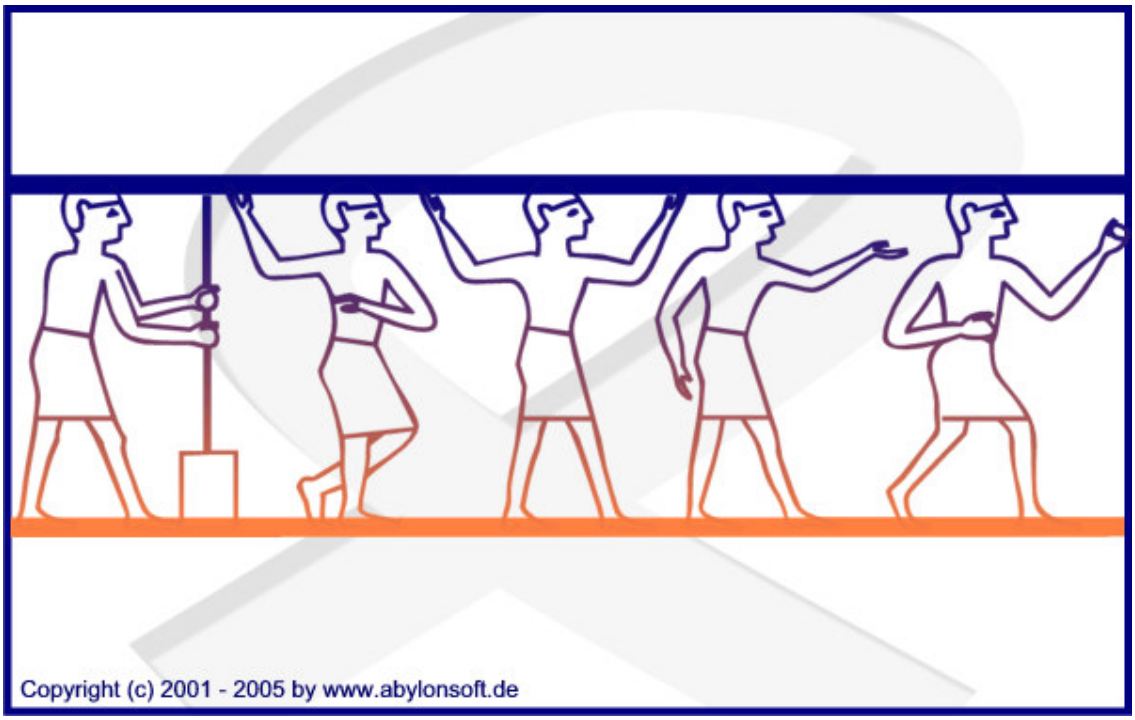
# WITHEPAPER ABYLON LOGON

## ABYLONSOFT – DR. KLABUNDE GBR




### Softwareentwicklung, Beratung und Verkauf von IT-Sicherheitssoftware

### Revision 1.00.1

abylonsoft - Dr. Thomas Klabunde GbR
Amselweg 18
D-55442 Stromberg
Tel.: +49-(0)-6724-602759-0
Fax.: +49-(0)-6724-602759-0
Email: mail@abylonsoft.de
Homepage: http://www.abylonsoft.de

Stand: 14.05.2005

# HISTORIE

| Version | Datum | Kommentar |
|---|---|---|
| 1.00.1 | 21.06.2005 | Dokument neu erstellt |

