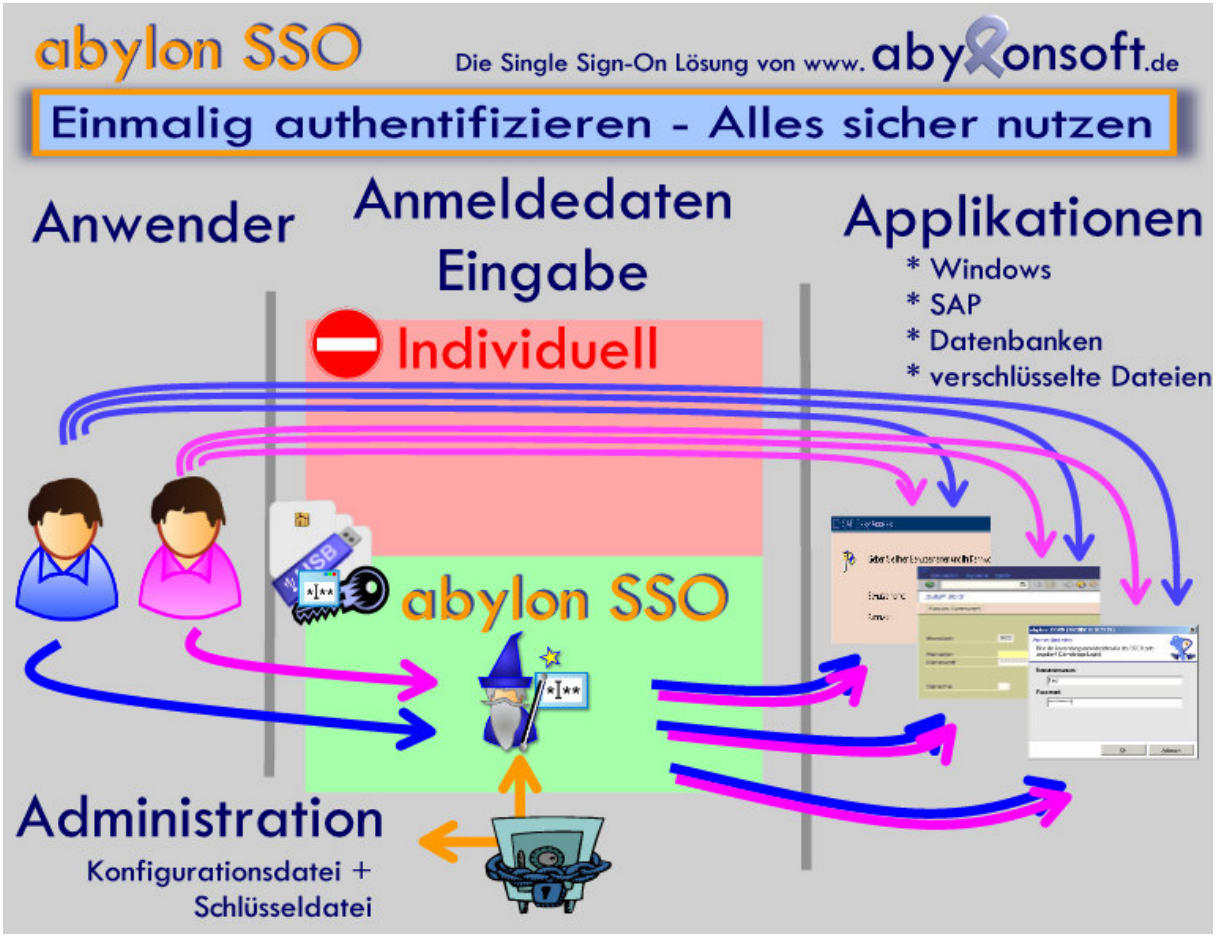
INHALTSVERZEICHNIS

1 EINFÜHRUNG

Dieses Whitepaper beschreibt die Funktionsweise und die Verwendung des Softwareproduktes **abylon SSO**. Anhand von Anwendungsbeispielen wird der Einsatz beschrieben und die Technik hinter dem Produkt erklärt.

- Anlernen von Fenstern
- Automatisches Eintragen von Anmeldedaten
- Administration

1.1 Allgemeine Funktionsweise



Die Software **abylon SSO** unterstützt den Anwender bei der Eingabe von Anmeldedaten, wie Anmeldename und Passwort. Dazu werden die Anmeldefenster einmalig durch Eingabe der entsprechenden Anmeldedaten angelernt. Diese Daten werden verschlüsselt gespeichert. In Zukunft werden nach der Legitimation des Anwenders automatisch die Anmeldedaten durch die Software **abylon SSO** in die entsprechenden Felder eingetragen. Zur Legitimation des Anwenders bieten sich folgende Möglichkeiten:

- Zertifikatschipkarte und Token
- Prozessorchipkarte
- Speicherchipkarte
- Wechseldatenträger
- CD/DVD
- RFID - Karten
- Passwort

HINWEIS Spezielle Unterstützung auf Anfrage!

Im übersichtlichen Administrationsbereich können einzelne User, Karten oder Applikationen aktiviert, deaktiviert oder gesperrt werden. Die kompletten Anmeldedaten werden in einer verschlüsselten XML-Datei gespeichert, sodass auch eine zentrale Administration auf einem Server möglich ist.

1.2 Vorteile

Die Anzahl der benötigten Passwörtern steigt unaufhaltsam und für normaler Anwender wird es immer schwerer sich diese alle zu merken. Als Strategie verwendet der Anwender identische Anmeldedaten für alle Authentifizierungen, leicht zu merkende, aber unsichere Passwörter oder schreib diese an einer unsicheren Stelle auf. Dadurch wird die eigentlich benötigte Sicherheit ausgehebelt und ermöglicht Crackern einen einfachen Angriffspunkt, z. B. durch Phishing-Attacken. Durch diese Unsicherheit können geheime Daten in die falschen Hände gelangen und im schlimmsten Fall kann sogar ein finanzieller Schaden entstehen.

Die Software **abylon SSO** bietet eine hilfreiche Unterstützung, ohne die Sicherheit zu reduzieren. Der Anwender muss sich nur einmalig authentifizieren und kann im Anschluss auf alle sicher gespeicherten Anmeldedaten zugreifen.

In Netzwerken mit mehreren Anwender können die Konten und Anmeldedaten von einem Administrator zentral verwaltet werden. Durch die Verwendung von Hardwaretoken (z. B. Chipkarten oder USB – Sticks) kommt der einzelne Mitarbeiter nicht mehr in den Besitzt der realen Anmeldedaten. Durch ein spezielles Softwareverfahren wurde während des Single Sign-On Vorgangs die reale Tastatur- und Mauseingabe gesperrt, damit die Anmeldedaten nicht auf Klartextfelder umgelenkt und somit ausgespäht werden können.

Der Administrator kann die realen Zugangsdaten unabhängig ändern ohne die Token's erneut anzulernen. Einzelne Token's können nach Bedarf auch zeitweise deaktiviert oder gesperrt werden. Ein vollständiges Entfernen de Token's aus der Datenbank macht eine weitere Verwendung unmöglich.

- Nur noch einmalige Authentifizierung notwendig
- Automatische Fenstererkennung
- Keine unsichere Speicherung von Passwörtern
- Verwendung von komplexeren und unterschiedlichen Passwörtern
- Erhöhter Schutz gegen Keyloggern und Phishing-Attaken
- Hohe Flexibilität
- Zentrale Administration

1.3 Systemvoraussetzungen

- Prozessor: Pentium (oder vergleichbar)
- Arbeitsspeicher: 256 MByte RAM
- Freier Festplattenspeicher ca. 25 Mbyte
- Betriebssystem Windows NT4, 2000, XP, Vista 32 und 64bit, 2003 oder WTS
- Bildschirmauflösung: mind. 1024x768 Pixel
- Administrationsrechte für die Installation
- Optional Kartenleser mit Chipkarte, Wechseldatenträger oder CD

2 DER START

2.1 Start

2.1.1 Installation

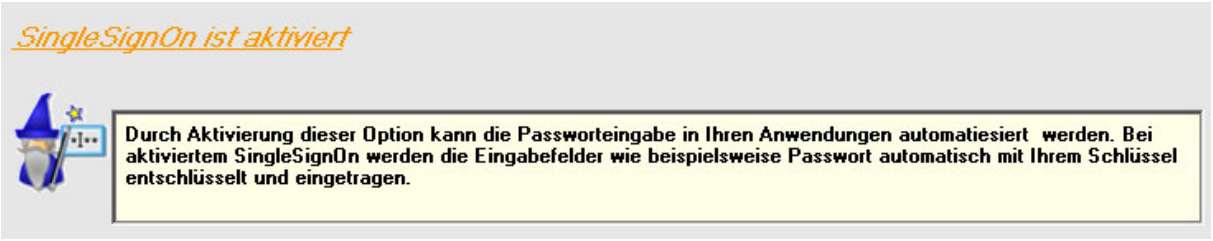
Die Software **abylon SSO** wird als ausführbares Setup ausgeliefert, mit dem Sie Schritt für Schritt durch die Installation geleitet werden. Dabei werden die benötigten Dateien in das Programmverzeichnis kopiert und erste grundlegende Einstellungen vorgenommen.

Für eine Testphase von 30 Tagen kann die Software **abylon SSO** kostenlos getestet werden. Um die Software auch nach Ablauf der Testphase nutzen zu können, müssen Registrierungsdaten zur Freischaltung eingegeben werden.

HIWEIS: Deinstallationsroutine zum Entfernen der Software ist ebenfalls vorhanden!

2.1.2 Aktivieren

Zum Aktivieren muss im Einstellungsdialog auf das "Zauberer-Icon" geklickt werden. Im Anschluss wird auf der Seite angezeigt, dass das Single Sign-On aktiviert ist.



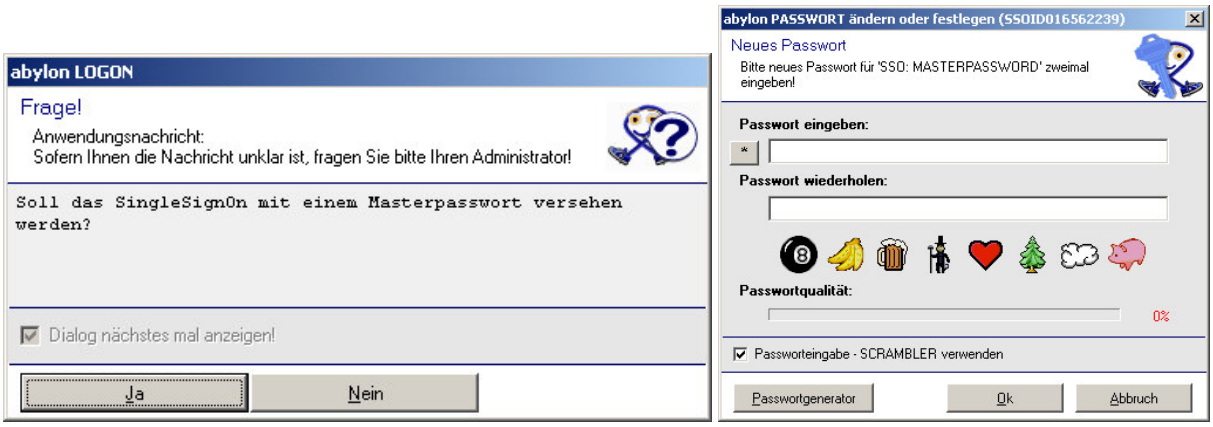
2.1.3 Legitimation festlegen

Zur Legitimation können unterschiedliche Medien verwendet werden, wie z. B. Chipkarten oder Wechseldatenträger (Detaillierte Supportübersicht siehe Hilfe oder sprechen Sie uns an). Wenn mehrere mögliche Medien am Rechner zur Auswahl stehen, wird eine Übersicht zur Auswahl angezeigt.

HINWEIS: In den Einstellungen auf der Seite 'SSO Einstellungen' könne die gültigen Medien aktiviert und deaktiviert werden (siehe Kapitel SSO Einstellungen auf Seite 13).

2.1.4 Masterpasswort

Nach der Festlegung der Legitimation kann optional ein Masterpasswort definiert werden.



Damit wird ein zusätzlicher Schutz der Passworteingabe erreicht. Neben der Legitimation durch das Medium muss zusätzlich das Masterpasswort eingegeben werden.

