Authention Safety Suite

Für Windows 2000/XP

Installation

digitronic
computersysteme gmbh

Oberfrohnaer Straße 62
D-09117 Chemnitz
Telefon: +49 (0) 371 81539-0
Fax: +49 (0) 371 81539-900
Internet: www.digitronic.net
E-Mail: info@digitronic.net

Verfasser: Sven Grzeszczuk
Stand: 9. April 2010
Version: 1.0

INHALT

Inhaltsverzeichnis

KAPITEL 1

1 Systemvoraussetzung

Die Authention Safety Suite setzt als Betriebssystem Windows 2000/XP voraus. Die Installation unter neueren Betriebssystemen wird nicht verhindert. Jedoch werden keine anderen als die genannten Betriebssysteme offiziell unterstützt.

Die Mindestanforderungen an die Hardware entsprechen denen des jeweils zu Grunde liegenden Betriebssystems.

Für die Installation der kompletten Authention Safety Suite wird eine verfügbare Festplattenkapazitä tvon mindestens 50 MB empfohlen.

Desweiteren sollten alle verfügbaren Service Packs und Updates des Betriebssystems installiert worden sein.

KAPITEL 2

2 Interaktives Setup

Für die Installation von Authention sind administrative Berechtigungen erforderlich. Diese sind meist dann gegeben, wenn der angemeldete Benutzer ein Administrator oder ein Mitglied der Gruppe der "Hauptbenutzer" ist.

2.1 Installation

2.1.1 Begrüßungsdialog

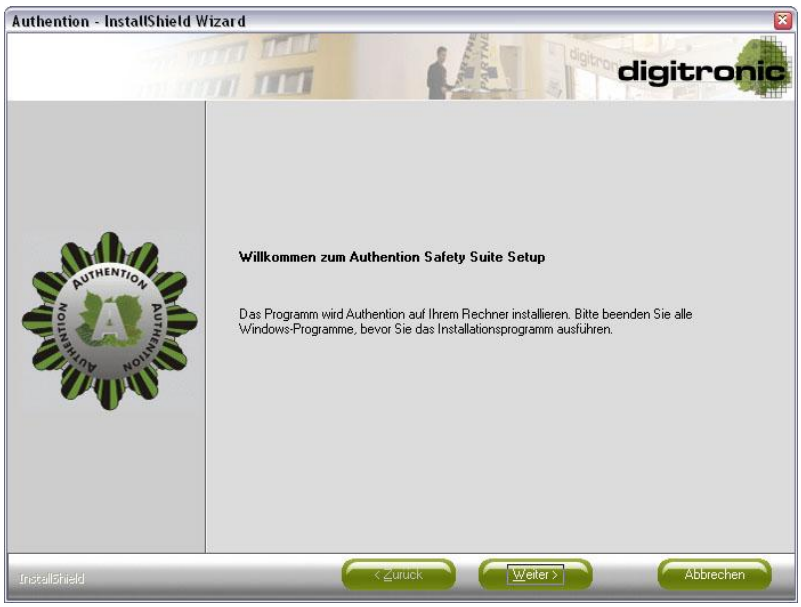

Abbildung 2.1: Begrüßungsdialog

Der Begrüßungsdialog bittet darum, alle geöffneten Anwendung zu schließen. Dies ist ratsam, da am Ende der Installation das Betriebssystem neu gestartet werden muss, damit die Installation abgeschlossen werden kann.

2.1.2 Informationen über Authention

Abbildung 2.2: Information über Authention

Die Informationen geben einen kurzen Überblick über die einzelnen Komponenten der Authention Safety Suite.

2.1.3 Lizenzbedingung

Abbildung 2.3: Lizenzbedingung

Sie müssen den Lizenzbedingungen von digitronic zustimmen, wenn Sie Authention installieren möchten.

2.1.4 Eingabe der Lizenzdaten

Für die Verwendung der Authention-Komponenten ist eine gültige Lizenz erforderlich. Da die Komponenten ohne diese Lizenz nicht funktionieren, ist die Eingabe an dieser Stelle zwingend erforderlich.

Wird keine Lizenz eingegeben ist nur die Installation der Token Management System Client- bzw. Administrations-Komponente möglich.

Abbildung 2.4: Lizenzdaten eingeben

Die Gültigkeit der Lizenz wird überprüft, sobald auf "Weiter" geklickt wird. Sollte die Lizenz ungültig sein, erscheint eine Fehlermeldung und die Installation kann nicht fortgesetzt werden.

Die Lizenz kann automatisch eingelesen werden. Dazu muss sich die Datei "Authention.txt" in dem gleichen Verzeichnis befinden wie das Setup "Authention.exe", wenn dieses ausgeführt wird.

Nähere Informationen zu diesem Thema sind im Kapitel "Lizenzdatei" zu finden.

2.1.5 Auswahl der Installationsvariante und des Zielordners

Abbildung 2.5: Installationsvariante und –pfad wählen

In diesem Dialog kann das Installationsverzeichnis geändert werden, in das Authention installiert werden soll.

Darüber hinaus ist hier eine Installationsvariante zu wählen, die sich entscheidend auf den weiteren Verlauf der Installation und des zu verwendenden Token auswirkt.

Die erweiterte Installation bietet Möglichkeiten, die einzelnen Komponenten individuell zu konfigurieren. Dies erfordert jedoch umfassende Authention-Kenntnisse.

Während der Standardinstallation werden die jeweiligen Komponenten mit Standardeinstellungen installiert.

Im weiteren Verlauf werden alle Dialoge des Setups angezeigt. Am linken Rand wird verdeutlicht, in welcher Installationsvariante dieser erscheint.

2.1.6 Komponenten Auswahl (nur erweitert)

Abbildung 2.6: Komponentenauswahl - Standartansicht

Dieser Dialog zeigt die Standardansicht der Komponenten-Liste und gibt einen Überblick über die zu installierenden Authention-Komponenten. Einige Komponenten besitzen Unterkomponenten, die optional installiert werden können.

Abbildung 2.7: Komponentenauswahl – Ansicht mit Unterkomponenten

Standardmäßig sind alle Komponenten ausgewählt, die anhand der eingegebenen Lizenz installiert werden können. Nicht benötigte Komponenten können abgewählt werden und werden entsprechend nicht installiert.

Auf der rechten Seite werden kurze Beschreibungen zu den jeweiligen Komponente angezeigt.

Durch Klicken auf "Weiter" werden für die gewählten Komponenten Einstellungsdialoge angezeigt. Diese Einstellungsdialoge variieren entsprechend der vorgenommenen Komponentenauswahl. Das bedeutet, dass ein Einstellungsdialog für eine Komponente nur dann angezeigt wird, wenn die entsprechende Komponente für die Installation ausgewählt wurde.

Für die Logon-Komponente sind an dieser Stelle keine Einstellungen erforderlich. Zu beachten ist, dass die Logon-Komponente so konfiguriert wird, dass sie die Arbeitsstation für den angemeldeten Benutzer sperrt, sobald der Token vom System getrennt wird. Dies ist in beiden Installations-varianten gleich und kann später in den Logon-Einstellungen geändert werden.

2.1.7 Einstellungsdialog für Single Sign On (nur erweiter)

Für die Single Sign On-Komponente sind zwei Einstellungen erforderlich: zum einen der Speicherort für die benötigten Daten und zum anderen eine Tastenkombination zum Steuern von Single Sign On.

Abbildung 2.8: Einstellungsdialog für Single Sign On I

Wird als Medium ein "Beliebiges anderes Verzeichnis..." ausgewählt, muss mit Hilfe von "Durchsuchen..." auch ein entsprechendes Verzeichnis ausgewählt werden. Vorher kann der Dialog mit den aktuellen Einstellungen nicht verlassen werden.

Abbildung 2.9: Einstellungsdialog für Single Sign On II

Sobald ein Verzeichnis ausgewählt wurde, wird es angezeigt, wenn das entsprechende Medium ausgewählt ist.

2.1.8 Einstellungsdialog für Virtual Private Drive (nur erweitert)

Mit einem Klick auf "Weiter" gelangt man zum Einstellungsdialog der Virtual Private Drive-Komponente.

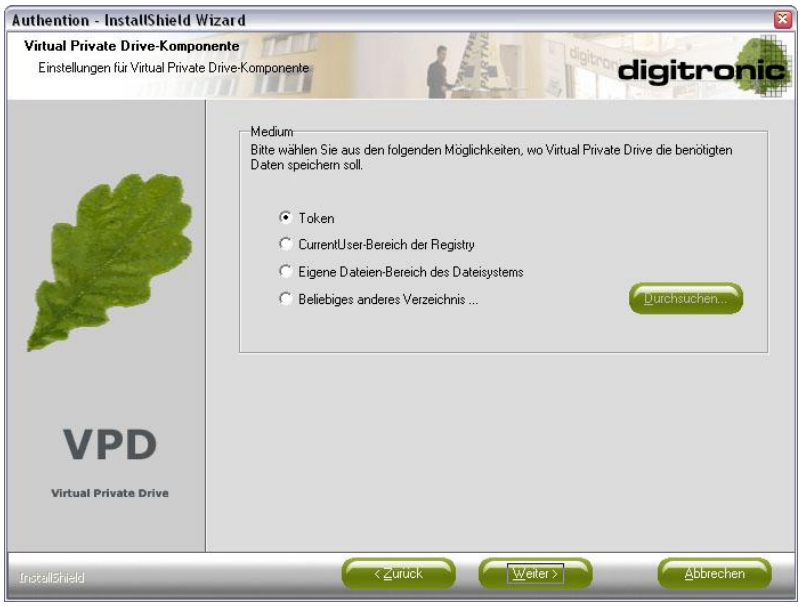

Abbildung 2.10: Einstellungsdialog für Virtual Private Drive

Hier ist, wie bei der Single Sign On-Komponente, die Angabe des Mediums zum Speichern der Daten erforderlich.