# INHALTSVERZEICHNIS

*1 Einleitung ..... 4*

*2 Softwaretechnologien und Features ..... 4*

**2.1 Funktionsweise ..... 4**

2.1.1 Funktionsweise mit Zertifikatschipkarte oder USB-Token ..... 4

2.1.2 Funktionsweise mit EC-, HBCI-, KV- und sonstigen Chipkarten ..... 5

**2.2 Bedienung ..... 5**

2.2.1 Installation ..... 5

2.2.2 Konto erstellen ..... 6

2.2.3 Im Einsatz ..... 6

2.2.4 Verwendung von Zertifikatschipkarten oder USB-Token ..... 7

2.2.5 Die Optionen ..... 8

*3 Die Technik ..... 10*

*4 Hinweise ..... 11*

**4.1 Systemvoraussetzungen ..... 11**

4.1.1 Hard- und Software ..... 11

4.1.2 Unterstützte Standards: ..... 12

4.1.3 Technische Informationen: ..... 12

**4.2 Unterstütze Chipkarten ..... 12**

4.2.1 Zertifikatschipkarten / USB-Token ..... 12

4.2.2 EC-/HBCI-/Fotokarten ..... 12

4.2.3 Speicherchipkarten (z. B. Krankenversichertenkarten) ..... 13

4.2.4 Sonstige Chipkarten ..... 13

**4.3 Weitere Dokumente und FAQs ..... 13**

# 1 EINLEITUNG

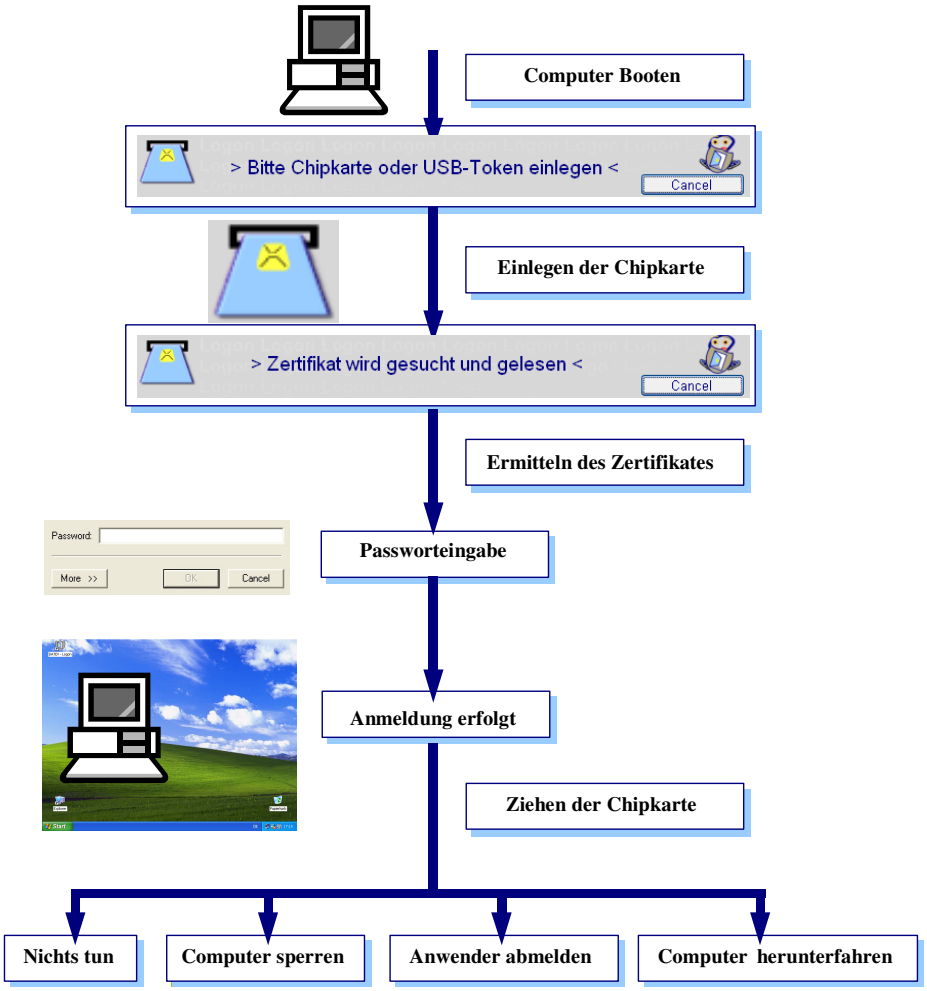
Dieses Whitepaper beschreibt anhand von Anwendungsbeispielen und Schaubildern die Funktionsweise und Technologie des Softwareproduktes **abylon LOGON**.