2.1.5 Überwachung

In Zukunft überwacht die Software **abylon SSO** alle geöffneten Fenster. Sobald ein Fenster mit Passwortabfrage erkannt wird, kann dieses Fenster angelernt werden. Sobald das Fenster erneut geöffnet wird, trägt die Software **abylon SSO** die Anmeldedaten automatisch in die entsprechenden Felder ein.

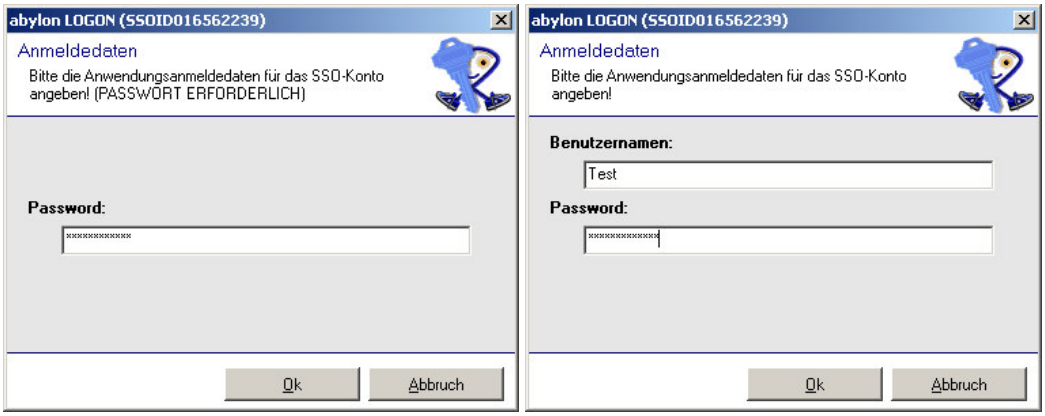
2.2 Passwortdialoge anlernen

Damit Anmeldedialoge automatisch durch die Software **abylon SSO** ausgefüllt werden, müssen die Anmeldedaten einmalig angelernt werden. Dieser Vorgang kann **automatisch** oder **manuell** erfolgen.

2.2.1 Automatisch

Die Software **abylon SSO** erkennt einen geöffneten Passwortdialog automatisch und öffnet folgenden Fragedialog.

Nach Bestätigung dieses Fragedialog mit 'Ja' müssen Ihre Anmeldedaten in den folgenden Fenstern eingegeben werden.

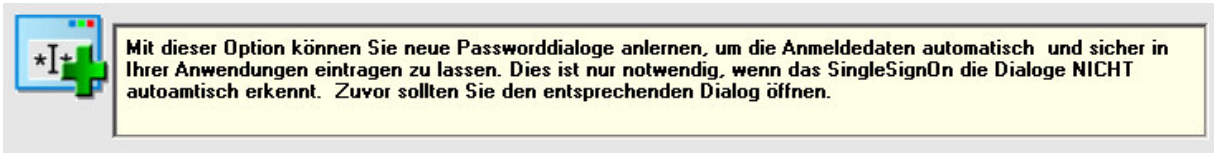


Diese Daten werden nun in den Anmeldedialog eingetragen. Für zukünftige Anmeldevorgänge werden die Daten in einer verschlüsselten Datei gespeichert.

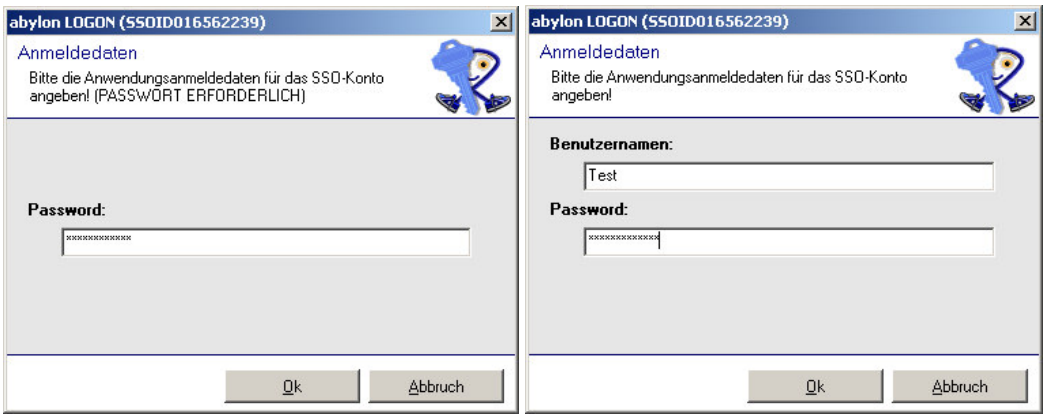
Wenn dieser Fragedialog mit 'Nein' bestätigt wird, wird der entsprechende Passwortdialog in Zukunft ignoriert. In den Einstellungen auf der Seite 'SSO Applikationen' kann das Verhalten der entsprechenden Applikation geändert werden (siehe Kapitel Einführung auf 10 Seite).

2.2.2 Manuell

Für den Fall, das ein Passwortdialog nicht automatisch durch die Software **abylon SSO** erkannt wird, kann der Dialog auch manuell angelernt werden. Öffnen Sie dazu den Einstellungsdialog und klicken auf 'Passwortdialog anlernen'.



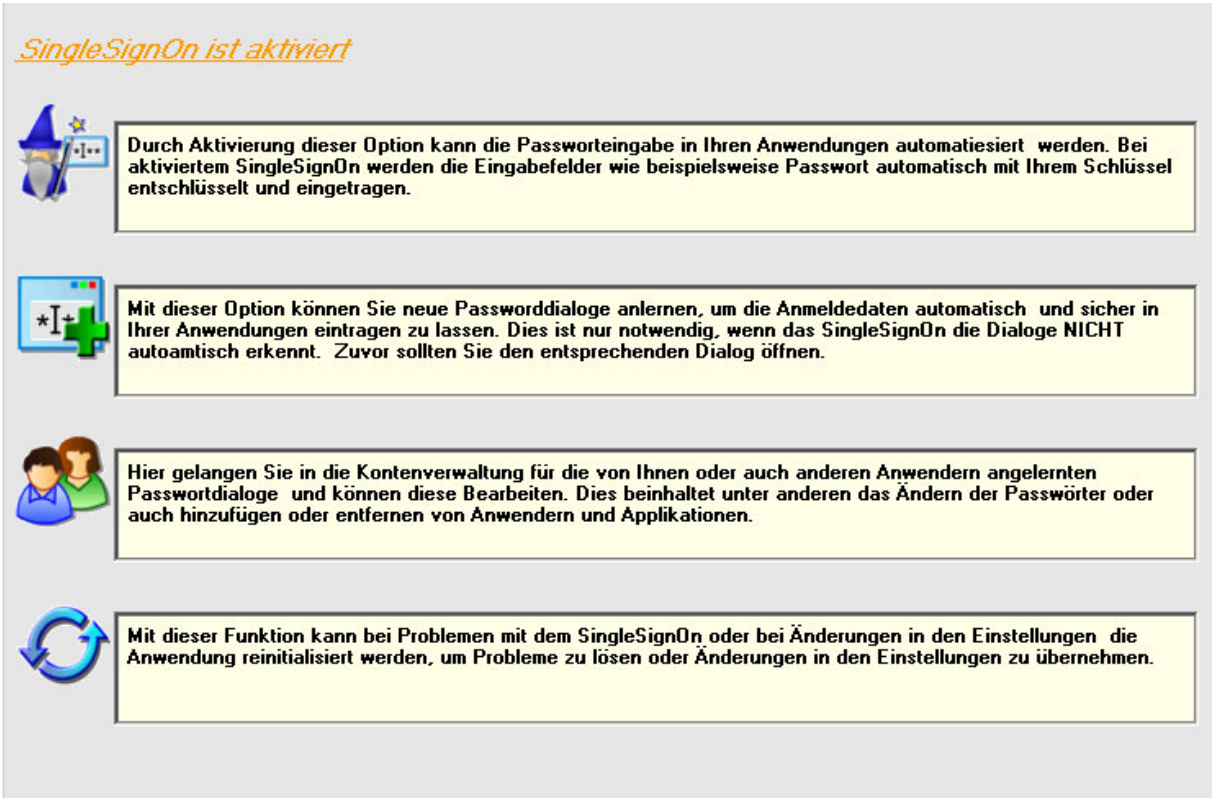
Es wird eine Liste mit allen geöffneten Fenstern angezeigt, in dem das anzulernende Fenster ausgewählt wird. Im Anschluss geben Sie die benötigten Anmeldedaten ein.



Die Software **abylon SSO** trägt die Daten in das entsprechende Passwortdialog ein.

2.3 Einstellungen

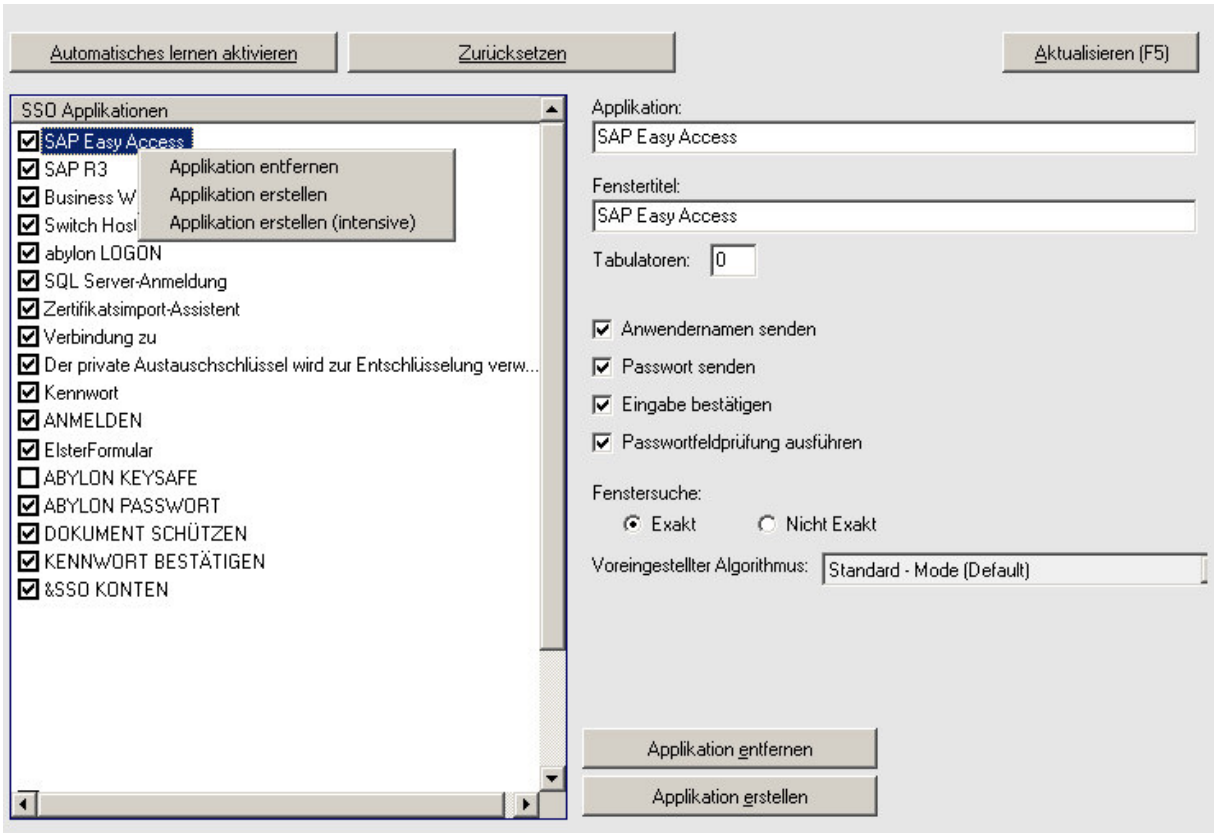
2.3.1 Startseite



Auf der ’SSO Startseite’ werden folgende Funktionen mit einer kurzen Beschreibung angezeigt:

- abylon SSO aktivieren/deaktivieren
- Manuelles Anlernen von Passwortdialogen
- Aufruf der Kontenverwaltung
- Reinitialisieren der Anwendung