2.1.9 Einstellungsdialog für Crypted Group Share (nur erweitert)

Abbildung 2.11: Einstellungsdialog für Crypted Group Share

Analog zu den beiden vorangegangenen Dialogen arbeitet der Einstellungsdialog für die Crypted Group Share-Komponente.

2.1.10 Einstellungsdialog für Universal Device Block (nur erweitert)

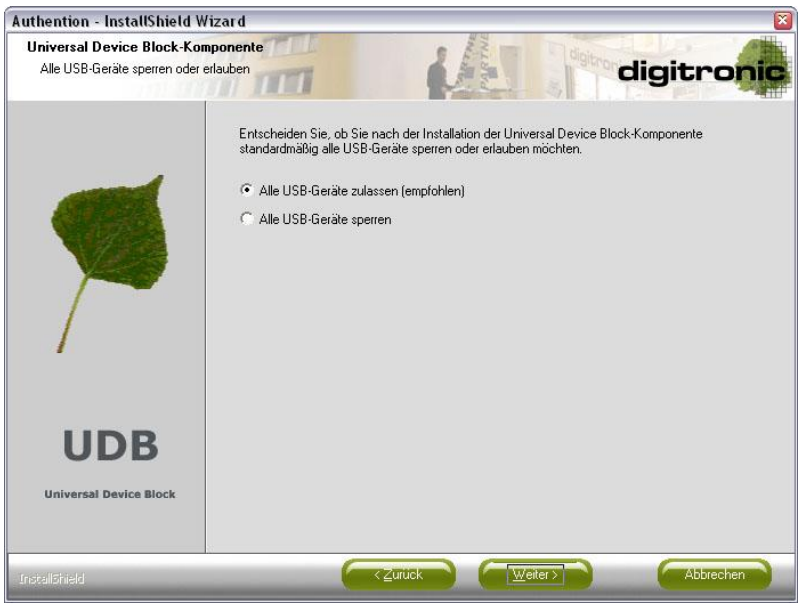

Abbildung 2.11: Einstellungsdialog für Universal Device Block

Für die Universal Device Block-Komponente wird festgelegt, ob nach der Installation alle USB-Geräte blockiert oder zugelassen werden. Die empfohlene Standardeinstellung, alle Geräte zuzulassen, ist beim ersten Anzeigen dieses Dialogs voreingestellt.

Für die Extended Device Block-Komponente sind keine Einstellungen erforderlich. Hier werden anfangs vordefinierte Standardeinstellungen angenommen, die in einer XML-Datei gespeichert sind.

2.1.11 Einstellungsdialoge für das Token Management System (nur erweitert)

Die Einstellungsdialoge für das Token Management System variieren in Abhängigkeit von den für die Installation ausgewählten Komponenten des Token Management Systems. Hierbei wird unterschieden, ob die Client-Komponente als einzige Komponente des Token Management Systems ausgewählt wurde oder nicht. Wurde die Client-Komponente des Token Management Systems als einzige Komponente ausgewählt, werden zwei Modi unterschieden. Zum einen kann die Client-Komponente im StandAlone - Modus und zum anderen als Teil des Token Management System, im sogenannten TMS-Modus, installiert werden.

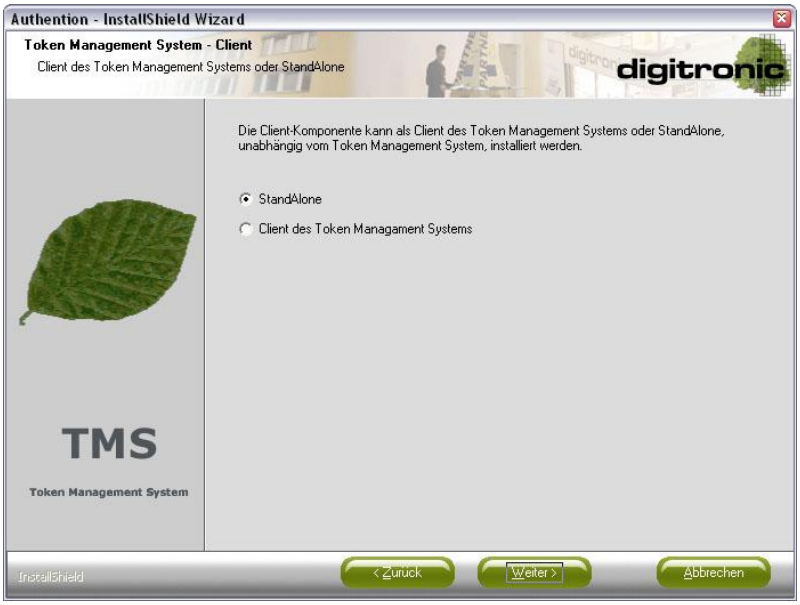

Abbildung 2.12: Einstellungsdialog für Token Management System – Client I

Im TMS-Modus ist die Angabe der IP-Konfigurationsdaten für die Server-Komponente erforderlich, damit die Client-Komponente im Netzwerk arbeiten kann.

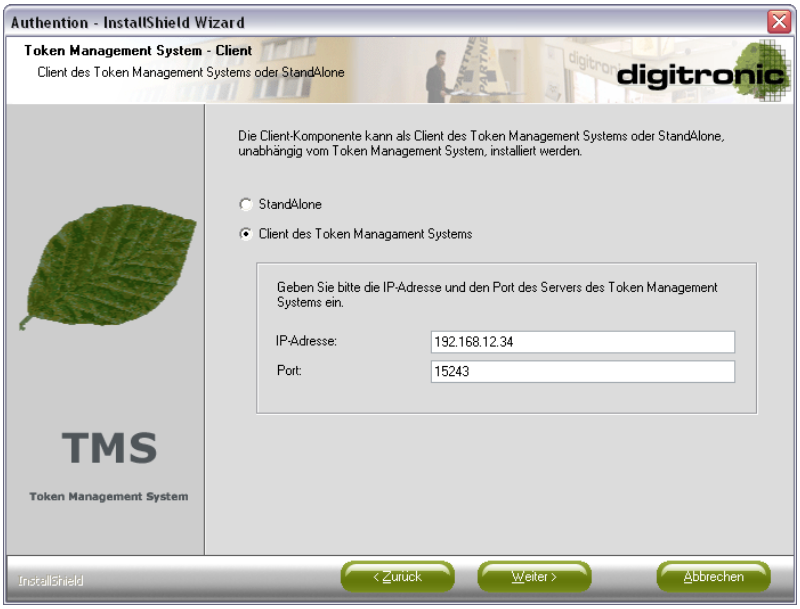

Abbildung 2.13: Einstellungsdialog für Tokenmanagement System – Client II

Die Eingabe eines DNS-Namens ist als IP-Adresse unzulässig. Der Port sollte 5-stellig sein und darf von keiner anderen Anwendung verwendet werden.

Wird die Server-Komponente des Token Management Systems als einzige Komponente ausgewählt, wird der zu verwendende Port abgefragt, auf dem eingehende Verbindungen verwaltet werden sollen.

Sobald nur die Administrations-Komponente oder mehr als eine Komponente ausgewählt werden, erscheint die Abfrage der IP-Konfigurationsdaten.

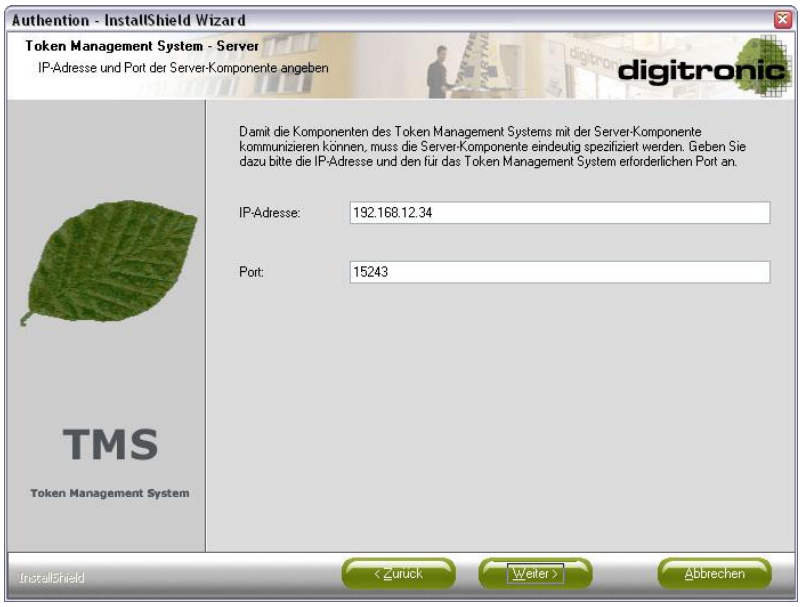

Abbildung 2.14: Einstellungsdialog für Tokenmanagement System - Server

Die nachfolgenden Dialoge enthalten keine Komponenten-spezifischen Einstellungsmöglichkeiten, sondern beziehen sich allgemein auf die Installation von Authention.