# 2 SOFTWARETECHNOLOGIEN UND FEATURES

## 2.1 Funktionsweise

### 2.1.1 Funktionsweise mit Zertifikatschipkarte oder USB-Token

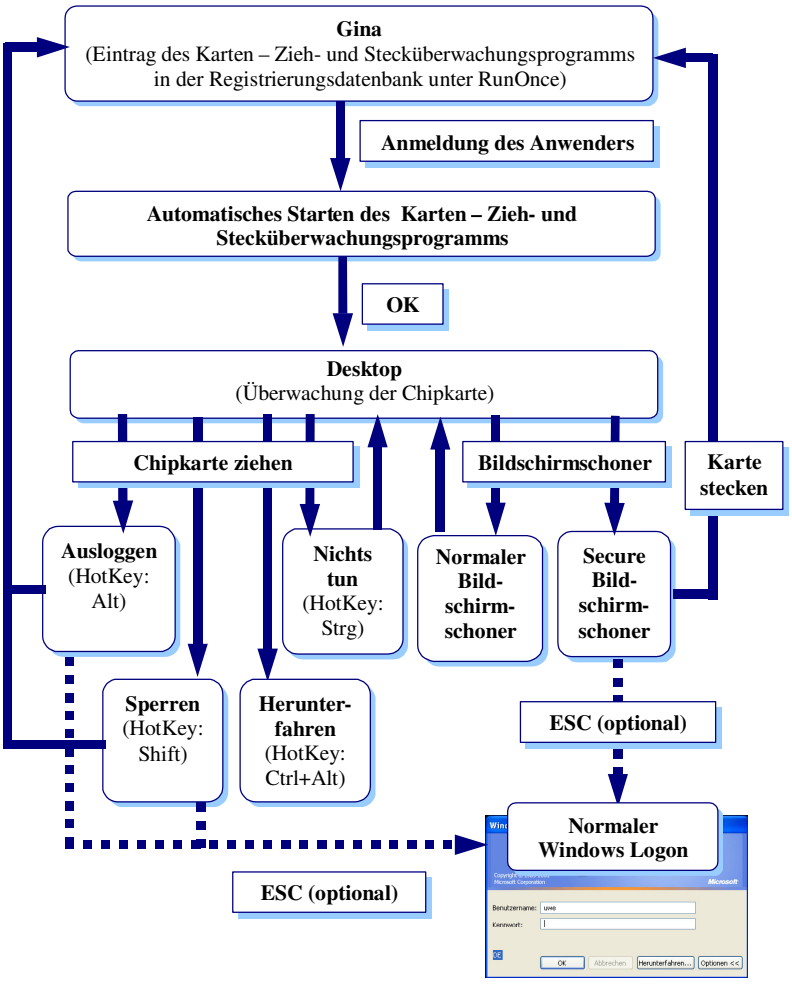
**abylon LOGON** ersetzt den Anmeldevorgang unter Windows NT, 2000 oder XP und ermöglicht somit die einfache Anmeldung **zertifikatsbasierter Chipkarte** oder z. B. den **USB-Token** von Aladdin (eToken). Das Zertifikat auf der Chipkarte oder den USB-Token wird zur Verschlüsselung der Anmeldedaten verwendet.



### 2.1.2 Funktionsweise mit EC-, HBCI-, KV- und sonstigen Chipkarten

**abylon LOGON** ersetzt den Anmeldevorgang unter Windows NT, 2000 oder XP und ermöglicht somit die einfache Anmeldung mit Ihrer **Chipkarte**. Abweichend von der zertifikatsbasierten Anmeldung werden spezifischen Einträgen der Karte gelesen und darüber eine Quersumme (Hashwert) gebildet. Dieser Quersumme dient als Basis für die Verschlüsselung der Anmeldedaten.