2.3.2 SSO Applikationen

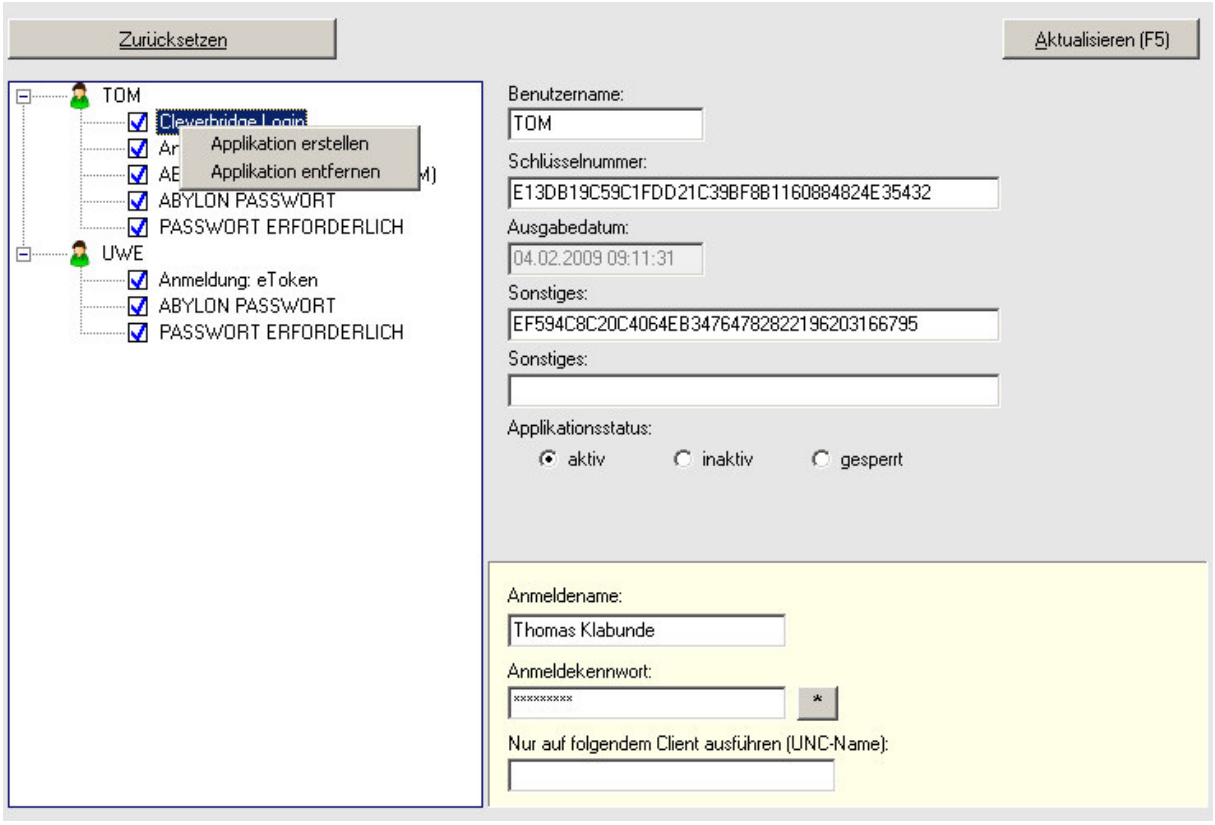


Auf der Seite 'SSO Applikationen' wird eine Liste mit allen angelernten Applikationen angezeigt. Als Applikation wird der Passwortdialog bezeichnet.

Hier können einzelne Applikationen erstellt, aktiviert (Häkchen), deaktiviert (kein Häkchen) oder entfernt werden. Zudem ist hier das Eintragverhalten der Software administrierbar, wie z. B. ob der Anmeldename gesendet oder ob eine Passwortfeldprüfung ausgeführt werden soll.

Sofern das "Automatische lernen" aktiviert ist, werden die Applikationen automatisch der Liste hinzugefügt.

2.3.3 SSO Konten



Auf der Seite 'SSO Konten' wird eine Liste mit allen Konten und angelernten Applikationen angezeigt.

Konten können hier erstellt, entfernt oder kopiert werden. Applikationen können anwenderspezifisch erstellt, entfernt, deaktiviert oder gesperrt werden. Zudem ist das Ändern von Anmeldename und Passwort möglich.

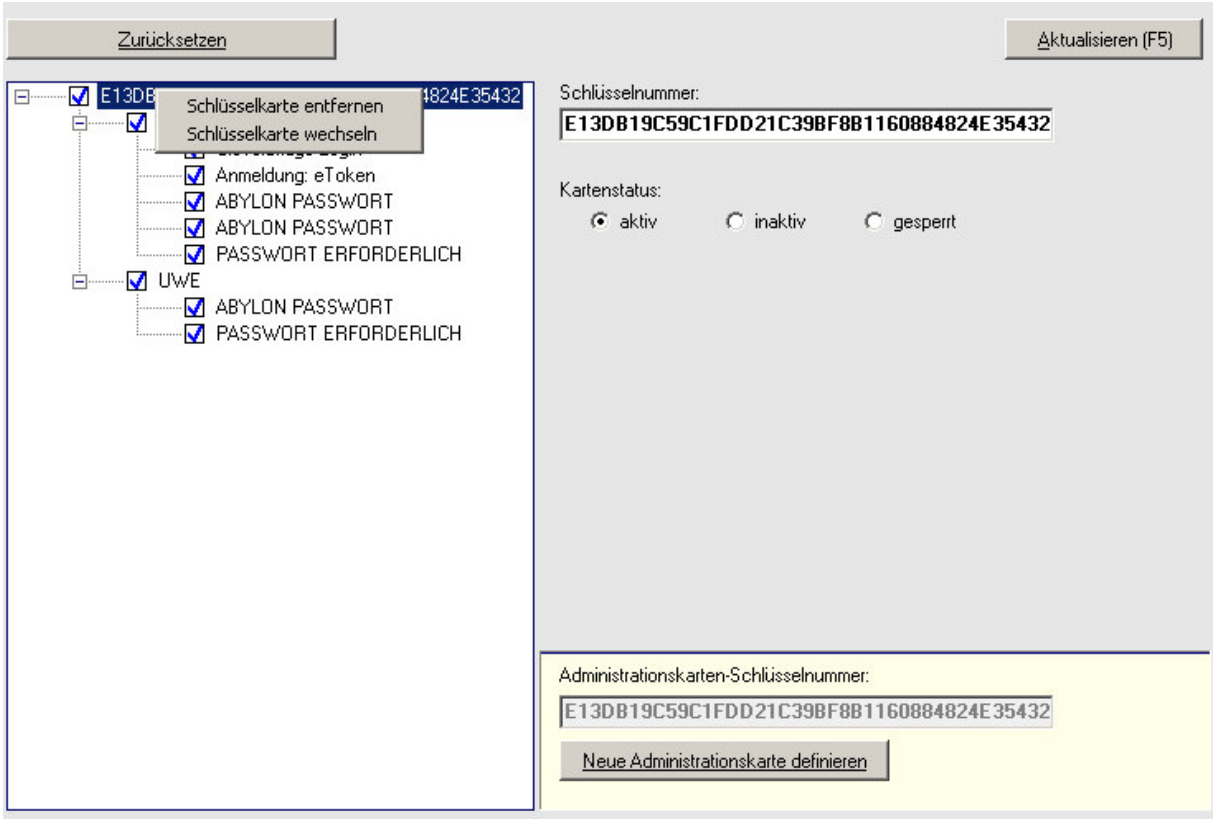
2.3.3.1 Applikationsdaten

- **Benutzername:** Name des Benutzers (kann frei definiert werden)
- **Schlüsselnummer:** Einmalige Nummer des verwendeten Schlüssels (kann frei definiert werden)
- **Ausgabedatum:** Datum, an dem die Applikationsdaten angelegt wurden (wird beim Erstellen festgelegt)
- **Sonstiges:** Frei definierbares Feld (z. B. für Berechtigungscode)
- **Sonstiges (2):** Frei definierbares Feld (z. B. für Applikationscode)
- **Status:** Möglicher Status der Applikation **aktiv**, **inaktiv** und **gesperrt** (kann frei definiert werden)

Anmeldedaten (im gelben Feld): Diese sind nur für den Administrator mit Eigentümerkarte sichtbar und editierbar.

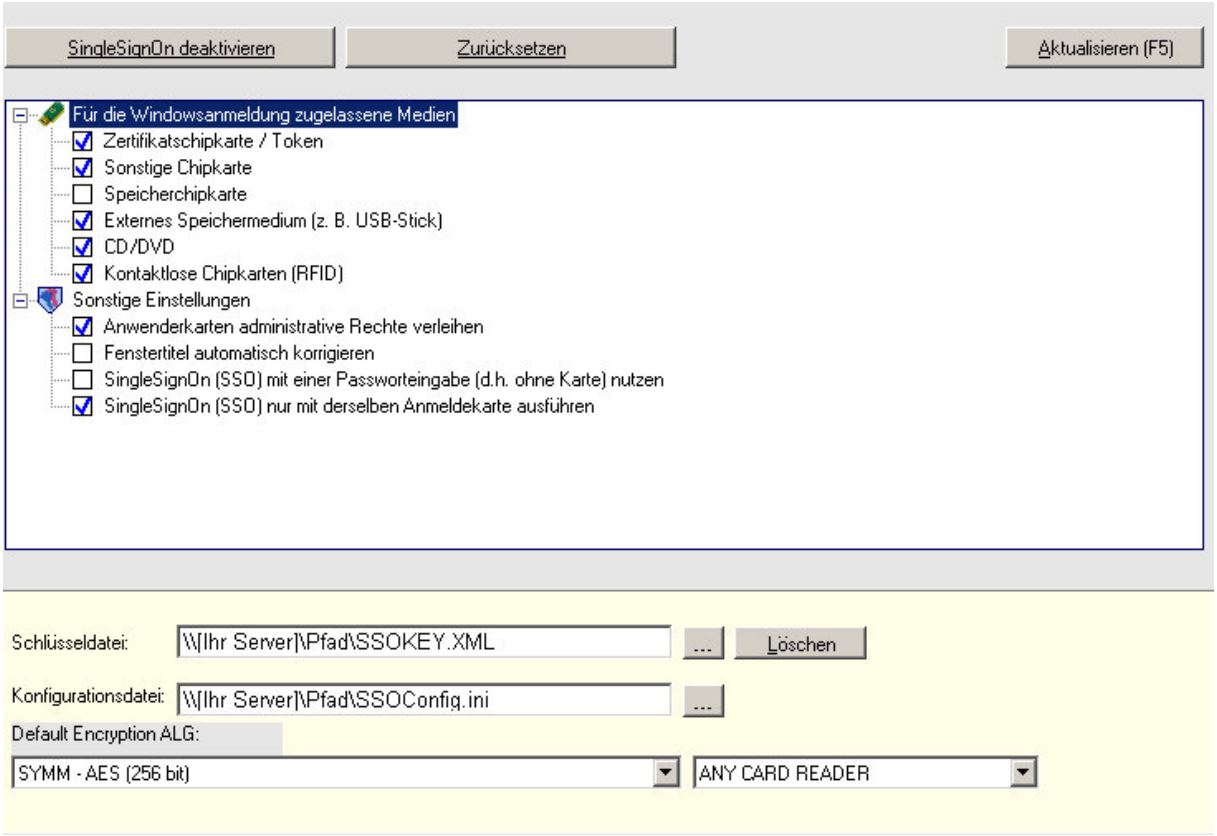
- **Anmeldename:** Benutzername für die Anmeldung (kann frei gelassen werden!)
- **Anmeldekennwort:** Passwort für die Anmeldung
- **Client:** Angabe des Rechnernamen, auf die diese Applikation nur ausgeführt werden darf! (Alle anderen Rechner werden ignoriert!)

2.3.4 SSO Karten



Auf der Seite 'SSO Karten' wird eine Liste mit allen Karten, Konten und angelernten Applikationen angezeigt. Diese können hier individuell aktiviert, deaktiviert (inaktiv) und gesperrt werden. Zudem ist hier das Wechseln der Administratorkarte möglich.