Die beiden nachfolgenden Dialoge erscheinen nur dann, wenn mindestens eines der folgenden Kriterien erfüllt ist.

- Die Logon-Komponente soll installiert werden.
- Als Medium wurde bei der Single Sign On-Komponente "Token" ausgewählt.
- Als Medium wurde bei der Virtual Private Drive-Komponente "Token" ausgewählt.
- Als Medium wurde bei der Crypted Group Share-Komponente "Token" ausgewählt.

Im folgenden Dialog werden die Token ausgewählt, die von Authention nach der Installation unterstützt werden sollen.

2.1.12 Token Auswahl (nur erweitert)

Die folgende Liste zeigt die derzeit unterstützten und getesteten Token an, für die eine automatische Treiber-Installation während des Authention-Setups möglich ist.

An dieser Stelle sei der Begriff "Token" einmal etwas näher erläutert:

Ein Token ist ein sicheres Medium zum Speichern von Informationen. Das sind zum Beispiel Smartcards, biometrische Systeme und so weiter. Der Vorteil solcher Token ist neben der Flexibilität in erster Linie die verschlüsselte Speicherung der Daten. Um Daten auslesen und schreiben zu können, ist in der Regel die Eingabe einer PIN erforderlich. Im Gegensatz dazu muss bei biometrischen Systemen durch einen Fingerabdruck oder ähnliches das Gerät für die Benutzung freigegeben werden. Eine PIN ist in diesem Fall nicht erforderlich.

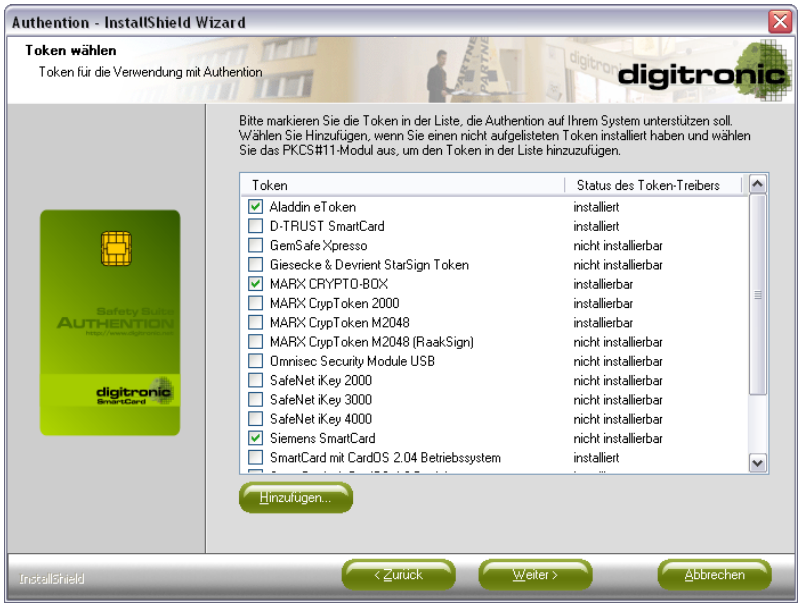

Abbildung 2.15 einstellungsdialog Token Auswahl I

In der zweiten Spalte der Token-Liste ist der Status für den jeweiligen Token-Treiber dargestellt. Hier gibt es die folgenden Möglichkeiten.

installiert:

Entweder ist der erforderliche Treiber bereits vorhanden und muss nicht installiert werden oder ein Treiber ist für diesen Token nicht erforderlich. Die automatische Installation während des Authention-Setups ist in diesem Fall ausgeschlossen.

installierbar:

Der erforderliche Treiber für diesen Token ist nicht installiert. Er kann aber automatisch während des Authention-Setups installiert werden.

nicht installierbar:

Es wurde kein installierter Treiber für den Token gefunden und der Treiber kann auch nicht automatisch installiert werden, weil dem Setup das notwendige Treiber-Paket nicht zur Verfügung steht.

Token, die bereits installiert sind, aber in dieser Liste nicht erscheinen, können über den Button "Hinzufügen..." dieser Liste hinzugefügt werden.

Abbildung 2.16 einstellungsdialog Token Auswahl II

Um auf einen Token zuzugreifen, wird der PKCS#11-Standard-verwendet. Die meisten Token-Hersteller liefern mit den Token-Treibern ein Modul aus, dass die PKCS#11-Funktionalität zur Verfügung stellt. Dieses Modul (meist eine DLL) muss an dieser Stelle ausgewählt werden. Nach dieser Auswahl wird die DLL überprüft, ob Sie tatsächlich die gewünschte Funktionalität bereitstellt. Andernfalls wird eine Fehlermeldung angezeigt und der Token nicht der Token-Liste hinzugefügt.

Ist die Überprüfung erfolgreich, wird der gewählte Dateiname stellvertretend für den benutzerdefinierten Token in der Token-Liste angezeigt und gleichzeitig ausgewählt.

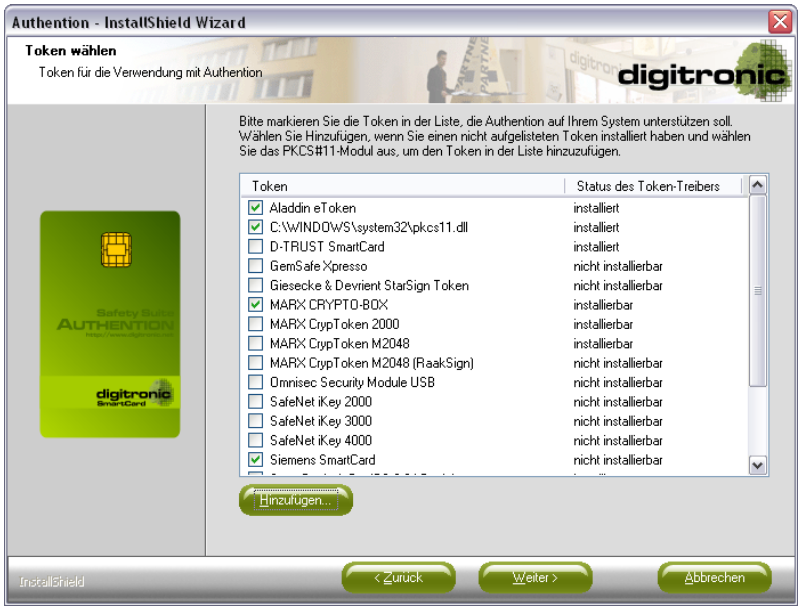

Abbildung 2.17 einstellungsdialog Token Auswahl III

Generell ist es empfehlenswert, nur einen einzigen und nicht mehrere, verschiedene Token zu verwenden. Dennoch ist es möglich, mehrere Token auszuwählen.

Dabei gibt es jedoch Einschränkungen, die eingehalten werden müssen.

- Es können nicht mehrere Token der Firma MARX gleichzeitig verwendet werden (ausgenommen davon ist MARX CrypToken M2048 (RaakSign)).
- Die Token "Wechseldatenträger" und "SmartCard mit TCOS 2.0 Betriebssystem" können nicht gleichzeitig verwendet werden.

Diese Konstellationen werden durch das Setup verhindert und mit einer entsprechenden Fehlermeldung angezeigt.

Darüber hinaus gelten die folgenden Empfehlungen.

- Es sollten nicht gleichzeitig verschiedene Token der Firma SafeNet verwendet werden.
- Der Token "Siemens SmartCard" sollte nicht in Verbindung mit anderen PKCS#11-Token verwendet werden.
- Token der Firma GemSafe sollten nicht mit "SafeNet iKey3000" oder "Giesecke und Devrient StarSign Token" kombiniert werden.

Diese Konstellationen werden zwar nicht verhindert, sollten aber nicht verwendet werden.

Mit einem Klick auf "Weiter" wird die aktuelle Token-Auswahl überprüft. Wurde ein Token ausgewählt, dessen Treiber-Status "nicht installierbar" ist, erscheint eine Warnung.

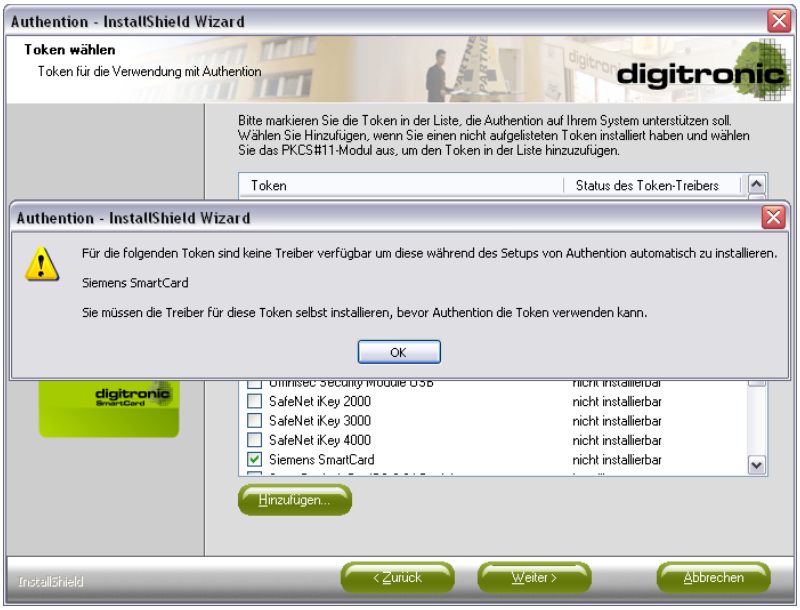

Abbildung 2.18 einstellungsdialog Token Auswahl IV

Diese besagt, dass der Treiber manuell installiert werden muss. Vorher kann der Token nicht mit Authention verwendet werden. Gegebenenfalls kann es sogar zu einer zeitlichen Verzögerung kommen, da der Token-Treiber nicht gefunden werden kann.