## 2.2 Bedienung




### 2.2.1 Installation

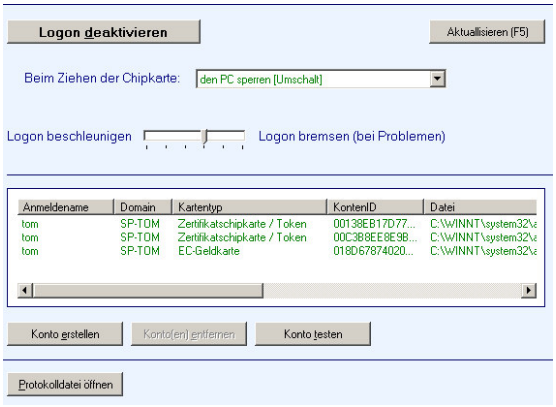
**abylonsoft** liefet seine Software **abylon LOGON** mit einer Installations- und Deinstallationsroutine aus. Nach Erfolgreicher Installation kann der Anwender im Einstellungsdialog von **abylon LOGON** den chipkartenbasierten Anmeldevorgang aktivieren, spezielle Einstellungen vornehmen und einzelne Konten erstellen.

## 2.2.2 Konto erstellen

Im Einstellungsdialog und während der Anmeldung können neue Konten angelegt werden.

Dazu gehen Sie wie folgt vor:

1. Öffnen der Einstellungsdialog
2. Button ‚**Konto erstellen**'




3. Einlegen der Chipkarte in Ihren Chipkartenleser


4. Angabe der Anmeldedaten und bestätigen mit ‚**Ok'**
5. Die Anmeldedaten werden geprüft und bei Erfolg wird ein Konto auf dem Rechner angelegt.

   HINWEIS Dieses Konto befindet sich im Unterverzeichnis ‚DATA' des Programmverzeichnisses und können von hier auf weitere Rechner verteilt werden.


## 2.2.3 Im Einsatz

Nachdem ein Konto erfolgreich eingerichtet wurde, reagiert der Rechner auf das Ziehen der Chipkarte. Dabei kann in den Einstellungen festgelegt werden, was beim Ziehen der Chipkarte erfolgt:

1. Nichts tun [Strg]
2. PC sperren [Umschalt]
3. PC abmelden [Alt]
4. PC herunterfahren [Strg + Alt]

Die einzelnen Reaktionen können auch durch Drücken von entsprechende Hotkey während dem Ziehen der Chipkarte erzwungen werden (eckige Klammern).

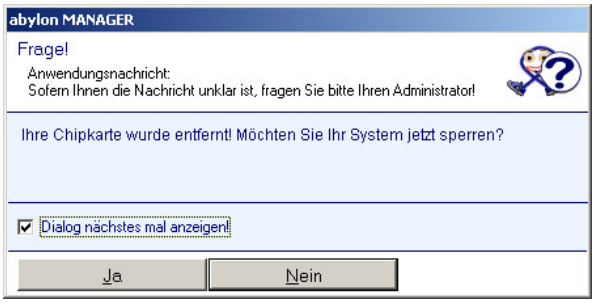
Beispiel: Sperren des Rechners!

1. Ziehen der Chipkarte
2. Anzeige des Frage-Dialoges

   ‚**Ja**' -> Computer wird gesperrt

   ‚**Nein**' -> Computer wird nicht gesperrt

   HINWEIS Die Anzeige dieses Dialoges kann unterbunden werden!
3. Der Rechner wird wieder freigeschaltet, nachdem die entsprechende Chipkarte erneut in des Kartenleser gesteckt wird.

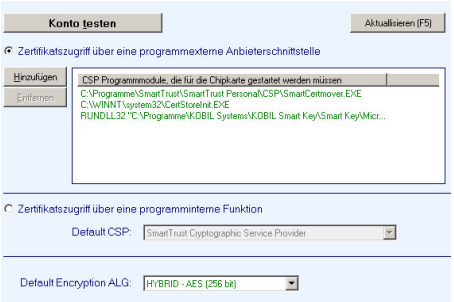



## 2.2.4 Verwendung von Zertifikatschipkarten oder USB-Token

Für den Einsatz von personalisierten Zertifikatschipkarten oder USB-Token wird eine CSP (Crypto Service Provider) des entsprechenden Anbieter benötigt.