2.3.5 SSO Einstellungen



Auf der Seite 'SSO Einstellungen' wird eine Liste mit möglichen Einstellungen angezeigt. Hier können die zugelassenen Medien, sonstigen Einstellungen, der Verschlüsselungsalgorithmus und der Speicherort der Schlüssel- und Konfigurationsdatei geändert werden. Detaillierte Informationen zu den einzelnen Punkten sind in Kapitel Einstellungen auf Seite 27 aufgeführt.

3 ERWEITERTE EINSTELLUNGEN / ADMINISTRATION

Die Software **abylon SSO** übernimmt viele Einstellungen und erleichtert so die Administration. Jedoch sind gerade im komplexen betrieblichen Umfeld viele spezielle Bedingungen zu berücksichtigen, welche zusätzlich in der Oberfläche und Konfigurationsdateien angepasst werden können. Sollten weitere spezielle Anpassungen oder Hilfen benötigt werden, so treten Sie bitte über das Kontakt-Formular auf unserer Homepage http://www.abylonsoft.de mit uns in Kontakt.

3.1 Applikationen

Unter Applikationen werden die Fenster bezeichnet, in denen Anmeldename und / oder Passwort eingegeben werden kann. Diese werden im Einstellungsdialog auf der Seite 'SSO Applikationen' administriert.

3.1.1 Applikationen anlegen

Bei aktivierter automatischer Erkennung werden Fenster mit Passwortfeldern in der Regel automatisch erkannt. In speziellen Fällen kann das Anlernen auch manuell erfolgen.

Nach dem Drücken des Schalters werden alle geöffneten Fenster in einer Liste angezeigt. Nach Auswahl und Eingabe der entsprechenden Daten wird die Applikation in die Applikationsliste übernommen.

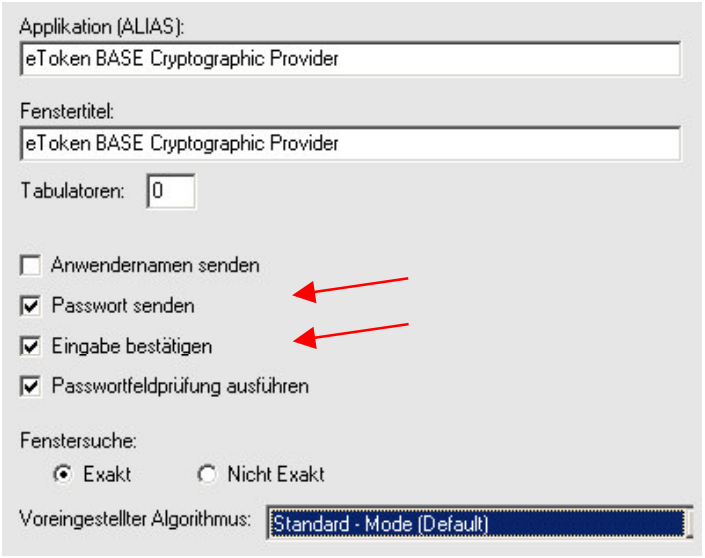
Applikationen können durch entfernen des Häkchens deaktiviert werden, wodurch die Überwachung für diese Applikation nicht mehr erfolgt.

HINWEIS: Ein deaktivierte Applikation wird auch angelegt, wenn bei der automatischen Fenstererkennung der Fragedialog mit 'Nein' bestätigt wird.

Die Software unterscheidet zwischen Applikationen (Fenstern) mit **Passwortfeld**, **Anmeldename und Passwortfeld** und **Passwortwechseldialoge**.

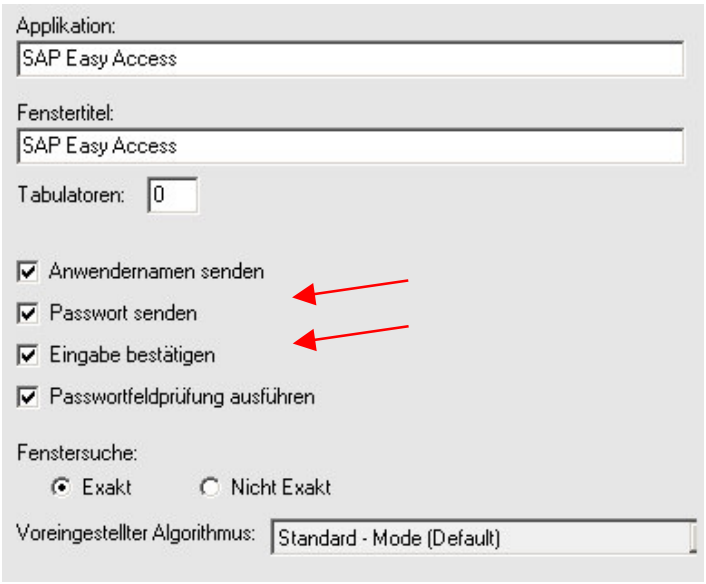
3.1.1.1 Nur Passwortfeld

In diesem Beispiel handelt es sich um die Applikation "eToken BASE Cryptographic Provider", welche den identischen Fenstertitel besitzt und nur einem Passwortfeld anbietet. Nachdem die Software **abylon SSO** das Passwort eingetragen hat, wird noch die Eingabe bestätigt, sodass die Applikation sofort startet.



3.1.1.2 Anmeldename und Passwortfeld

In diesem Beispiel handelt es sich um die Applikation "SAP Easy Access", welche den identischen Fenstertitel besitzt und ein jeweils ein Feld für Anmeldename und Passwort anbietet. Nachdem die Software **abylon SSO** den Anmeldenamen und das Passwort eingetragen hat, wird noch die Eingabe bestätigt, sodass die Applikation sofort startet.



3.1.1.3 Passwortwechseldialoge

Passwortwechseldialoge werden zur Zeit noch nicht in der GUI angezeigt und müssen manuell über die Konfigurationsdatei administriert werden.

Dazu muss folgende Werte definitiv gesetzt werden:

```
CAPTION=[Titel des Fensters]
CHGPASS=[Wert = 1]
WINDOWID=[Eingetragene WindowsID von der zugehörigen Applikation]
```

Weitere Informationen zur Konfigurationsdatei finden sie in Kapitel 3.3.2 auf Seite 28!

3.1.2 Applikationen optimieren

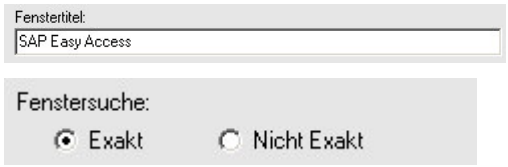
Die folgenden Punkte werden von der Software **abylon SSO** automatisch festgelegt und sollten nur in wirklichen Ausnahmefällen geändert werden!

3.1.2.1 Passwortfeldprüfung ausführen

In der Regel besitzen Passwortfelder eine spezielle Eigenschaft, sodass das Passwort nicht als Klartext, sondern z. B. verdeckt als Sternchen angezeigt wird. Wenn das Eingabefeld diese Eigenschaft besitzen, so ist die Erkennung durch die Software **abylon SSO** sicherer.

Sollte das Passwortfeld diese Eigenschaft nicht besitzen, so muss diese Option deaktiviert werden.

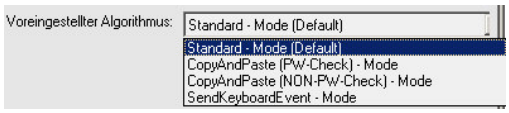
3.1.2.2 Fenstertitel



Anhand des Fenstertitels wird die entsprechende Applikation zugeordnet. Je exakter der Fenstertitel angegeben wird, desto geringer sind Fehlinterpretationen.

HINWEIS: Bei automatischer Fenstererkennung wird der Fenstertitel immer "Exakt" gespeichert!

3.1.2.3 Algorithmus



Die Software **abylon SSO** bietet unterschiedliche Methoden zum Ausfüllen der Anwendernamen und Passwortfelder. In der Regel sollte als Algorithmus der Default-Wert "**Standart – Mode**" ausgewählt sein. Daneben werden noch drei weitere Algorithmen angeboten.

Standart – Mode (Default): Beim Default-Algorithmus probiert die Software **abylon SSO** den optimalsten Weg zum Ausfüllen des Dialoges aus und speichert diesen Wert.

CopyAndPaste (PW-Check) – Mode: Das Passwort und der Anmeldename werden durch Kopieren über die Zwischenablage in die entsprechenden Felder eingefügt. Dabei besitzt dass Passwortfeld die Eigenschaft "Passwortfeld". In diesem Fall ist auch die "Passwortfeldprüfung ausführen" aktiviert.

CopyAndPaste (NON-PW-Check) – Mode: Das Passwort und der Anmeldename werden durch Kopieren über die Zwischenablage in die entsprechenden Felder eingefügt. Dabei besitzt dass Passwortfeld nicht die Eigenschaft Passwortfeld (normales Edit-Feld). In diesem Fall ist auch die "Passwortfeldprüfung ausführen" deaktiviert.

SendKeyboardEvent – Mode: Das Passwort und der Anmeldename werden durch Senden von Keyboard-Events in die entsprechenden Felder eingefügt. Dies ist notwendig, wenn das Kopieren über die Zwischenablage unterbunden wird, wie z. B. beim SAP-Gui-Dialog.

3.1.2.4 Tabulator

Die Anzahl der Tabulatoren besitzt den Defaultwert von "**0**".

Nur wenn das Passwort und/oder der Anmeldename in die falschen Felder eingetragen werden, kann durch setzten der Tabulatoren das Eintragen in die korrekten Felder erzwungen werden. Der angegebene Wert entspricht der Anzahl zu sendender Tabs, bis das 1. Anmeldefeld (z. B. Passwortfeld) erreicht ist.

3.2 Zentrale Schlüsselverwaltung für mehrerer Konten

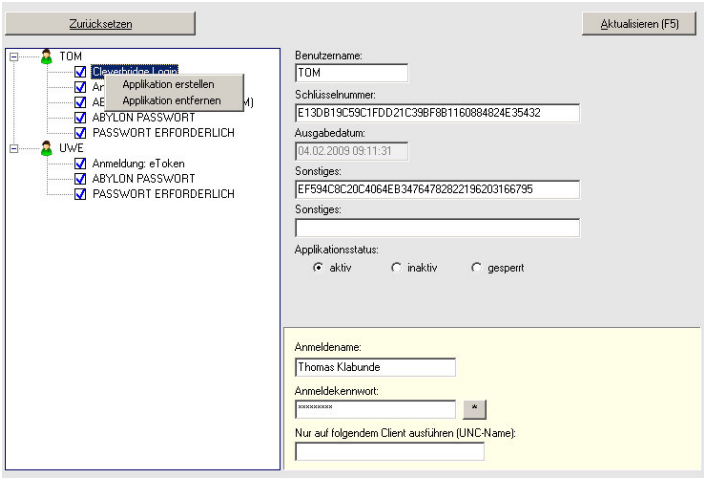
In der Schlüsseldatei werden alle Informationen zu den verwendeten Karten, den Benutzern und der angelernten Applikationen verschlüsselt gespeichert. Durch universellen Aufbau kann diese Datei an einer zentralen Stelle (z. B. Server) gespeichert werden, womit eine einfache Administration auch für mehrere Konten (Anwender) möglich ist.

3.2.1 Konto erstellen

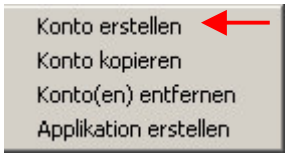
Die folgenden Punkte beschreiben das Vorgehen zum Anlegen eines Kontos!

HINWEIS: Beim 1. Konto muss zunächst die Administratorkarte festgelegt werden!

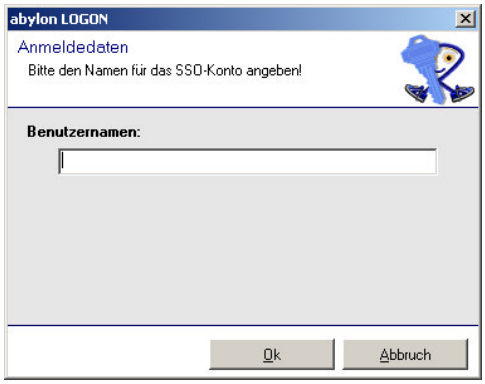
1. Öffnen Sie den Einstellungsdialog und wechseln auf die Seite 'SingleSigOn->SSO Konten'.