Sind keine Fehler aufgetreten, wird der nächste Dialog angezeigt. Dieser erscheint nur dann, wenn Token ausgewählt wurden, deren Treiber-Status "installierbar" ist.

2.1.13 Token Treiber Auswahl (nur erweitert)

Abbildung 2.19: Einstellungsdialog Token-TreiberAuswahl

Hier können die Token demarkiert werden, deren Treiber nicht installiert werden sollen. Standardmäßig sind alle "installierbaren" Token markiert, so dass die automatische Treiber-Installation gestartet werden kann.

Der folgende Dialog wird im erweiterten Setup immer angezeigt.

2.1.14 Auswahl des Startmenü-Ordners (nur erweitert)

Abbildung 2.20: Startmenü - Ordner

Hier kann festgelegt werden, in welchem Ordner im Startmenü die Verknüpfungen zu den Authention-Komponenten angelegt werden sollen.

Standardmäßig wird der Ordner "digitronic\Authention" vorgeschlagen. Die Verknüpfungen können jedoch auch in einem bereits existierenden Ordner angelegt werden.

Der letzte Dialog vor dem Kopieren der Dateien fasst die vorgenommenen Einstellungen zusammen.

2.1.15 Zusammenfassen vor dem Kopieren der Datei

Abbildung 2.21: Zusammefassung vor dem Kopieren

Dieser Dialog wird sowohl im Standard- als auch im erweiterten Setup angezeigt.

Um Änderungen an den Einstellungen vorzunehmen, kann mit dem Button "Zurück" der entsprechende Dialog erneut aufgerufen werden, um die Einstellung zu ändern. Die Einstellungsdialoge erscheinen jedoch nur im erweiterten Setup.

Mit einem Klick auf "Weiter" wird der Kopiervorgang gestartet.

2.1.16 Kopieren der Authention Datei

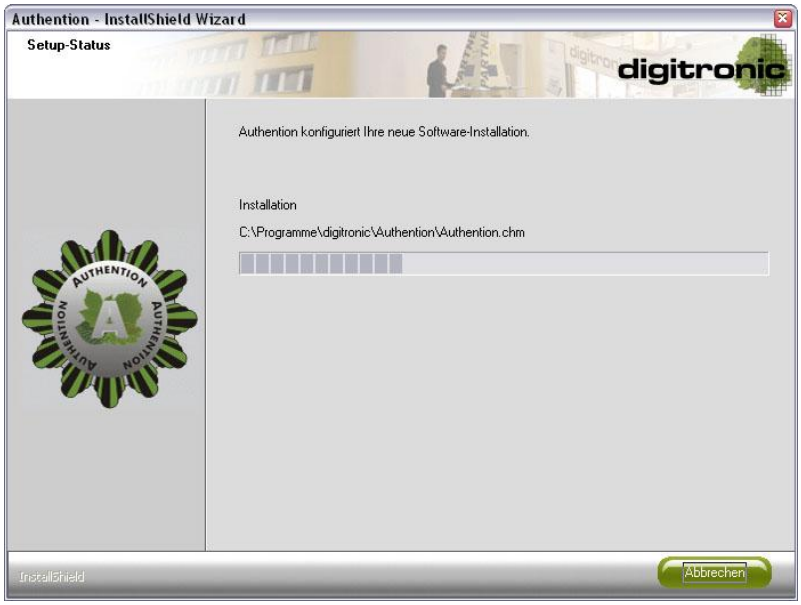

Abbildung 2.22: Kopieren von Dateien

Sobald alle Authention-Dateien kopiert sind, werden die Token-Treiber installiert, die in der Token-Treiber-Auswahlliste markiert wurden.

Werden dabei externe Setups gestartet, erscheint eine Warnung.

Abbildung 2.23. Meldung vor Token – Treiber - Installation

Diese Meldung warnt, dass ein Token-Treiber-Setup am Ende eventuell einen Neustart des Betriebssystems verlangen könnte. Dieser Neustart darf aber **auf keinen Fall** durchgeführt werden, da die Installation von Authention zu diesem Zeitpunkt noch nicht vollständig abgeschlossen ist.

Das Authention-Setup wartet mit der weiteren Installation von Authention, bis die Token-Treiber-Setups abgeschlossen sind.

Nähere Informationen zum Thema "Installation von Token-Treibern" sind im gleichnamigen Kapitel zu finden.

Nach dem Kopieren der Authention-Dateien und dem Installieren der erforderlichen Token-Treiber, erscheinen weitere Dialoge. Diese variieren in Abhängigkeit von vorgenommenen Einstellungen.

Damit Authention sofort nach dem abschließenden Neustart des Betriebssystems mit dem Token arbeiten kann, ist eine Initialisierung des Tokens erforderlich. Diese stellt sicher, dass erforderliche Strukturen angelegt werden.

2.1.17 Initialisierung des Token

Abbildung 2.24: Token Initialisierung

Sollte der Token bereits initialisiert sein, muss er im Setup nicht initialisiert werden.

Die Initialisierung des Tokens ist nur dann möglich, wenn alle folgenden Kriterien erfüllt sind.

- Die Client-Komponente des Token Management Systems wurde im StandAlone-Modus installiert.
- Die Token-Treiber waren bereits installiert oder wurden automatisch installiert und können sofort verwendet werden.
- Die Initialisierung dieses Tokens während des Authention-Setups wurde getestet. Der Token kann während der Installation initialisiert werden.

Soll der Token nicht initialisiert werden, kann die Markierung entfernt werden.

Wurde die Logon-Komponente installiert, können nun die für die Anmeldung am Betriebssystem erforderlichen Anmeldedaten auf dem Token gespeichert werden.

2.1.18 Speichern der Logo Daten auf dem Token

Abbildung 2.25: Logon Daten speichern I

Dies stellt sicher, dass der Token sofort nach dem abschließenden Neustart als Authentifizierungsmittel verwendet werden kann.

Hierfür ist die Eingabe der Benutzerdaten erforderlich.

Sollen die Logon-Daten nicht auf dem Token gespeichert werden, können die Felder leer gelassen werden.

Abbildung 2.26:. Logon Daten speichern II

Mit einem Klick auf "Ja" muss in diesem Fall eine explizite Bestätigung erfolgen, dass die Logon-Daten nicht auf dem Token gespeichert werden sollen.

Wenn der Token initialisiert werden soll und/oder wenn die Logon-Daten auf dem Token gespeichert werden sollen, wird der folgende Dialog angezeigt.

2.1.19 Konfiguration des Token

Abbildung 2.27: Token konfigurieren I

Dies ist der Start-Dialog für die Konfiguration des Tokens. Mit einem Klick auf "Weiter" wird die Client-Komponente des Token Management Systems im Hintergrund gestartet, um den Token zu initialisieren und/oder die Logon-Daten auf dem Token zu speichern. Soll der Token trotz der entsprechenden Auswahl in den beiden vorherigen Dialogen zu diesem Zeitpunkt nicht konfiguriert werden, kann dies durch Klicken auf den Button "Überspringen" verhindert werden.

Soll der Token jedoch konfiguriert werden, ist es wichtig, dass der Token bereits mit dem System verbunden ist, bevor der Button "Weiter" aktiviert wird.

Abbildung 2.28: Token konfigurieren II

Die dargestellte Meldung bietet die letzte Möglichkeit, die Bearbeitung des Tokens während des Setups abzubrechen.

Abbildung 2.29: Token konfigurieren III

Danach wird die Client-Komponente des Token Management Systems gestartet, um den Token entsprechend der vorgenommenen Einstellungen zu konfigurieren.

Während der Initialisierung werden die neue und (bei PKCS#11-Token) die alte PIN abgefragt.

Abbildung 2.30: Token konfigurieren IV

Sollen nur die Logon-Daten gespeichert werden, ist in der Regel nur die aktuelle PIN erforderlich.

Die Client-Komponente bricht den Bearbeitungsvorgang nach spätestens 60 Sekunden ab, wenn kein Token erkannt wurde.

In diesem Fall wird der Dialog nicht verlassen und eine Fehlermeldung angezeigt.

Abbildung 2.31: Token konfigurieren V

Zu diesem Zeitpunkt ist der Token nicht fertig konfiguriert. Durch Auswahl von "Weiter" kann ein weiterer Versuch gestartet werden, den Token zu konfigurieren. Nach wie vor kann dies durch den Button "Überspringen" umgangen werden.