In den Einstellungen werden zwei Möglichkeiten angeboten, um auf die Zertifikate der Chipkarte zugreifen zu können.

Einstellungsdialog für den Zertifikatszugriff:




INFO Soweit möglich bietet **abylonsoft** bei Problemen oder Fragen zum Zertifikatszugriff technische Hilfe an.

### *2.2.4.1 Zertifikatszugriff über eine programmexterne Anbieterschnittstelle*

Viele CSPs (Crypto Service Provider) bieten ein Programmmodul an, mit dem ein Link vom Zertifikat auf der Chipkarte oder dem USB-Token in der Windows Zertifikatsdatenbank eingetragen wird. Dies ist erforderlich, damit mit dieser Software auf das Zertifikat

zugegriffen werden kann. Bei diesen Programmmodulen kann es sich um eine EXE- oder eine DLL-Datei handeln.

Zahlreiche dieser Programmmodule werden von unserer Software erkannt und automatisch in der Liste eingetragen. Sollte dies nicht der Fall sein, so kann das entsprechende Modul auch manuell hinzufügt werden.

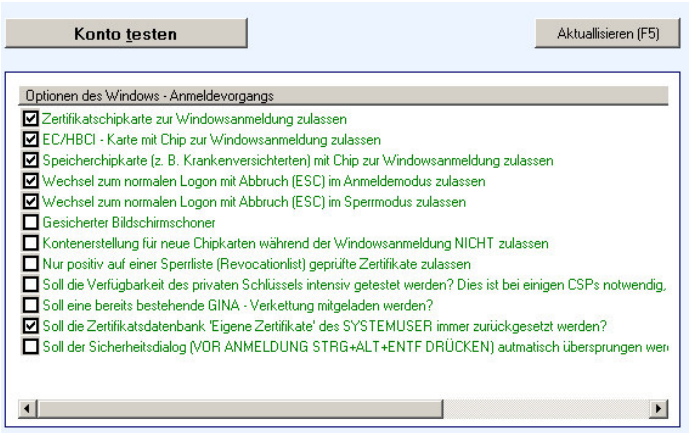
HINWEIS Um die entsprechenden Dateien in Erfahrung zu bringen, lesen Sie bitte die Anleitung Ihrer Chipkarten- oder Ihres Chipkartenlesers, bzw. wenden sich an deren Hersteller.

#### *2.2.4.2 Zertifikatszugriff über eine programminterne Funktion*

Alternativ bietet die Software auch die Möglichkeit eines direkten Zertifikatszugriffes an. Dazu muss im Pulldown-Menu der zu Ihrer Chipkarte oder dem USB-Token gehörenden CSP ausgewählt werden. Dieser CSP muss dafür korrekt in der Registry eingetragen sein und die entsprechenden Schnittstellen anbieten.

HINWEIS In der Regel ist der zu Ihrer Chipkarte oder dem USB-Token passende CSP am Namen zu erkennen. Sollte dies nicht der Fall sein, so lesen Sie bitte die Anleitung oder wenden sich an den Hersteller.

### 2.2.5 Die Optionen




1. **Zertifikatschipkarte zur Windowsanmeldung zulassen**

   Es werden beim Anmeldevorgang zertifikatsbasierte Chipkarten (z. B. vom Trustcenter) akzeptiert. Hierzu gehört beispielsweise auch der eToken von Aladdin.

2. **EC-/HBCI-Karte mit Chip zur Windowsanmeldung zulassen**

   Es werden beim Anmeldevorgang 'EC-Karten' (mit Chip) und HBCI-Karten akzeptiert.