2. Wählen Sie im Menü (rechte Maustaste) den Punkt 'Konto erstellen' aus.

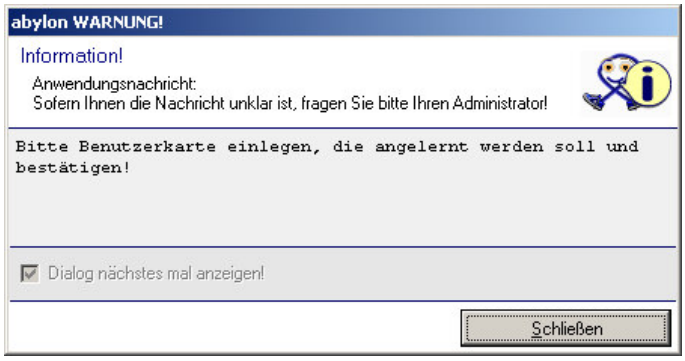


3. Geben Sie im angezeigten Fenster den gewünschten Benutzernamen an.

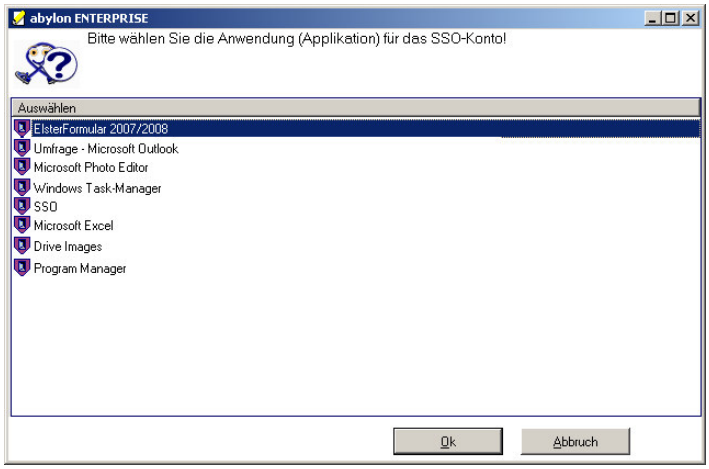


4. Nun werden Sie aufgefordert, die gewünschte Benutzerkarte einzulegen.

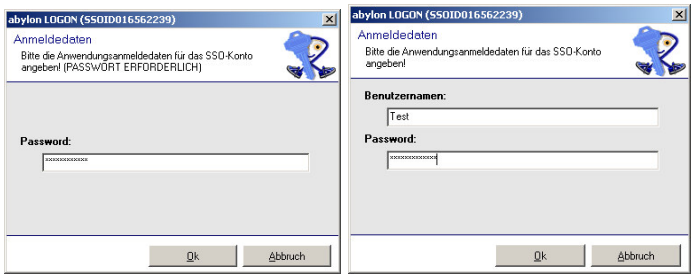
HINWEIS: Wenn die Software mehrere verfügbare Karten findet, wird zusätzlich ein Auswahldialog angezeigt!



5. Wählen Sie nun aus der angezeigten Liste eine Applikation aus, für die eine Anmeldung mit Passwort nötig ist.



6. Zum Abschluss werden Sie noch nach dem zugehörigen Passwort und Anmeldenamen gefragt (Abhängig von der gewählten Applikation).

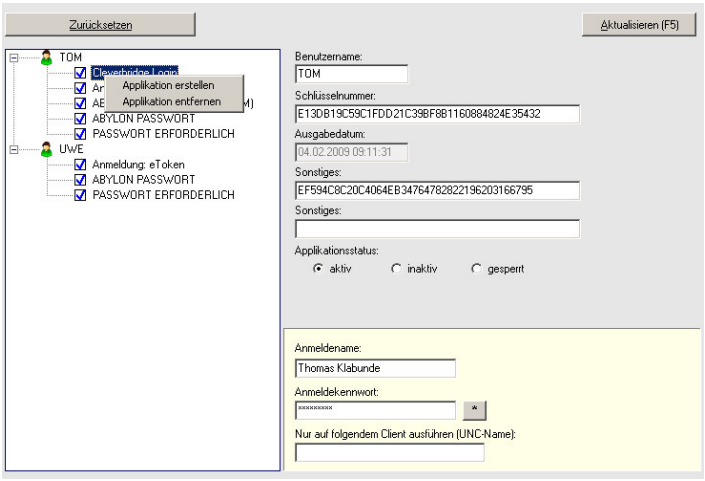


7. Das neue Konto mit der angelernten Applikation wird im Einstellungsdialog angezeigt.

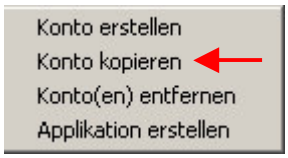
3.2.2 Konto kopieren

Die folgenden Punkte beschreiben das Vorgehen zum Kopieren (Duplizieren) eines bestehen Kontos!

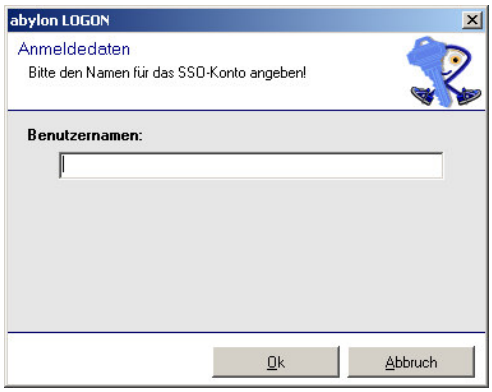
1. Öffnen Sie den Einstellungsdialog, wechseln auf die Seite 'SingleSigOn->SSO Konten' und wählen das zu kopierende Konto aus.



2. Wählen Sie im Menü (rechte Maustaste) den Punkt 'Konto kopieren' aus.

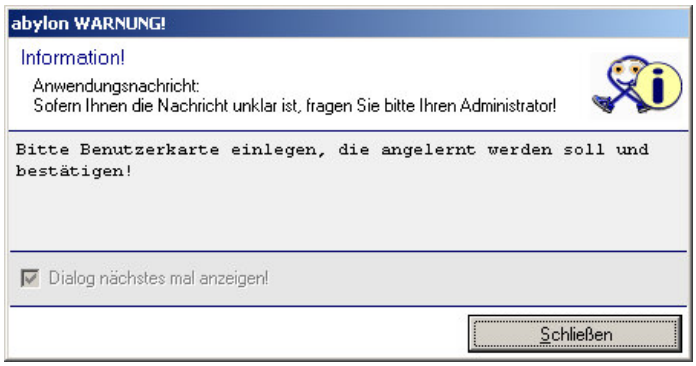


3. Geben Sie im angezeigten Fenster den gewünschten Benutzernamen für das neue Konto an.



4. Nun werden Sie aufgefordert, die gewünschte Benutzerkarte einzulegen.

   HINWEIS: Wenn die Software mehrere verfügbare Karten findet, wird zusätzlich ein Auswahldialog angezeigt!



5. Das neue Konto mit der angelernten Applikation wird im Einstellungsdialog angezeigt.

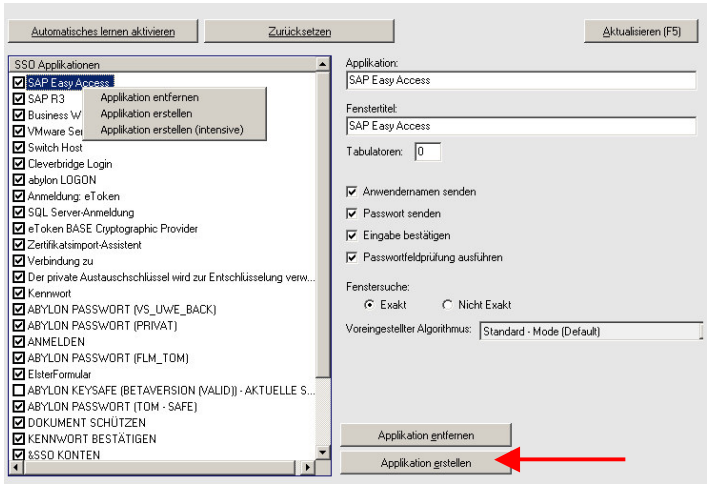
3.2.3 Applikation manuell erstellen

Die folgenden Punkte beschreiben das Vorgehen zum manuellen Erstellen einer Applikation!

HINWEIS: In der Großzahl der Fälle werden auch unbekannte Fenster automatisch erkannt und angelernt!

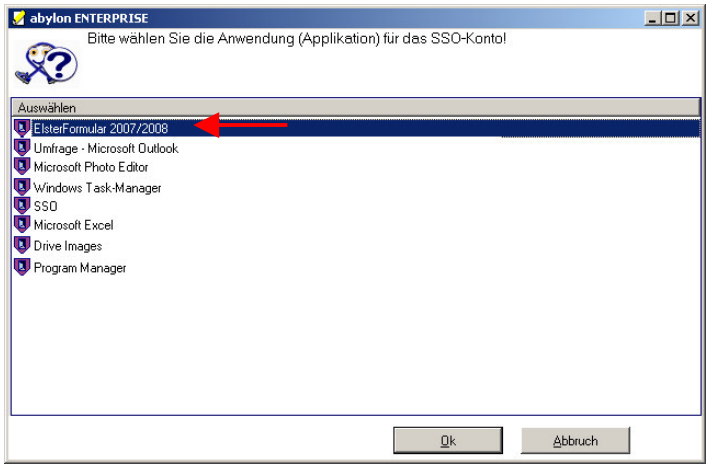
1. Öffnen Sie den Dialog, der eine Passworteingabe erfordert (hier Elster Formular).

2. Öffnen Sie zusätzlich den Einstellungsdialog, wechseln auf die Seite 'SingleSigOn->SSO Applikationen' und drücken den Schalter 'Applikation erstellen'.

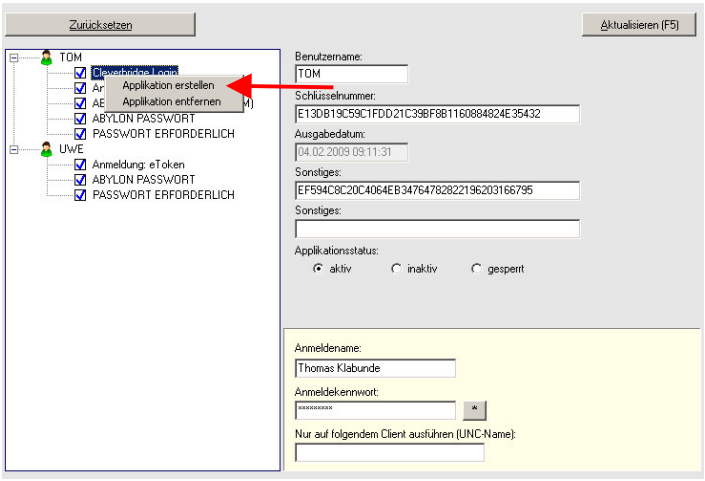


3. Es wird eine Liste mit allen geöffneten Fenstern angezeigt. Wählen Sie die entsprechende Applikation aus und bestätigen mit 'Ja'.

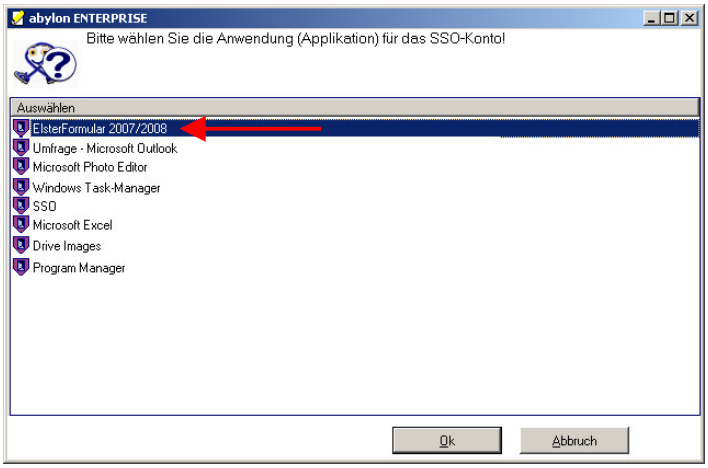
   Im Anschluss wird die Applikation im Einstellungsdialog auf der Seite 'SingleSigOn->SSO Applikationen' angezeigt und kann hier bearbeitet werden.