Sobald der Token erfolgreich konfiguriert wurde, wird dies durch eine entsprechende Erfolgsmeldung angezeigt.

Abbildung 2.32: Token konfigurieren VI

Wird nun auf "Weiter" geklickt, wird der nächste Setup-Dialog angezeigt.

2.1.20 Einführung zu Authention anzeigen

Abbildung 2.33: Einführung starten

Der letzte Dialog vor dem Abschluss der Installation bietet die Möglichkeit, eine Einführung zu Authention anzuzeigen. Diese ist auch zu einem späteren Zeitpunkt über eine Verknüpfung im Startmenü erreichbar.

Durch einen Klick auf "Weiter" wird diese Einführung gestartet. Das Setup wartet mit dem Abschluss der Installation bis die Einführung beendet ist.

2.1.21 Abschluss der Installation

Abbildung 2.34: Abschluss der Installation

Um die Installation von Authention abzuschließen, ist ein Neustart zwingend erforderlich, da Systemkomponenten ausgetauscht wurden, die beim Start des Betriebssystems geladen werden.

Sollte der Neustart nicht durchgeführt werden, erscheint die folgende Warnmeldung.

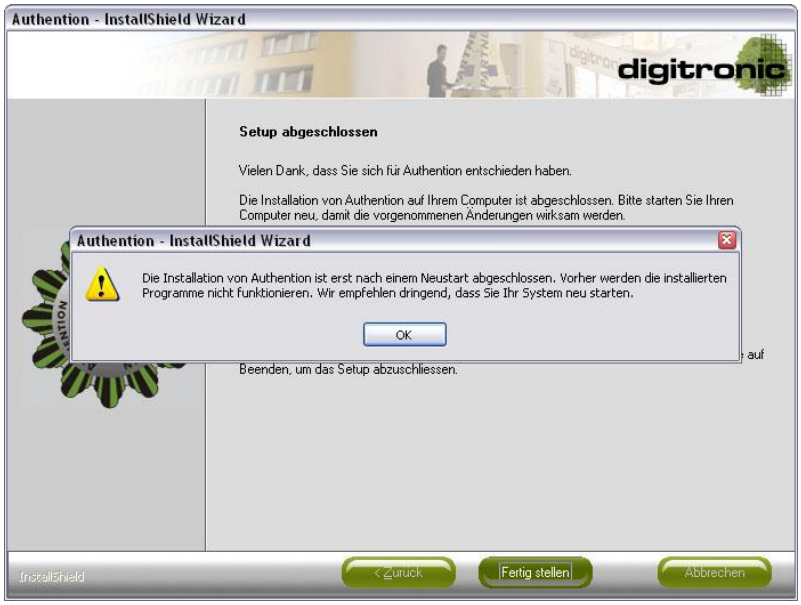

Abbildung 2.35: Hinweis auf Neustart

2.2 Ändern

Mit dem Wartungsmodus "Ändern" können nachträglich weitere Komponenten installiert oder bereits installierte Komponenten deinstalliert werden.

Es wird zu Beginn der Wartungsdialog angezeigt, wo die Auswahl "Ändern" vorgenommen wird.

2.2.1 Wartungsdialog ändern

Abbildung 2.36: Wartungsdialog - Ändern

Im Wartungsmodus "Ändern" sind alle Einstellmöglichkeiten verfügbar, die das erweiterte Setup bei der Installation auch geboten hat.

Vorab wird die Möglichkeit geboten, die aktuelle Lizenz zu ändern. Auch an dieser Stelle wird die Datei "Authention.txt" automatisch eingelesen, wenn sie sich neben der Datei "Authention.exe" befindet.

2.2.2 Eingabe der Lizenzdatei

Abbildung 2.37: Lizenzdaten eingeben

Danach werden alle Einstellungsdialoge angezeigt, die bei der Installation ausschließlich in der erweiterten Variante angezeigt werden.

Um nicht alle Einstellungsdialoge erneut darzustellen, sei an dieser Stelle auf das Kapitel "Installation" verwiesen.

Die bei der Installation vorgenommenen Einstellungen werden in den entsprechenden Dialogen voreingestellt. Wird eine Komponente erstmals installiert, werden Standard-Werte für die jeweiligen Einstellungen angenommen.

2.2.3 Abschluss der Wartungsarbeiten

Nach dem Kopieren der Dateien ist ein Neustart erforderlich.

Abbildung 2.38: Abschluss der Wartungsarbeiten

2.3 Reparieren

Das Reparieren der Installation ist nur dann erforderlich und sinnvoll, wenn die Authention-Komponenten nicht korrekt arbeiten sollten, weil Dateien gelöscht wurden oder Einstellungen fehlerhaft sind.

Während des Reparierens der Authention-Installation werden alle Dateien wiederhergestellt. Sollten zwischenzeitlich Dateien gelöscht worden sein, werden diese wiederhergestellt.

Alle Einstellungen werden auf die Werte zurückgesetzt, die nach der Installation von Authention gültig waren. Das bedeutet, dass alle später vorgenommenen Änderungen an den Einstellungen der einzelnen Komponenten rückgängig gemacht werden.

Es wird zu Beginn der Wartungsdialog angezeigt, wo die Auswahl "Reparieren" vorgenommen wird.

2.3.1 Wartungsdialog Reparieren

Abbildung 2.39: Wartungsdialog - Reparieren

Mit einem Klick auf "Weiter" wird die Reparatur gestartet.

2.3.2 Reparatur der installierten Komponenten

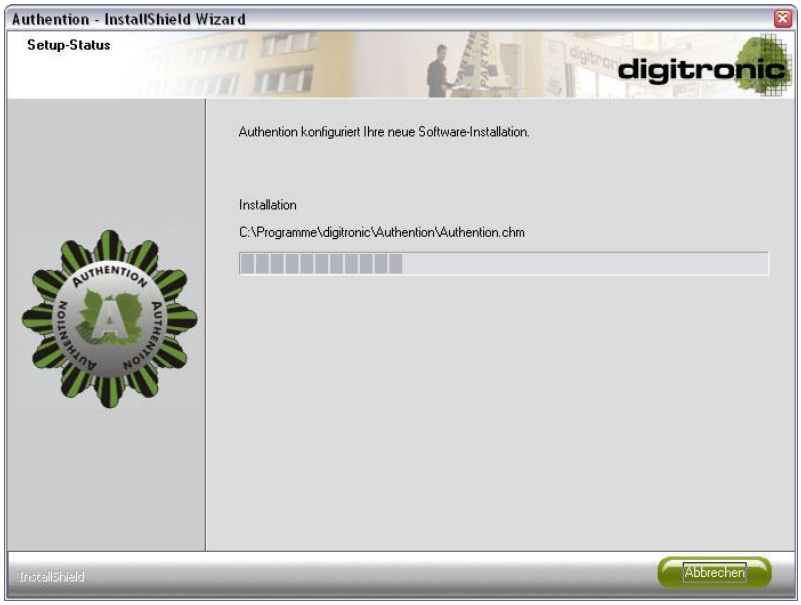

Abbildung 2. 40: Reparatur

2.3.3 Abschluss der Reparatur

Nach der Reparatur ist ein Neustart erforderlich.

Abbildung 2.41: Abschluss der Reparatur

2.4 Aktualisieren

Das Aktualisieren der installierten Komponenten ist nur dann sinnvoll, wenn es aktuellere Versionen der Komponenten-Dateien gibt.

Bei der Aktualisierung werden keine Änderungen an den Einstellungen der einzelnen Komponenten vorgenommen. Alle benutzerdefinierten Einstellungen, die nach der Installation durch die Verwendung der Komponenten vorgenommen wurden, bleiben erhalten.

Es wird zu Beginn der Wartungsdialog angezeigt, in dem die Auswahl "Aktualisieren" vorgenommen wird.

2.4.1 Wartungsdialog aktualisieren

Abbildung 2.42: Wartungsdialog - Aktualisieren

Mit einem Klick auf "Weiter" wird die Aktualisierung gestartet.

2.4.2 Aktualisierung der installierten Komponenten

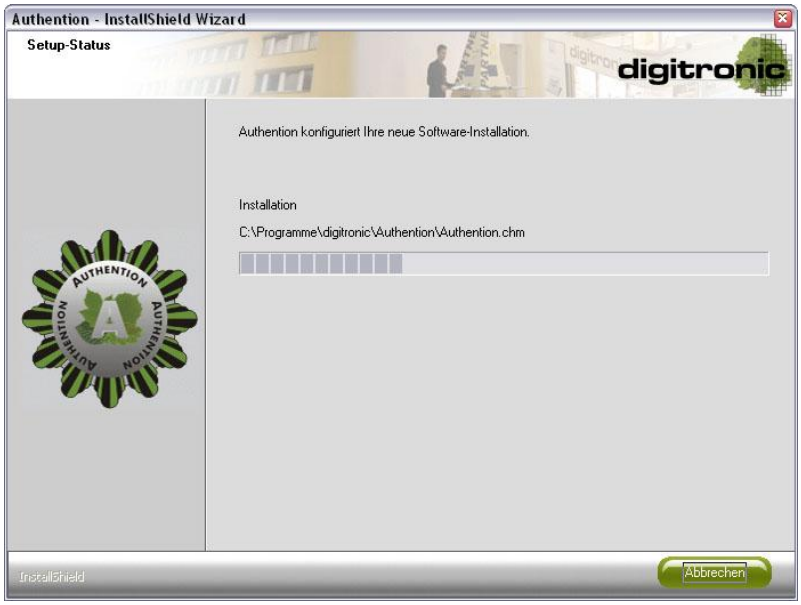

Abbildung 2.43: Aktualisieren

Nach der Aktualisierung ist ein Neustart erforderlich.