   HINWEIS Für die EC-Karte ist die PC/SC-Schnittstelle notwendig, die mit dem Windows-Betriebssystem mitgeliefert wird.

| | |
|---|---|
| **3. Speicherchipkarte (z. B. Krankenversichertenkarten) mit Chip zur Windowsanmeldung zulassen.** | Diverse Speicherchipkarten (z. B. Krankenversichertenkarten) werden zur Windowsanmeldung zulassen.<br><br>HINWEIS Für die Speicherchipkarten benötigen Sie eine CT32-API, die mit den Treibern des B1 kompatiblen Kartenlesers installiert wird. |
| **4. Wechsel zum normalen Logon mit Abbruch (ESC) im Anmeldemodus zulassen** | Erlaubt oder Unterbindet während des Anmeldevorgangs den Wechsel zur normalen Windowsanmeldung.<br><br>HINWEIS Die Aktivierung dieser Option erhöht zwar die Sicherheit der Anmeldung, beinhaltet jedoch die Gefahr, dass bei Verlust oder Defekt der Chipkarte der komplette Zugang zum Rechner unterbunden ist. |
| **5. Wechsel zum normalen Logon mit Abbruch (ESC) im Sperrmodus zulassen** | Erlaubt oder Unterbindet den Wechsel zur normalen Windowsanmeldung, während der Computer gesperrt ist. |
| **6. Gesicherter Bildschirmschoner** | Bei Aktivierung ist nach dem Auslösen des Bildschirmschoners eine Anmeldung mit Ihrer Chipkarte zwingend erforderlich.<br><br>HINWEIS Entspricht beim Bildschirmschoner der 'Kennworteingabe bei Reaktivierung'! |
| **7. Kontenerstellung für neue Chipkarten während der Windowsanmeldung NICHT zulassen** | Erlaubt oder Unterbindet das Erstellen von Anmeldekonten während dem Anmeldevorgang. Wenn diese Option aktiviert ist, können neue Konten nur im Einstellungsdialog über den Schalter '**Konto erstellen**' angelegt werden.<br><br>HINWEIS Die Aktivierung dieser Option erhöht zwar die Sicherheit der Anmeldung, beinhaltet jedoch die Gefahr, dass bei Verlust oder Defekt der Chipkarte der komplette Zugang zum Rechner unterbunden ist. |
| **8. Nur positiv auf einer Sperrliste (Revocationlist) geprüfte Zertifikate zulassen** | Bei der Verwendung von Zertifikatschipkarten für die Windowsanmeldung, kann eine automatische Sperrlistenüberprüfung durchgeführt werden. Gesperrte Zertifikate werden damit nicht zu Anmeldung zugelassen!<br><br>HINWEIS Die Aktivierung dieser Option sollte nur erfolgen, wenn Sie ganz genau wissen, was Sie tun. Wenn Ihre Chipkarte oder das Zertifikat keine Sperrlisten unterstützt oder ein direkter Zugriff nicht möglich ist, dann kann der Anmeldevorgang unmöglich werden. |
| **9. Soll die Verfügbarkeit des privaten Schlüssels intensiv getestet werden? Dies ist bei einigen CSPs notwendig, die einen permanenten Link in der Datenbank eintragen!** | Die Aktivierung dieser Option ist notwendig, wenn der CSP das Zertifikat in die Windows-Zertifikatsdatenbank einträgt. In diesem Fall erfolgt eine zusätzliche Verfügbarkeitsprüfung, wofür eine Authentifikation mit Passworteingabe nötig ist.<br><br>HINWEIS Wenn mehrere Chipkartenleser oder USB-Token angeschlossen sind, dann muss das Passwort für jedes Gerät eingegeben werden! |
| **10. Soll eine bereit bestehende GINA-Verkettung mitgeladen werden?** | Hinter der Windows-Anmeldung von Microsoft verbirgt sich die sogenannte GINA (Graphical Identification and Authentication). Diese GINA wird von unserer Software und vielen weiteren |

Programmen ausgetauscht, wie beispielsweise auch von Virenscanner. Wenn mehr wie ein Programm eine eigene GINA benötigt, dann werden diese in der Regel verkettet. Durch dieses 'Huckepackverfahren' wird eine GINA nach der anderen aufgerufen.

HINWEIS Um Probleme zu vermeiden, sollte dies Option IMMER aktiviert sein!