4. Um die Applikation mit den entsprechenden Anmeldedaten einem Konto zuzuweisen, öffnen Sie im Einstellungsdialog die Seite 'SingleSigOn->SSO Konten' und wählen im Menu den Punkt 'Applikation erstellen'.



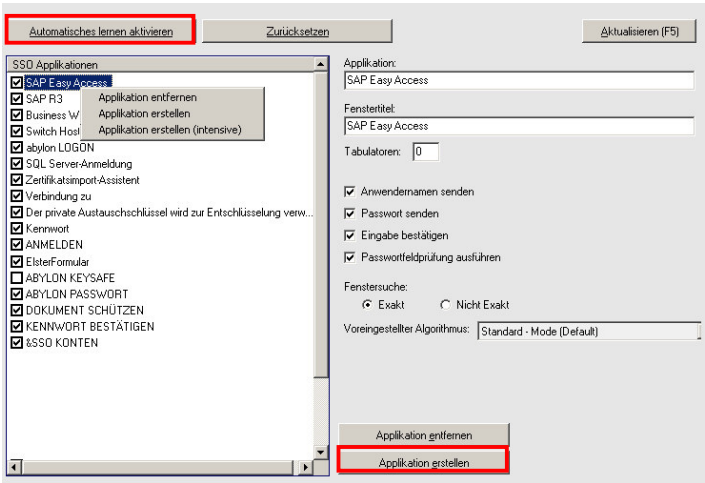
5. Nun können Sie in der Liste der angelegten Applikationen den Eintrag 'ElsterFormular' auswählen und im Anschluss das Passwort festlegen.



3.2.4 Einsatz des SSO am Beispiel von SAP - Software

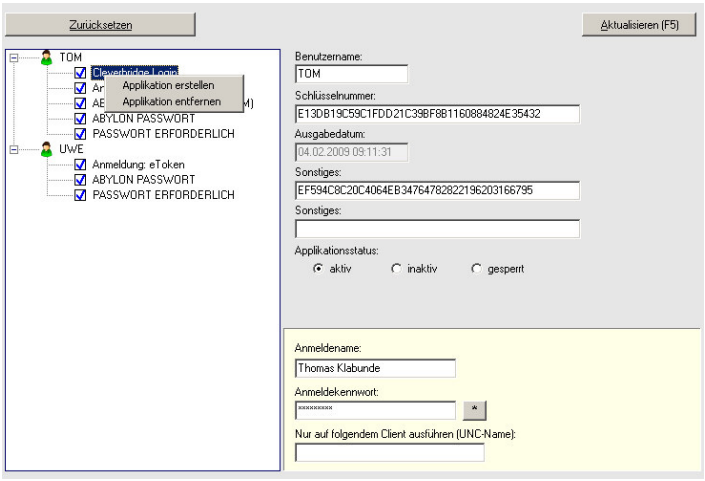
Am Beispiel des SAP Easy Access und der SAP R3 Anmeldung wird die Funktionsweise der Software **abylon SSO** beschrieben.

1. Zunächst müssen die Passwortdialoge angelernt werden. Dies kann manuell auf der Seite 'SingleSigOn->SSO Applikationen' mit dem Schalter 'oder durch das 'Automatische Lernen' erfolgen.



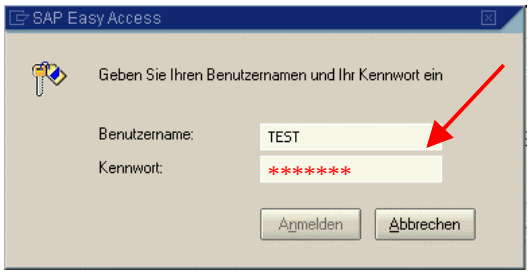
2. Im Einstellungsdialog auf der Seite 'SingleSigOn->SSO Konten' werden die Applikationen durch drücken des Schalter 'Applikation erstellen' angelegt.

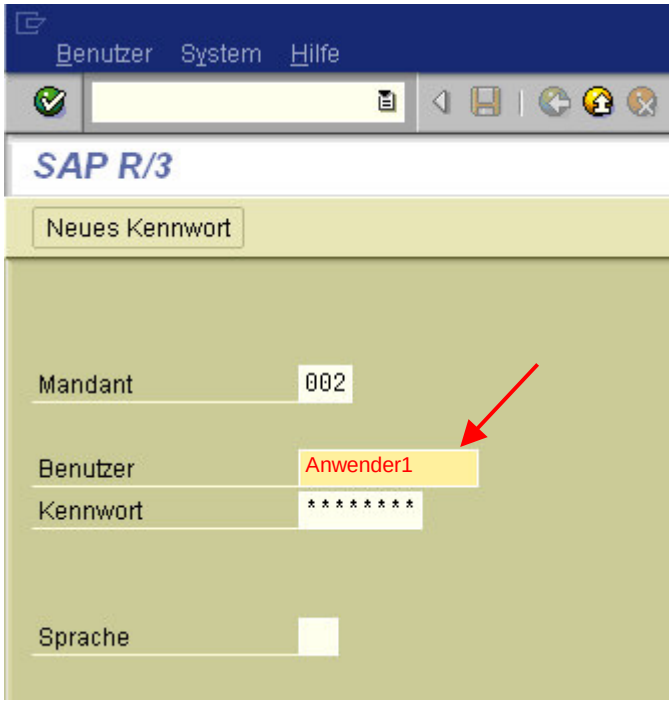
Die Applikationen werden mit den Zugangsdaten verschlüsselt in der XML-Schlüsseldatei gespeichert und stehen in Zukunft nach der Legitimation zur Verfügung.



3. Sobald das Fenster geöffnet wird, erkennt dies die Software **abylon SSO** und trägt den Benutzernamen und das Passwort in die entsprechenden Felder der SAP-Anmeldemasken ein.

Zum Abschluss wird das Anmeldefenster bestätigt und die Applikation geöffnet.





Eintragungen in der INI-Datei für SAP Easy Access und R3:

```
[SAP Easy Access]
CAPTION=SAP Easy Access
APP_CAPTION=
SENDUSER=1
SENDPASS=1
SENDOK=1
```

```
CHGPASS=0
COMPARE_EXACT=1
CHECK_PASSFIELD=1
DONTASKAGAIN=0
USERHEADER=
PASSHEADER=
PASSNEU1HEADER=
PASSNEU2HEADER=
OKHEADER=
SENDTABS=0
ALGORITHM=0
APPLICATION=SAP Easy Access
WINDOWID=1F14AD8306B1368060E42EBB2EE8A569C1167EB7

[SAP R3]
CAPTION=SAP R/3
APP_CAPTION=
SENDUSER=1
SENDPASS=1
SENDOK=1
CHGPASS=0
COMPARE_EXACT=1
CHECK_PASSFIELD=0
DONTASKAGAIN=0
USERHEADER=
PASSHEADER=
PASSNEU1HEADER=
PASSNEU2HEADER=
OKHEADER=
SENDTABS=0
ALGORITHM=4
APPLICATION=SAP R3
WINDOWID=A1691CA45C1F43C4BE46607FDC5BC4482C3417D4
```

3.2.5 Schlüsselkarte, Konto und Applikation sperren

Die Schlüsseldaten können in einer Datei verwaltet werden. Dies ermöglicht dem Administrator eine zentrale Administration, wobei auch einzelne Schlüsselkarten, Konten oder Applikationen gesperrt werden können. Dabei wird unterschieden zwischen:

- **Inaktiv:** Anmeldedaten werden NICHT eingetragen
- **Gesperrt:** Anmeldedaten werden nicht eingetragen und zusätzlich erhält der Anwender eine Nachricht

Im Einstellungsdialog auf der Seite 'SingleSigOn->SSO Karten' kann der Status für

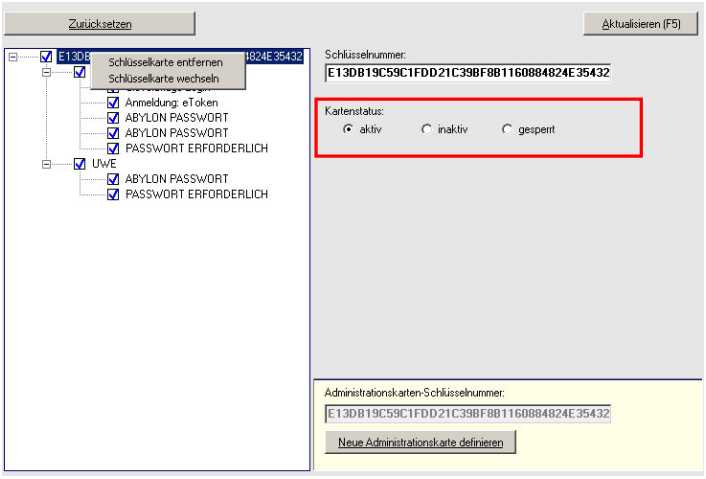
- **Karten**
- **Konten**
- **Applikationen**

festgelegt werden.

Mögliche Werte sind:

- **Aktiv**: Anmeldedaten werden automatisch eingetragen
- **Inaktiv**: Anmeldedaten werden NICHT eingetragen
- **Gesperrt**: Anmeldedaten werden NICHT eingetragen und der Anwender erhält eine Nachricht!

Die Änderungen werden innerhalb von maximal einer Minute auf allen angeschlossenen System gültig.



3.2.6 Schlüsselkarte, Konto und Applikation löschen

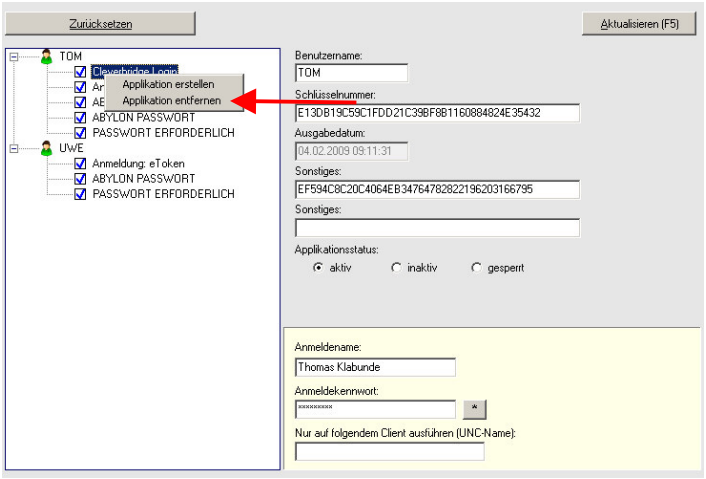
Zum Entfernen von Schlüsselkarten, Konten oder Applikationen gehen Sie wie folgt vor:

Öffnen Sie im Einstellungsdialog die Seite 'SingleSigOn->SSO Karten'. Selektieren Sie hier den zu löschenden Knoten

- **Schlüsselkarte**
- **Konto**
- **Applikation**

aus und wählen den Menüpunkt '... entfernen'.

Alle unterhalb angeordneten Einträge werden dabei mit gelöscht.



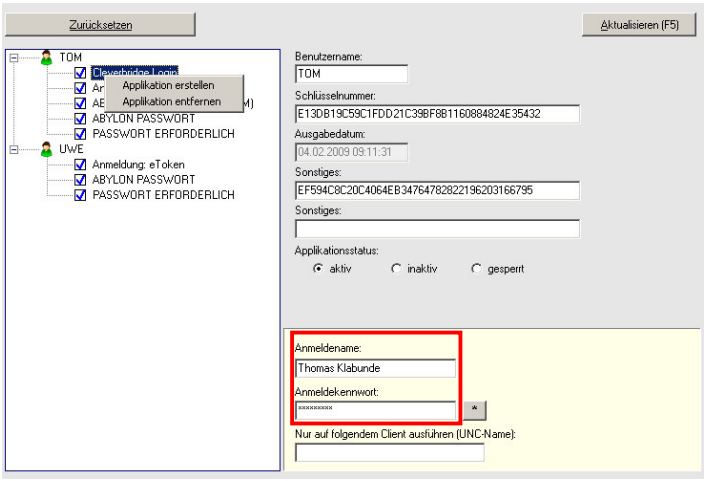
3.2.7 Ein Applikationskonto für mehrere Anwender nutzen

Die Software **abylon SSO** ermöglicht es auch ein Applikationskonto für mehrere Anwender mit unterschiedlichen Karten zu nutzen. Wenn das Passwort in einem Konto geändert wird, so ist dies umgehend für alle zugehörigen Konten gültig.