2.4.3 Abschluss der Aktualisierung

Nach der Aktualisierung ist ein Neustart erforderlich.

Abbildung 2.44: Abschluss der Aktualisierung

2.5 Entfernen

Beim Entfernen wird Authention vollständig deinstalliert. Alle Dateien sowie alle benutzerdefinierten Einstellungen werden gelöscht.

Es wird zu Beginn der Wartungsdialog angezeigt, in dem die Auswahl "Entfernen" vorgenommen wird.

2.5.1 Wartungsdialog entfernen

Abbildung 2.45: Wartungsdialog - Entfernen

Durch einen Klick auf "Weiter" wird die Deinstallation gestartet.

2.5.2 Entfernen der Installierten Komponenten

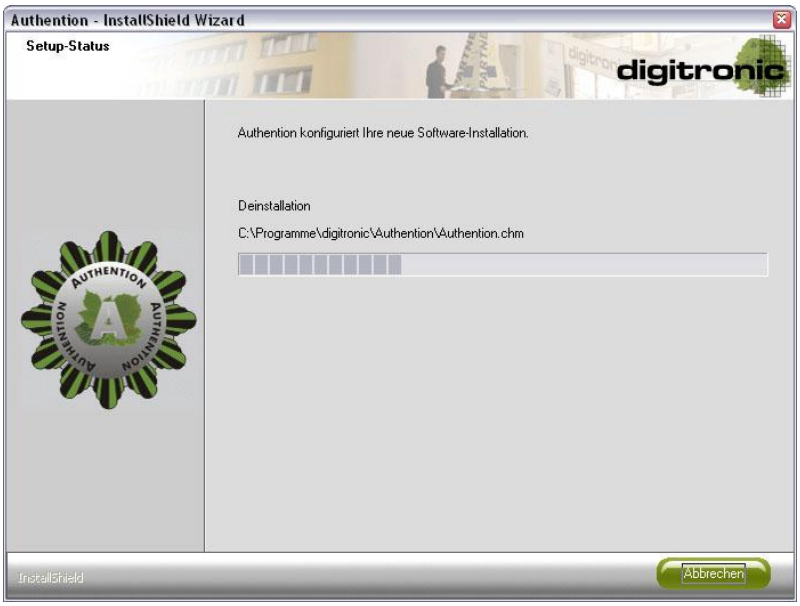

Abbildung 2.46: Deinstallation

2.5.3 Abschluss der Deinstallation

Nach der Deinstallation ist ein Neustart erforderlich.

Abbildung 2.47: Abschluss der Deinstallation

KAPITEL 3

3 Automatisiertes Setup (Silent Setup)

3.1 Normal-Modus

Wird das Setup von Authention im NORMAL-Modus gestartet, werden die Dialoge, wie sie im vorherigen Kapitel beschrieben sind, dargestellt.

Der Start des Setups erfolgt in diesem Fall ohne Parameter.

3.2 RECORD-Modus

Der RECORD-Modus ist ein interaktives Setup und dient der Vorbereitung eines automatisierten Setups. Wird das Setup in diesem Modus gestartet, werden alle Auswahlen und Einstellungen, die während dieses interaktiven Setups vorgenommen werden, protokolliert und in einer Konfigurationsdatei gespeichert. Diese Konfigurationsdatei ist für das automatisierte Setup notwendig.

Um das Setup im RECORD-Modus zu starten, muss es mit dem Parameter **/r** aufgerufen werden. Der Aufruf des Setups lautet dann wie folgt:

Authention.exe /r

Dies führt dazu, dass im Windows-Verzeichnis die erwähnte Konfigurationsdatei entsteht. Sie heißt **Setup.iss** und enthält alle Informationen, die für eine Ausführung des Setups im SILENT-Modus notwendig sind. Alternativ kann diese Datei auch in einem benutzerdefinierten Verzeichnis erstellt werden. Dies wird ebenfalls mit Hilfe von Übergabeparametern definiert. Der Aufruf des Setups könnte daher wie folgt lauten:

Authention.exe /r /f1"C:\Setup.iss"

Der Parameter /f1 gibt an, wo sich die Konfigurationsdatei befindet bzw. wo sie erstellt werden soll.

An dieser Stelle ist es wichtig, dass zwischen dem Parameter **/f1** und dem danach anzugebenden Pfad kein Leerzeichen steht. Es wird empfohlen, für die Konfigurationsdatei einen absoluten Pfad zu verwenden und den Pfad in Anführungszeichen einzuschließen.

3.3 SILENT-Modus

Im SILENT-Modus werden keine Setup-Dialoge angezeigt. Alle notwendigen Informationen werden aus der im RECORD-Modus erstellten Konfigurationsdatei entnommen.

Während der Installation im NORMAL-Modus können Token-Treiber installiert werden. Dies ist im SILENT-Modus nicht möglich, da es sich bei den jeweiligen Treiber-Paketen um herstellerabhängige Softwareinstallationen handelt, die nicht der Kontrolle des Setups von Authention unterliegen.

Der Aufruf des SILENT-Modus erfolgt mit folgenden Parametern:

Authention.exe /s /f1"C:\Setup.iss"

Der Parameter **/s** startet das Setup im SILENT-Modus. Die Verwendung von **/f1** ist analog zum RECORD-Modus und gibt den Pfad und den Namen der Protokoll-Datei an, die während der Aufzeichnung erstellt wurde.

Wurde wie empfohlen am Ende des Setups ein Neustart durchgeführt, wird dieser Neustart im SILENT-Modus ohne Nachfrage vollzogen.

Optional kann der Parameter **/f2** angegeben werden. Dieser bewirkt, dass eine Protokolldatei benutzerdefiniert erstellt wird. Standardmäßig wird diese genauso benannt wie die Konfigurationsdatei. Sie entsteht auch im gleichen Verzeichnis, in dem sich die Konfigurationsdatei befindet. Um den Namen oder den Pfad der Protokolldatei zu ändern, kann das Setup von Authention beispielsweise mit den folgenden Parametern aufgerufen werden:

Authention.exe /s /f1"C:\Setup.iss" /f2"D:\Silent.log"

Analog zum Parameter **/f1** ist es an dieser Stelle wichtig, dass zwischen dem Parameter **/f2** und dem danach anzugebenden Pfad kein Leerzeichen steht.

Es wird dringend empfohlen, für die Protokolldatei einen absoluten Pfad zu verwenden und den Pfad in Anführungszeichen einzuschließen.

Anhand der Protokolldatei lässt sich ermitteln, ob das Setup im SILENT-Modus erfolgreich durchgeführt wurde. Die Protokolldatei einer erfolgreichen Durchführung im SILENT-Modus sollte in etwa wie folgt aussehen:

[Application]
Name=Authention
Version=2.1
Company=digitronic
Lang=0409

[ResponseResult]
ResultCode=0

Ist der **ResultCode** gleich Null, wurde das Setup erfolgreich durchgeführt. Die folgende Übersicht gibt Anhaltspunkte über mögliche Fehlerursachen, wenn der Wert ungleich Null ist.

3.3.1 ResultCodes

Code	Bedeutung
0	Es ist kein Fehler aufgetreten.
-1	Allgemeiner Fehler
-2	Ungültiger Modus
-3	Für eine Durchführung im SILENT-Modus wurden in der Konfigurationsdatei erforderliche Daten nicht gefunden.
-4	Es steht nicht genügend Speicherplatz zur Verfügung.
-5	Die angegebene Datei existiert nicht.
-6	Die Konfigurationsdatei kann nicht geschrieben werden.
-7	Die Protokolldatei kann nicht geschrieben werden.
-8	Ungültiger Pfad zur Konfigurationsdatei
-9	Kein gültiger Listentype (String oder Number)
-10	Ungültiger Datentyp
-11	Es ist ein unbekannter Fehler während des Setups aufgetreten.
-12	Dialogfelder können nicht angezeigt werden.
-51	Das Verzeichnis kann nicht angelegt werden.
-52	Auf das Verzeichnis oder die Datei kann nicht zugegriffen werden.
-53	Auf das Verzeichnis oder die Datei kann nicht zugegriffen werden.

Tabelle 3.1: Resultcodes von automatisierten Setups

KAPITEL 4

4 Besonderheiten

4.1 Lizenzdatei

4.1.1 Lizenzdaten

Die Lizenzdatei von Authention ist optionaler Bestandteil des Setups. Sie enthält sowohl den Namen des Lizenzinhabers (**Lizenznehmer**) als auch den Lizenzcode (**Lizenzschlüssel**). Beide Teile zusammen bilden die Lizenz. Die Eingabe der Lizenz während der Installation ist erforderlich, um die Komponenten von Authention installieren zu können.