**11. Soll die Zertifikatsdatenbank 'Eigene Zertifikate' als Systemuser immer zurück gesetzt werden?**

Die CSPs (Crypto Service Provider) tragen einen Link der Zertifikate auf den Token (USB-Token oder Chipkarte) in der Windows Zertifikatsdatenbank ein. Dies ist erforderlich, damit unsere Software auf die Zertifikate zugreifen kann. Einige CSPs entfernen nach der Operation die Zertifikatseinträge nicht oder nur unvollständig, was in der Regel auch kein Problem darstellt. Wenn sich jedoch mehrere Personen mit unterschiedlichen Zertifikaten an einem Rechner angemeldet haben, füllt sich die Zertifikatsdatenbank mit Links. Dadurch ist vor der Anmeldung die manuelle Auswahl Ihres Zertifikates aus der Liste notwendig.

HINWEIS Bei Aktivierung dieser Option werden vor der Anmeldung alle Links gelöscht, wodurch die Auswahl des eigenen Zertifikates wegfällt.

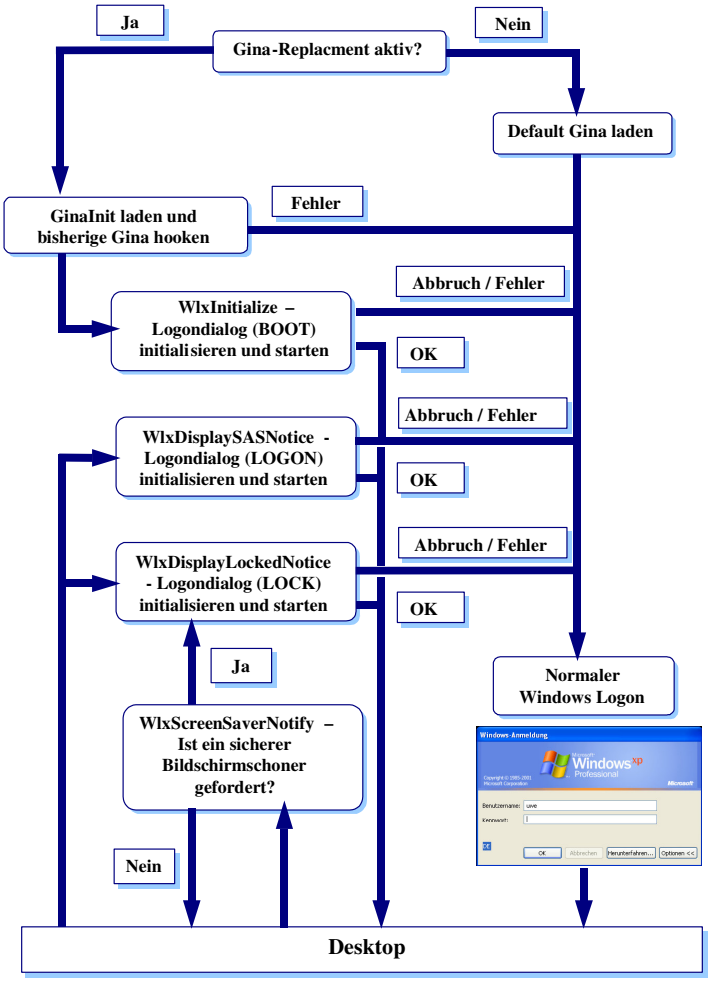
**12. Soll der Sicherheitsdialog (VOR ANMELDUNG Strg+Alt+Entf DRÜCKEN) automatisch übersprungen werden?**

Aus Sicherheitsgründen kann bei den modernen Windowsbetriebssystemen vor der Anmeldung die Aufforderung zur Eingabe von Strg+Alt+Entf aktiviert werden. Dies stellt sicher, dass alle Prozesse terminiert werden, die beispielsweise die Eingabe des Passwortes protokollieren. Bei Aktivierung dieser Option wird die Sicherheitsoption Strg+Alt+Entf übersprungen.

HINWEIS Diese Option kann bei Windows NT von Vorteil sein, wo sich dieser Dialog nicht deaktivieren lässt!

