktiviert oder deaktiviert werden. Standard hier ist deaktiviert.

Konfiguration der Sperrlistenabfrage

Komplette Kette erforderlich:
HKLM\<Wow6432Node>\Software\Aloaha\CSP\EnforceChain

HKLM\<Wow6432Node>\Software\Aloaha\CSP\ ForceCRLChecks
Details in Kapitel: **ForceCRLChecks**

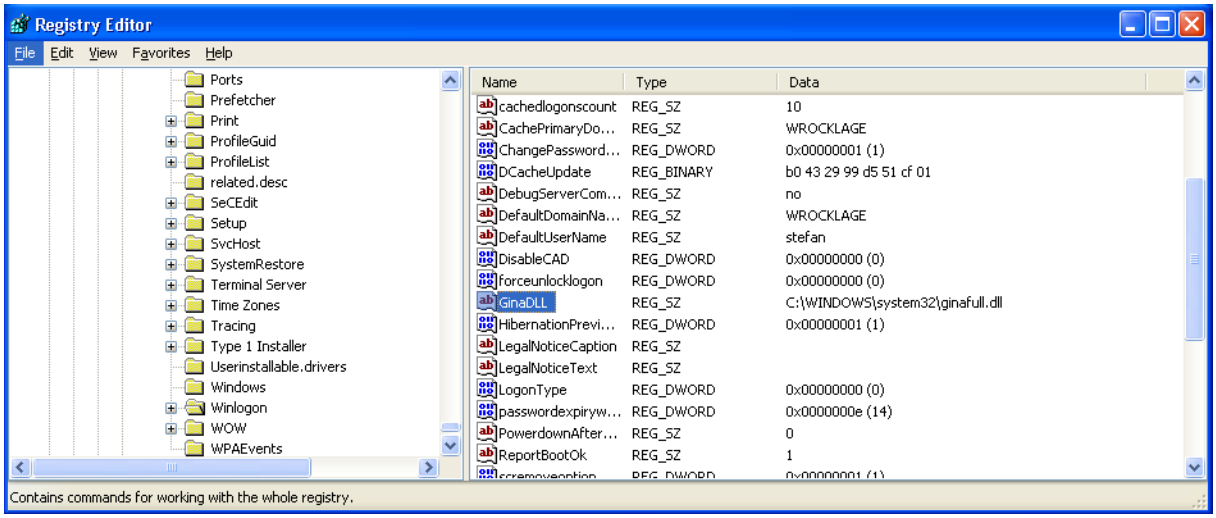
Welche CRL soll benutzt werden?
HKLM\<Wow6432Node>\Software\Aloaha\CSP\ForceCRL
HKLM\<Wow6432Node>\Software\Aloaha\CSP\offCRL
HKLM\<Wow6432Node>\Software\Aloaha\CSP\onlCRL
HKLM\<Wow6432Node>\Software\Aloaha\CSP\ForceOCSP

Falls Sperrlistenstatus unbekannt ist akzeptiere das Zertifikat:
HKLM\<Wow6432Node>\Software\Aloaha\CSP\UnknownCertStatusIsValid

Erlaube abgelaufene Zertifikate:
HKLM\<Wow6432Node>\Software\Aloaha\CSP\IgnoreCertTime

Windows XP/2003 and GINA (nicht mehr unterstuetzt)

Auf Windows XP/2003 benutzt Aloaha eine GINA dll und keinen Credentialprovider. Manchmal ist es erforderlich die Gina zu entfernen oder zu de-aktivieren. IN diesem Fall entfernen Sie bitte GinaDLL aus HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion.



SSO fuer standard Windows Anwendungen

Bitte lesen Sie dazu folgende Dokumente:

PDF: http://www.aloaha.com/handbuecher/l_sso.pdf

DOCX: http://www.aloaha.com/handbuecher/l_sso.docx

Single Sign-On fuer Web Anwendungen

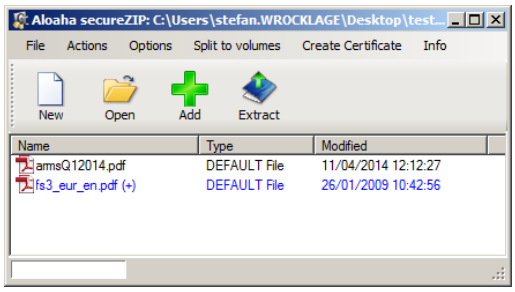
PDF: http://www.aloaha.com/handbuecher/HTML_SSO.pdf

DOCX: http://www.aloaha.com/handbuecher/HTML_SSO.docx

Andere nuetzliche Anwendungen

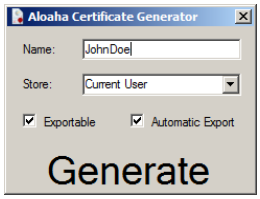
Aloaha bietet eine Reihe von nuetzlichen portablen Anwendungen fuer lizensierte Aloaha Benutzer an.

AloahaZIP



Mit AloahaZIP koennen Sie Ihre ZIP Dateien mit Zertifikaten verschluesseln:

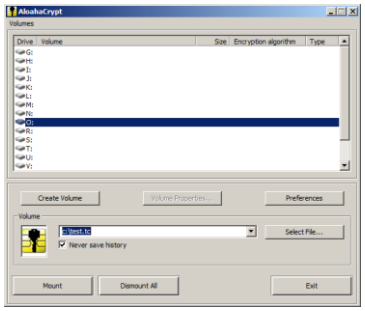
http://www.aloaha.com/download/aloahazip.zip



Zertifikate erstellen

Natuerlich gibt es auch ein Tool um schnell und einfach Zertifikate zu erstellen:

http://www.aloaha.com/download/AloahaCertificateCreator.zip

Laufwerk mit einem Zertifikat verschluesseln:

http://www.aloaha.com/download/AloahaCrypt%20Setup1.3b.zip