Die Lizenz kann manuell im entsprechenden Setup-Dialog eingetragen werden. Zur Vereinfachung besteht die Möglichkeit, dass die Lizenz automatisch vom Setup aus der Lizenzdatei eingelesen wird. Dazu ist es notwendig, dass die Lizenzdatei "Authention.txt" heißt und sich im gleichen Verzeichnis wie das Setup von Authention befindet. Ist das der Fall, wird die Lizenz automatisch im Lizenzdialog eingetragen. Eine manuelle Eingabe ist in diesem Fall unnötig. Die Lizenzdatei muss dazu folgenden Aufbau haben:

Lizenznehmer: Hans Wurst

Lizenzschlüssel: 7DDA2547-9E441BF7-3D5DAAA3-FB177861

Wichtig ist, dass die beiden Zeilen mit den Worten "Lizenznehmer" und "Lizenzschlüssel" beginnen und dass die jeweiligen Werte danach mit Doppelpunkt und anschließendem Leerzeichen von diesen Worten abgetrennt sind. Andernfalls kann die Lizenz nicht korrekt aus der Lizenzdatei ermittelt werden.

Werden in der Lizenzdatei mehrere Zeilen gefunden, die potentielle Lizenzdaten enthalten, so werden die zuletzt gefundenen Werte verwendet.

4.1.2 Standart Token

In der Lizenzdatei kann zusätzlich der gewünschte Standard-Token ausgewählt werden. Dies ist der Token, der während der Standard-Installation von Authention als zu verwendender Token eingerichtet wird.

Die entsprechende Lizenzdatei sollte dann etwa wie folgt aussehen:

Lizenznehmer: Hans Wurst

Lizenzschlüssel: 7DDA2547-9E441BF7-3D5DAAA3-FB177861

Standard-Token: SmartCard mit TCOS 2.0 Betriebssystem

Wichtig ist, dass diese Zeile mit dem Wort "Standard-Token" beginnt und dass der entsprechende Wert danach mit Doppelpunkt und anschließendem Leerzeichen von diesem Wort abgetrennt ist. Andernfalls kann der Standard-Token nicht korrekt aus der Lizenzdatei ermittelt werden.

Werden in der Lizenzdatei mehrere Zeilen gefunden, die einen Standard-Token definieren, so wird die zuletzt gefundene Zeile verwendet.

Die folgende Liste zeigt alle Token, die als Standard-Token in der Lizenzdatei definiert werden können. In Klammern sind die Begriffe angegeben, an denen der jeweilige Token erkannt wird. Sind bei einem Token mehrere Begriffe angegeben, so müssen alle diese Begriffe in der entsprechenden Zeile vorkommen.

- Aladdin eToken
  ("aladdin" oder "etoken")
- GemSafe Xpresso
  ("gemsafe")
- Giesecke & Devrient StarKey
  ("giesecke" oder "devrient" oder "starkey")
- MARX CRYPTO-BOX (USB)
  ("crypto-box")
- MARX CrypToken 2000
  ("cryptoken" und "2000")
- MARX CrypToken M2048
  ("cryptoken" und "m2048")
- Omnisec Security Module USB
  ("omnisec" und
  ("sm" oder ("security" und "module")))
- SafeNet iKey 2000
  ("ikey" und "2000")
- SafeNet iKey 3000
  ("ikey" und "3000")
- SafeNet iKey 4000
  ("ikey" und "4000")
- Siemens SmartCard
  ("siemens")
- SmartCard mit CardOS 2.04 Betriebssystems
  ("cardos" und "2.04")
- SmartCard mit CardOS 4.3 Betriebssystems
  ("cardos" und "4.3")
- SmartCard mit TCOS 2.0 Betriebssystems
  ("tcos")
- Speicherkarte mit Baltech-Kartenleser
  ("baltech")
- Wechseldatenträger

Groß- bzw. Kleinschreibung wird ignoriert. Die hier angegebene Reihenfolge entspricht der Suchreihenfolge.
Wird beispielsweise die Zeile

Standard-Token: MARX CrypToken 2000 oder Aladdin eToken PRO

in der Lizenzdatei gefunden, so wird als Standard-Token **Aladdin eToken PRO** angenommen.

In den folgenden Fällen wird **Wechseldatenträger** als Standard-Token angenommen:

- Die Lizenzdatei wurde nicht gefunden.
- Die Lizenz-Datei enthält keine Zeile, die mit "Standard-Token" beginnt.
- Der in der Lizenzdatei angegebene Token konnte durch keinen der oben genannten Begriffe identifiziert werden.

Der Setup-Dialog, der zur Entscheidung zwischen Standard- und erweitertem Setup auffordert, zeigt an, welcher Token als Standard-Token angenommen wird.

Abbildung 3.1: Installationsvariante und –pfad wählen

4.1.3 Baltech Parameter

Weiterhin können in der Lizenzdatei die folgenden Parameter angegeben werden. Diese beschränken sich ausschließlich auf den Token "Speicherkarte mit Baltech-Kartenleser". Sie sind für die korrekte Durchführung des Setups nicht zwingend erforderlich, ermöglichen jedoch eine weiterführende Konfiguration des Kartenlesers von Baltech.

Die Parameter sind voneinander unabhängig.

Wichtig ist, dass die folgenden Zeilen mit dem jeweiligen Wort beginnen und dass die entsprechenden Werte danach mit Doppelpunkt und anschließendem Leerzeichen von den Worten abgetrennt sind. Andernfalls können die Parameter nicht korrekt aus der Lizenzdatei ermittelt werden.

Hier ein Beispiel für alle möglichen Parameter:

Baltech-Konfiguration: 2F B0 C3 30 D2 FD BA 12 3D…

Baltech-Protokollschlüssel: B4 2D 12 81 DF 1A 56 9F 23 …

Baltech-Modus: 1

Baltech-Maximallänge-PIN: 8

Baltech-Maximallänge-Benutzername: 20

Baltech-Maximallänge-Kennwort: 20

Die Parameter "Baltech-Konfiguration" und "Baltech-Protokollschlüssel" enthalten hexadezimal kodierte Werte.

Mit dem "Baltech-Modus" kann die Verwendung des Tokens auf die Logon-Komponente eingeschränkt werden (1). In diesem Fall wird zusätzlich der Speicherplatzbedarf auf dem Token minimiert. Standardmäßig (0) können alle Komponenten Daten auf dem Token speichern.

Die Parameter für die Maximallängen der PIN, des Benutzer-namens und des Kennwortes sind Zahlenwerte, die die Anzahl der möglichen Zeichen entsprechend beschränken.

4.2 Installation von Token Treibern

Das Setup von Authention unterstützt die automatische Installation von Token-Treibern. Diese Treiber-Pakete müssen während der Installation von Authention im gleichen Verzeichnis wie das Setup vorhanden sein – ähnlich wie die Lizenzdatei.

4.2.1 Externe Token Treiber

Für die folgenden Token sind auf der Homepage von digitronic (www.digitronic.net) Treiber-Pakete downloadbar, die automatisch während der Installation von Authention gestartet werden können:

- Aladdin eToken
  ("Aladdin eToken.msi")
- GemSafe Xpresso
  ("GemSafe Libraries.exe")
- Giesecke & Devrient StarKey
  ("SafeSign-Identity-Client-2.2.0-admin.exe ")
- MARX CrypToken M2048 (RaakSign)
  ("SafeSign-Identity-Client-2.2.0-admin.exe")
- SafeNet iKey 2000
  ("Rainbow iKey 2000.exe", "Rainbow iKey.exe")
- SafeNet iKey 3000
  ("SafeSign-Identity-Client-2.2.0-admin.exe")
- SafeNet iKey 4000
  ("SafeNet iKey 4000.exe", "IKEYDRVR.MSI")
- Siemens SmartCard
  ("Siemens SmartCard.exe")

In Klammern sind die Namen der Treiber-Pakete angegeben. Werden diese Pakete umbenannt, werden sie nicht gefunden. Eine automatische Treiber-Installation wäre damit ausgeschlossen.

Sind mehrere Treiber-Pakete angegeben, werden diese in der angegebenen Reihenfolge gestartet.

digitronic ist stets bemüht, die aktuellsten Treiber zur Verfügung zu stellen. Dennoch sollten die aktuellsten Treiber vom jeweiligen Token-Hersteller direkt bezogen werden.

digitronic übernimmt keine Gewährleistung für die Funktionalität der Treiber oder für etwaig entstehende Schäden am PC oder am Token.

Die Treiber-Pakete werden unmittelbar nach dem Kopieren der Authention-Dateien gestartet. Die Installation von Authention wird erst dann fortgesetzt, wenn alle gewählten Treiber-Setups wieder beendet wurden. Sie starten in alphabetischer Reihenfolge der Token-Bezeichnungen.

Einige Treiber-Pakete erwarten einen abschließenden Neustart. Dieser darf jedoch **nicht** durchgeführt werden, da zu diesem Zeitpunkt die Installation von Authention noch nicht vollständig abgeschlossen ist. Wird zu diesem Zeitpunkt ein Neustart durchgeführt, wird das Setup abgebrochen. Während dieses Abbruchs werden alle kopierten Dateien entfernt und alle vorgenommenen Änderungen am System rückgängig gemacht. Wird dieser Abbruch nicht komplett durchgeführt, weil das Betriebssystem zu schnell beendet wird, ist das Ergebnis eine fehlerhafte Authention-Installation.