Im Einstellungsdialog auf der Seite 'SingleSigOn->SSO Konten' muss folgende Änderungen vorgenommen werden:

Ändern Sie bei den zusammengehörigen Applikationen den Anmeldenamen und das Anmeldekennwort so, dass diese identisch sind. Der Anmeldenamen muss auch übereinstimmen, wenn dieses für die Anmeldung nicht erforderlich ist.

HINWEIS: Dies kann auch direkt beim Anlegen der Applikationen berücksichtig werden!

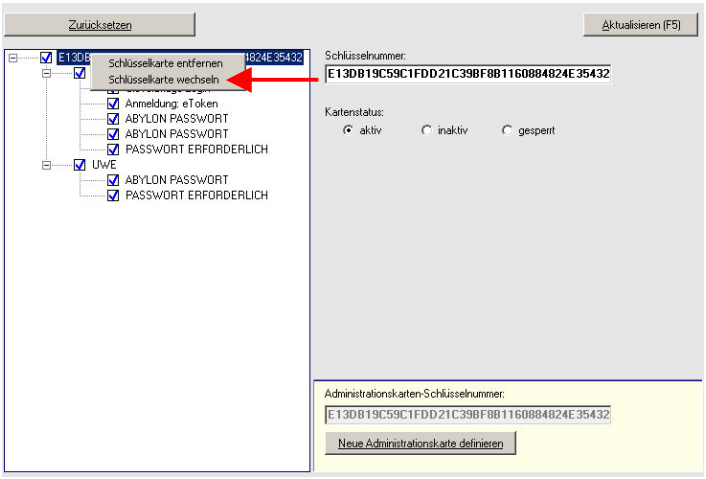


3.2.8 Schlüsselkarte wechseln (z. B. bei Verlust)

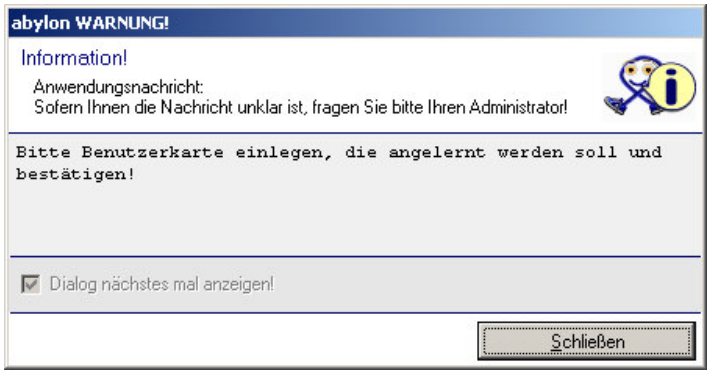
Beispielsweise bei Verlust einer Schlüsselkarte kann es notwendig sein, die Berechtigungen gegen eine neue Schlüsselkarte zu wechseln.

HINWEIS: Voraussetzung zum Wechseln der Schlüsselkarte ist das Vorhandensein der Administratorkarte oder der zu wechselnden Vorgängerkarte!

1. Öffnen Sie den Einstellungsdialog, wechseln auf die Seite 'SingleSigOn->SSO Karten' und wählen die zu wechselnde Schlüsselkarte aus. Im Menü der rechten Maustaste finden Sie den Punkt 'Schlüsselkarte wechseln!



2. Sie werden nun aufgefordert die neue Benutzerkarte einzulegen. Sofern mehrere Karten zu Verfügung stehen, werden diese in einer Auswahlliste angezeigt.

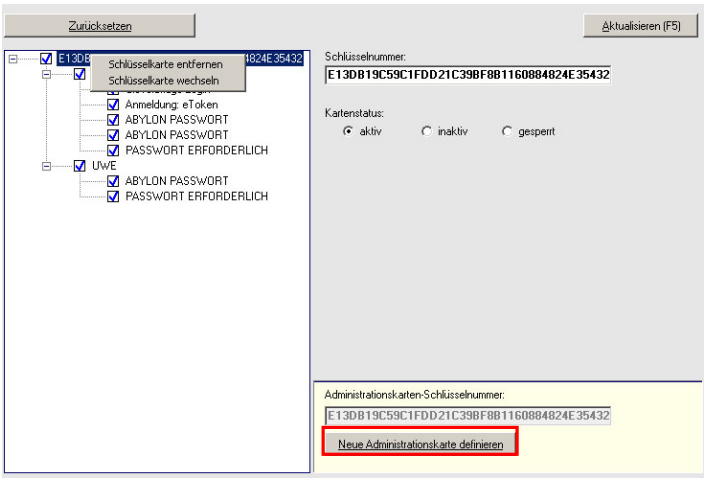


3.2.9 Administratorkarte wechseln

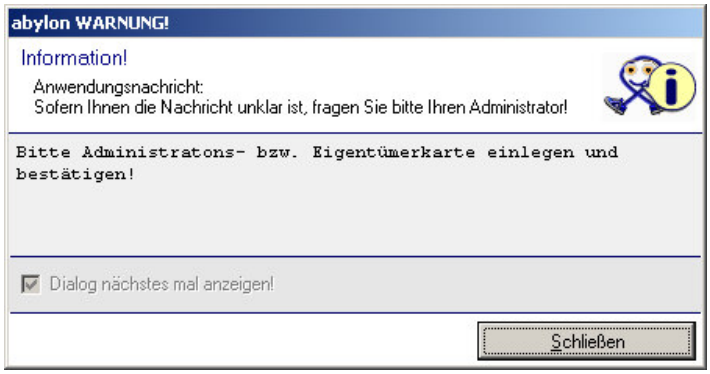
Zum Wechseln der Administratorkarte gehen Sie wie folgt vor:

1. Öffnen Sie den Einstellungsdialog, wechseln auf die Seite 'SingleSigOn->SSO Karten' und drücken den Schalter 'Neue Administratorkarte definieren!

   HINWEIS: Dieses Feld wird nur bei eingelegter Administratorkarte sichtbar!



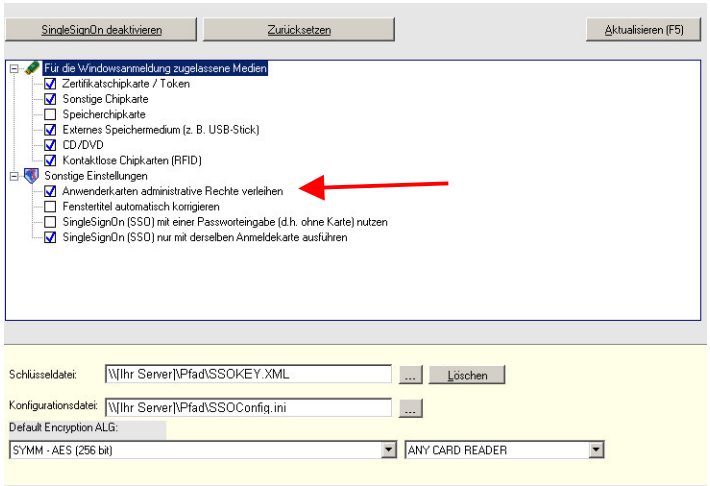
2. Sie werden nun aufgefordert die neue Administratorkarte einzulegen. Sofern mehrere Karten zu Verfügung stehen, werden diese in einer Auswahlliste angezeigt.



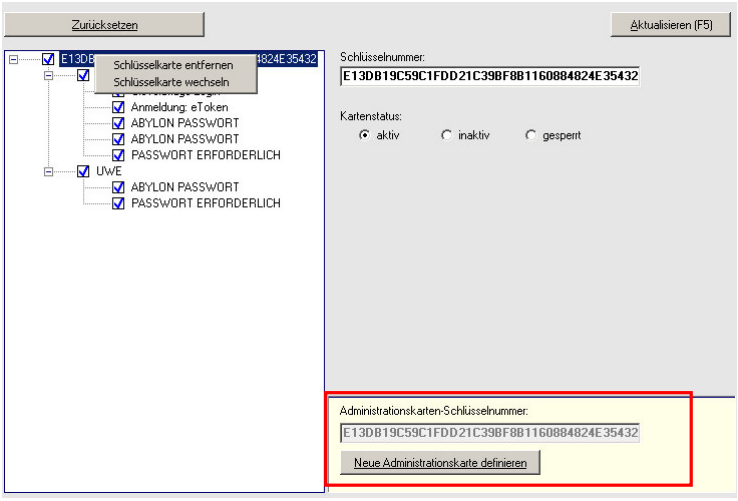
Vorgehen bei nicht vorhandener Administratorkarte (z. B. Verlust):

HINWEIS: Um bei nicht vorhandener Administratorkarte diese neu zu definieren, benötigen Sie **lokale Administratorrechte** auf dem Rechner!

1. Öffnen Sie den Einstellungsdialog, wechseln auf die Seite 'SingleSigOn->SSO Einstellungen' und aktivieren den Punkt 'Anwender administrative Rechte verleihen'!

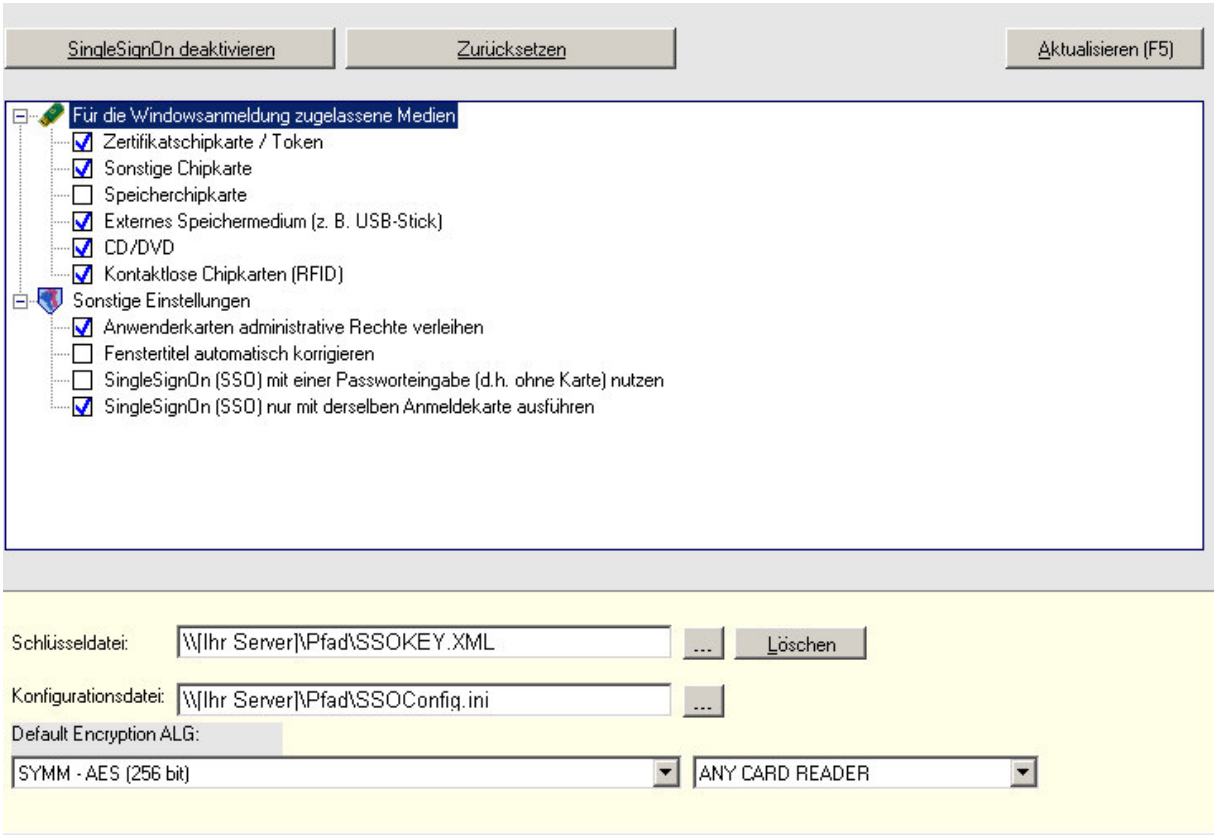


2. Hierdurch erhält der lokale Administrator die Möglichkeit auf der Seite 'SingleSigOn->SSO Karten' die Administratorkarte neu zu definieren!