# 3 DIE TECHNIK

Bei der Anmeldung unter Windows NT, 2000 oder XP wird während des Startprozesses durch das Modul Winlogon.exe die MSGina.DLL (Graphical Identification and Authentification) aufgerufen. **abylon LOGON** ersetzt die MSGina.DLL von Microsoft. Im Fall einer erfolgreichen Identifizierung des Anwenders mit einer Chipkarte übergibt das neue Gina-Modul von abylonsoft die korrekten Anmeldedaten an die Winlogon.exe. Damit wird das Betriebssystem weiter hochgefahren und der Anwender kann mit seiner Arbeit beginnen. Durch das Drücken der ESC-Taste während des Anmeldevorgangs wird die originale MSGinaina.DLL geladen und der Anwender kann sich über den bekannten Anmeldedialog einloggen. Diese Funktionalität kann in den Einstellungen unterbunden werden.




# 4 HINWEISE

## 4.1 Systemvoraussetzungen

### 4.1.1 Hard- und Software

- Prozessor: Pentium
- Arbeitsspeicher: 128 MByte RAM
- Freier Festplattenspeicher ca. 12 MByte
- Betriebssystem Windows NT, 2000 oder XP
- Chipkartenleser und Chipkarte (z. B. EC Karte, HBCI-Karte, Fotokarte, Zertifikatschipkarte) oder alternative eine USB-Anschluss mit dem Aladdin eToken

### 4.1.2 Unterstützte Standards:

- CAPI (Microsoft Crypt API),
- PKCS#7 (Cryptographic Message Syntax Standard)
- PKCS#11 (Cryptographic Token Interface Standard)
- PKCS#12 (Personal Information Exchange Syntax)
- RSA
- PC/SC
- RC4, Blowfish, AES, 3DES...
- X.509 v3 Zertifikate
- SCard-API
- CT32-API
- Microsoft Zertifikatsdatenbank

### 4.1.3 Technische Informationen:

- Installations- und Deinstallationsroutine
- Treiber für Chipkartenleser oder USB-Token muss separat installiert werden
- Aus das Zertifikat der Chipkarte kann optional direkt oder indirekt über den CSP zugegriffen werden.
- CSP (Crypto Service Provider) muss separat installiert werden (siehe auch Kapitel 2.1.1)
- EC-Karte muss mit einem Chip ausgestattet sein
- Für die Speicherchipkarten (z. B. Krankenversicherten-Karten) muss der Kartenleser eine CT32-API unterstützen

## 4.2 Unterstütze Chipkarten

### 4.2.1 Zertifikatschipkarten / USB-Token

Für die Verwendung von Zertifikatschipkarten oder USB-Token (z. B. Aladdin eToken) muss auf dem Rechner ein CSP (Crypto Service Provider) installiert sein, wobei die Software **abylon LOGON** zwei Optionen (direkt und indirekt) für den Zugriff auf das Zertifikat zur Verfügung stellt.

### 4.2.2 EC-/HBCI-/Fotokarten

Für die Verwendung von EC-Karten, HBCI-Karten oder Fotokarten mit Chip muss der entsprechende Kartenleser eine PC/SC-Schnittstelle anbieten.

### 4.2.3 Speicherchipkarten (z. B. Krankenversichertenkarten)

Für die Verwendung von Speicherchipkarten muss der Kartenleser eine CT32-API anbieten. Diese muss in den Einstellungen ausgewählt werden.

### 4.2.4 Sonstige Chipkarten

Sollten unsere Software spezielle Chipkartenleser, USB-Token, CSP's oder auch Software nicht unterstützt oder erkennen, so treten Sie einfach mit uns in Verbindung. Individueller Support oder spezielle Anpassungen unserer Software können in der Regel nach Anfrage relativ schnell umgesetzt werden.

## 4.3 Weitere Dokumente und FAQs

Weitere Dokumente, FAQs (Frequently Ask Questions), Downloads, Testversionen, Pressematerialien, Screenshots finden Sie auf unserer Homepage (http://www.abylonsoft.de) oder schicken wir Ihnen gerne auf Anfrage zu.