Um dies zu vermeiden wird dringend empfohlen, das System erst nach Abschluss des Authention-Setups neu zu starten und die eventuelle Aufforderung zum Neustart eines Treiber-Pakets zu ignorieren.

Treiber-Pakete werden nur bei der Installation und im Wartungsmodus "Ändern" und auch nur im NORMAL- bzw. im RECORD-Modus gestartet. Während eines SILENT-Setups werden keine Treiber-Pakete gestartet.

4.2.2 Integrierte Token Treiber

Neben den externen Token-Treibern besitzt das Authention-Setup auch integrierte Treiber.

Für die folgenden Token kann das Authention-Setup Treiber installiere, ohne externe Treiber-Pakete starten zu müssen:

- MARX CRYPTO-BOX (USB)
- MARX CrypToken 2000
- MARX CrypToken M2048

Diese integrierten Treiber werden genauso behandelt, als wären es externe Treiber-Pakete. Sie werden nach dem Kopieren der Authention-Dateien installiert.

4.3 Einschränkungen

4.3.1 Token-Kombination

Authention unterstützt grundsätzlich die gleichzeitige Verwendung mehrerer Token. Dennoch wird empfohlen, sich auf einen Token bzw. auf eine Token-Art zu beschränken.

Einige technische Einschränkungen verhindern darüber hinaus die Verwendung von bestimmten Token-Kombinationen. Andere Kombinationen verursachen Probleme im Umgang mit den gewählten Token.

Das Setup unterscheidet hier die folgenden drei Fälle.

- Es gibt keine Komplikationen zwischen den gewählten Token.
- Es besteht die Möglichkeit von Komplikationen, wenn die Token in der gewählten Kombination eingesetzt werden.
- Der Einsatz der gewählten Token-Kombination ist aus technischen Gründen nicht möglich.

Sollte es technische Einschränkungen geben, ist die gewählte Token-Kombination unzulässig. Das Setup kann an dieser Stelle nicht fortgesetzt werden, bis die Kombination aufgehoben wird. Eine entsprechende Fehlermeldung wird im Setup angezeigt.

Die folgenden Kombinationen sind z.B. aus technischer Sicht unzulässig.

- mehrere Token der Firma MARX

Einige bekannte Kombinationen von Token, die in der Praxis nicht stabil zusammenarbeiten, werden im Folgenden dargestellt.

- Es sollten nicht gleichzeitig verschiedene Token der Firma SafeNet verwendet werden.
- Der Token "Siemens SmartCard" sollte nicht in Verbindung mit anderen PKCS#11-Token verwendet werden.
- Token der Firma GemSafe sollten nicht mit "SafeNet iKey3000" oder "Giesecke und Devrient StarSign Token" kombiniert werden.
- Bei der Kombination der Token "SafeNet iKey 4000" und "Speicherkarte mit Baltech-Kartenleser" funktioniert der Token "Speicherkarte mit Baltech-Kartenleser" nicht zuverlässig.

Werden solche Kombinationen erkannt, gibt das Setup eine Warnung aus, die auf mögliche Probleme hinweist.

Darüber hinaus wird Ihr System nach bereits installierten Token-Treibern durchsucht, um ebenfalls auf mögliche Token-Kombinationen hinzuweisen, die problematisch sind.

4.3.2 Initialisierbare Token während der Installation

Nicht alle Token, die während der Installation ausgewählt werden können, können auch während des Setups konfiguriert werden. Dies hängt von den folgenden Kriterien ab:

- Der Treiber für den Token ist bereits installiert oder der Treiber für den Token wurde während der Installation von Authention installiert, benötigt jedoch keinen Neustart und kann sofort verwendet werden.
- Die Initialisierung des Tokens während der Installation von Authention wurde von digitronic erfolgreich getestet.

Aufgrund dieser Kriterien ist eine Konfiguration der folgenden Token während der Installation möglich:

- GemSafe Xpresso
- MARX CRYPTO-BOX (USB)
- MARX CrypToken 2000
- MARX CrypToken M2048
- SafeNet iKey 4000
- SmartCard mit TCOS 2.0 Betriebssystem
- Omnisec Security Module USB
- Wechseldatenträger

Token, die der Token-Liste manuell hinzugefügt wurden, können grundsätzlich nicht während der Installation konfiguriert werden.

4.4 Aktualisierung von Version 2.0.X

Das Setup unterstützt generell die Aktualisierung älterer Authention-Versionen. Dabei werden die folgenden Fälle unterschieden:

- Aktualisierung von Version 1.x
- Aktualisierung von Version 2.0.x
- Aktualisierung von Version 2.1.x

4.4.1 Aktualisierung von Version 1.X

Eine Aktualisierung von diesen Versionen wird nicht unterstützt. Wird das Setup in diesem Fall ausgeführt, wird Authention ohne jegliche Beachtung der vorhandenen Authention-Version installiert. Dadurch wird die bestehende Installation unbrauchbar.

In diesem Fall sollte die ältere Version komplett deinstalliert und anschließend die neue Version installiert werden.

4.4.2 Aktualisierung von Version 2.0.X

Eine Aktualisierung dieser Version ist grundsätzlich möglich. Dabei müssen die folgenden Dinge beachtet werden:

- Verwendung spezieller Token für Logon
- Verwendung von Einzelsetups für neue Komponenten

Wird eine solche Version vorgefunden, lässt das Setup nur eine einzige Wartungsoperation zu: Aktualisieren.

Abbildung 3.2: Aktualisierung älterer Versionen

Dabei werden die Installationen aller installierten Authention-Komponenten an die Version 2.1.x angepasst.

Anders als beim herkömmlichen Aktualisieren werden in diesem Fall auch einige Änderungen an der Registry vorgenommen. Die jeweiligen Programmeinstellungen der Komponenten bleiben davon jedoch unberührt.

Wird der damals verwendete Token-Manager gefunden, wird dieser deinstalliert. Als Ersatz wird die Client-Komponente des Token Management Systems im StandAlone-Modus installiert.

4.4.3 Verwendung spezieller Token für Logon

Die Logon-Komponente unterstützte bisher zusätzlich zu den genannten Token, die auch von anderen Authention-Komponenten verwendet wurden, auch einige spezielle Lesegeräte. Diese speziellen Lesegeräte können mit dem Setup der neuen Authention-Version 2.1.x nicht mehr installiert werden.

Nach der Aktualisierung von Version 2.0.x können diese Geräte nach wie vor benutzt werden. Nur die Installation dieser Geräte wird durch das neue Setup nicht mehr unterstützt. Für die Verwendung solcher Lesegeräte ist daher die Installation des letzten Setups der Version 2.0.x notwendig. Anschließend kann diese Version mit dem Setup der Version 2.1.x aktualisiert werden.

4.4.4 Verwendung von Einzelsetups für neue Komponenten

Vor der Veröffentlichung der Version 2.1.x von Authention wurden für die drei neuen Komponenten **Crypted Group Share**, **Extended Device Block** und **Token Management System** Einzelsetups als Vorab-Version ausgegeben. Diese Setups stellten Erweiterungen der bestehenden Authention-Installation dar und konnten nur installiert werden, wenn Authention bereits installiert war.

Anwender, die Authention Version 2.0.x und eine oder mehrere Vorab-Versionen installiert haben, können diese insgesamt vier Installationen mit einer Aktualisierung von Version 2.1.x vereinen. Dabei werden die Dateien aller Installationen aktualisiert und Einträge in der Softwareliste des Betriebssystems angepasst. Danach ist in der Softwareliste nur noch Authention Version 2.1.x zu finden.

Wird die manuelle Deinstallation der vier Installationen bevorzugt, müssen zuerst die Einzelsetups der neuen Authention-Komponenten und danach die bisherige Authention-Version deinstalliert werden.

4.4.5 Aktualisierung von Version 2.1.X

Eine Aktualisierung dieser Version wird vollständig und ohne Einschränkungen unterstützt.

4.5 Protokollierung

Das Setup von Authention verfügt über eine eigene Protokollierung. Die Protokolldatei heißt Authention.log und entsteht im gleichen Verzeichnis, in dem sich das Setup befindet.

Die Protokolldatei wird bei jedem Start des Setups neu erstellt bzw. überschrieben, wenn Sie bereits existiert, und enthält Daten zur Ausführung interner Abläufe. Darüber hinaus werden dabei alle Benutzerauswahlen und –eingaben protokolliert und können gegebenenfalls daraus gewonnen werden.

Die Protokolldatei dient einzig und allein dem Zweck, fehlerhafte Installationen aufzudecken und das Setup damit zu verbessern. Es sind keine Daten enthalten, die dem Endanwender von Nutzen sein können.
Sicherheitskritische Eingaben, wie beispielsweise das Passwort der Logon-Daten, werden nicht protokolliert.

Das Protokoll wird standardmäßig immer erstellt. Es kann durch Aufruf des Setup mit dem Parameter /nolog deaktiviert werden. Der folgende Aufruf würde also keine Protokolldatei während des Setups erzeugen:

Authention.exe /nolog

Der Parameter /nolog kann mit allen anderen Parametern kombiniert werden. Er ist also auch bei der Erstellung sowie bei der Ausführung eines Silent-Setups anwendbar.

A ANHANG

A Abbildungsverzeichnis

ANHANG B

B Tabellenverzeichnis