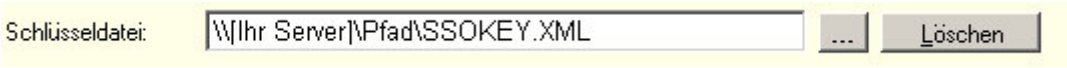
3.3 Einstellungen

In den Einstellungen können verschiedene Optionen gesetzt werden.



3.3.1 Schlüsseldatei

In der Schlüsseldatei werden die Anwender- und Kontendaten verschlüsselt gespeichert und verwaltet. Diese wird automatisch vom Programm angelegt. Die Schlüsseldatei wird im XML - Format angelegt und kann im Einstellungsdialog auf der Seite 'SSO Einstellungen' administriert werden.



Die Schlüsseldatei kann auf einzelnen PCs oder auch zentral im Netzwerk liegen. Von Vorteil ist ein gemeinsamer Speicherort für Schlüssel- und Konfigurationsdatei im Netzwerk mit entsprechender NTFS – Berechtigung und Freigabe.

3.3.1.1 Verschlüsselung

Vor dem Anlegen der Schlüsseldatei werden Sie nach dem Verschlüsselungsalgorithmus gefragt, mit dem die Schlüsseldatei verschlüsselt wird. Mögliche Werte siehe Kapitel Verschlüsselungsalgorithmus und Kartenleser auf Seite 30.

3.3.1.2 Löschen

Über den Schalter 'Löschen' kann die Schlüsseldatei komplett zurückgesetzt werden!

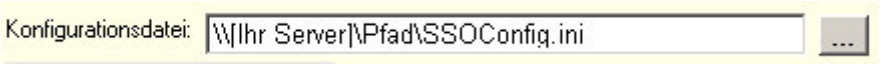
3.3.1.3 Aufbau

Die Schlüsseldatei enthält für jeden Anwenden einen Abschnitt mit seinen verschlüsselten Anmeldedaten.

Bezeichnung	Wert	Beschreibung
<LS_KEY_SET>	-	Verschlüsselungsinformationen
<K_USEAGE>	KEYID	
<LS_SYMM_METHODE>	[Zahl]	Verschlüsselungsalgorithmus
<[Anmeldename]>	[Anmeldename]	Name des Anwenders
<K_ENTRIES>	[Zahl]	Anzahl der Einträge
<K_DATASIZE>	[Zahl]	Größe des Datensatzes
<N0>	Verschlüsselter Text	
<[Anmeldename]_SESS>	-	
<LS_OTHER_SET>	-	
<LS_TEXT>	Verschlüsselte Einträge und Texte	Enthält die verschlüsselten Schlüsseldaten eines Anwenders

3.3.2 Konfigurationsdatei

Die Konfigurationsdatei wird im INI-Format angelegt und kann im Einstellungsdialog auf der Seite auf 'SSO Einstellungen' administriert werden. Am günstigsten ist ein gemeinsamer Speicherort für Schlüssel- und Konfigurationsdatei im Netzwerk mit entsprechender NTFS – Berechtigung und Freigabe am günstigsten.



Für jedes überwachte Fenster wird ein entsprechender Eintrag in der Konfigurationsdatei angelegt werden.

3.3.2.1 Beispiel eines Eintrags

```
[SAP Easy Access]
CAPTION=SAP Easy Access
COMPARE_EXACT=0
CHGPASS=0
SENDUSER=1
```

```
SENDPASS=1
SENDOK=1
USERHEADER=
PASSHEADER=
PASSNEU1HEADER=
PASSNEU2HEADER=
OKHEADER=
WINDOWTAG=
CHECK_PASSFIELD=
WINDOWID=1F14AD8306B1368060E42EBB2EE8A569C1167EB7
APPLICATION=SAP Easy Access
DONTASKAGAIN=
```

3.3.2.2 Beschreibung der Werte

Bezeichnung	Eintragart	Wert	Beschreibung
[Name]		Name des Eintrags	Individueller Name für den Eintrag
CAPTION		Caption (Fenstertitel)	Caption (Fenstertitel) des Anmeldedialoges
COMPARE_EXACT	Manuell	0 oder 1	Vergleich des Caption (Fenstertitels) mit dem eingetragenen Caption: 0 = Ungefähre Übereinstimmung (Caption muss enthalten sein) 1 = Exakte Übereinstimmung (Caption muss genau übereinstimmen)
CHGPASS	Manuell	0 oder 1	ChangePasswort (Passwort ändern) 0 = Normaler Anmeldedialog 1 = Passwortändern Dialog
SENDUSER	Manuell	0 oder 1	Username (Anmeldename) senden 0 = Nicht senden 1 = Senden
SENDPASS	Manuell	0 oder 1	Passwort senden 0 = Nicht senden 1 = Senden
SENDOK	Manuell	0 oder 1	Bestätigung senden (Entspricht OK-Button drücken) 0 = Nicht senden 1 = Senden
USERHEADER	Manuell (optional)	Bezeichnung	Bezeichnung (Titel) des Anmeldenamen-Feldes
PASSHEADER	Manuell (optional)	Bezeichnung	Bezeichnung (Titel) des Passwort-Feldes
PASSNEU1HEADER	Manuell (optional)	Bezeichnung	Bezeichnung (Titel) des 2. Passwort Neu-Feldes
PASSNEU2HEADER	Manuell (optional)	Bezeichnung	Bezeichnung (Titel) des 2. Passwort Neu-Feldes
OKHEADER	Manuell (optional)	Bezeichnung	Bezeichnung (Titel) des OK-Schalters
WINDOWTAG	Manuell (optional)	Schlüsselwort	Unterscheider bei gleichen Anmeldefenstern für unterschiedliche Anmeldedaten. Die Software sucht nach dem angegebenen Schlüsselwort in den Fenstertexten (z. B. Fenstertitel) Hinweis Zur Unterscheidung muss der Name des Eintrags mit #Zahl# durchnummeriert werden!

DONTASKAGAIN	Automatisch (optional)	0 oder 1	Frage zum Neuanlernen des Fensters 0 = Keine Frage-Dialog (Fenster wird nicht angelernt) 1 = Anzeige des Fragendialog (Fenster kann angelernt werden)
CHECK_PASSFIELD	Manuell (optional)	0	Wenn es sich beim Feld zur Eingabe des Passwort nicht um ein kein Passwortfeld mit speziellen API-Eigenschaften handelt, dann muss diese Wert auf 0 gesetzt werden! HINWEIS Dies ist bei der SAP-Anmeldung unbedingt erforderlich!
WINDOWID	Automatisch / Manuell	ID	Eindeutiger Kennzeichenwert für die Zuordnung und Beschreibung, welche bei Anmeldefenstern (CHGPASS = 0) automatisch vom Programm zugewiesen wird. Für die Zuordnung von Passwortändern Fenstern (CHGPASS = 1) muss die zugehörige ID manuell eingefügt werden
APPLICATION	Automatisch / Manuell	Bezeichnung der Anwendung	Freie definierbare Bezeichnung für die Anwendung, welche in der GUI angezeigt wird und für die Zuordnung der Anwender dient. Hinweis Eine nachträgliche Änderung führt zur Unterbrechung der Anwenderzuordnung!

3.3.3 Verschlüsselungsalgorithmus und Kartenleser

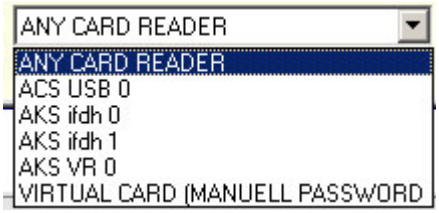
3.3.3.1 Default Encryption ALG

Voreinstellung für den Verschlüsselungsalgorithmus zum Verschlüsseln der Schlüsseldatei mit folgenden Werten:

- **SYMM-AES**: Passwortbasierte symmetrische Verschlüsselung mit dem AES-Algorithmus (Schlüssellänge 256 Bit).
- **SYMM-Blowfish**: Passwortbasierte symmetrische Verschlüsselung mit dem Blowfish-Algorithmus (Schlüssellänge 448 Bit).
- **SYMM-AES & Blowfish**: Passwortbasierte symmetrische Verschlüsselung mit dem AES-Algorithmus (Schlüssellänge 256 Bit) und anschließend mit dem Blowfish-Algorithmus (Schlüssellänge 448 Bit).
- **HYBRID-AES**: Zertifikatsbasierte asymmetrische Schlüsselverwaltung nach dem PKCS-Verfahren von RSA und interne Verschlüsslung der Daten mit dem AES-Algorithmus (Schlüssellänge 256 Bit).
- **HYBRID-Blowfish**: Zertifikatsbasierte asymmetrische Schlüsselverwaltung nach dem PKCS-Verfahren von RSA und interne Verschlüsslung der Daten mit dem Blowfish-Algorithmus (Schlüssellänge 448 Bit).
- **HYBRID-AES & Blowfish**: Zertifikatsbasierte asymmetrische Schlüsselverwaltung nach dem PKCS-Verfahren von RSA und interne Verschlüsslung der Daten mit dem AES-Algorithmus (Schlüssellänge 256 Bit) und anschließend mit dem Blowfish-Algorithmus (Schlüssellänge 448 Bit).

3.3.3.2 Kartenleser

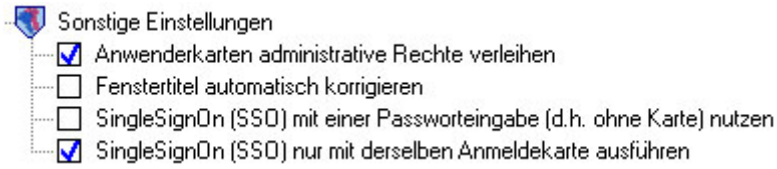
Hier legen Sie fest, ob Alle oder nur ein einzelner Kartenleser zugelassen ist.



Bei 'ANY CARD READER' werden alle angeschlossenen Kartenleser unterstützt (Voreinstellung).

Bei 'VIRTUAL CARD' ist nur die Eingabe eines Passwortes über die Tastatur erlaubt.

3.3.4 Sonstige Einstellungen



3.3.4.1 Weitere Einstellungen sind

Anwenderkarte administrative Rechte verleihen	Bei Aktivierung haben auch Anwender ohne administrative Rechte die Möglichkeit Einstellungen vorzunehmen.
Fenstertitel automatisch korrigieren	Bei Aktivierung werden in der Konfigurationsdatei die Fenstertitel entsprechend des gefundenen Namen angepasst.
Single Sign-On (SSO) mit einer Passworteingabe (d. h. ohne Karte) benutzen	Bei Aktivierung kann das Signle Sign-On auch ohne Karte nur mit Passworteingabe über die Tastatur verwendet werden.
Single Sign-On (SSO) nur mit desselben Anmeldekarte ausführen	Bei Aktivierung kann das Single Sign-On nur mit der Karte gestartet werden, die auch für die Windowsanmeldung mit **abylon LOGON** verwendet wurde.

3.3.5 Das Tray-Icon

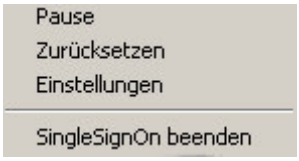
Sobald die Software **abylon SSS** gestartet ist, wird neben der Uhr in der Task-Leiste ein Tray-Icon angezeigt.

 Software ist gestartet und hat eine gültige Anwenderkarte gefunden!

 Software ist gestartet, es liegt jedoch keine Anwenderkarte vor!

 Software steht auf Pause, sodass keine Anmeldedaten eingetragen werden!

Über das Tray-Icon kann folgendes Menü aufgerufen werden:



Pause: Setzt den Signle SigOn Funktionalität auf Pause

Zurücksetzen: Reinitialisiert die Anwendung bei Problemen

Einstellungen: Öffnet den Einstellungsdialog

Single Sig-On beenden: Beendet das Programm komplett

4 ÄNDERUNGSCHRONIK

Version	Datum	Autor	Kommentar
1.0	12.11.2008	Thomas Klabunde	Dokument neu erstellt
1.1	04.12.2008	Uwe Velten	Dokument ergänzt
1.2	09.03.2009	Thomas Klabunde	Dokument überarbeitet