DIGITTRADE

Smartcard Manager 2

Benutzerhandbuch
User Manual

Version: 1.13
13.08.2020

Sicherheitshinweise

BITTE LESEN SIE DIE ANLEITUNG SORGFÄLTIG UND FOLGEN SIE DEN ANWEISUNGEN.

Der DIGITTRADE Smartcard Manager 2 sollte nur in einer absolut sicheren Umgebung verwendet werden. Wir raten daher bei der Verwendung zu einem vom Netzwerk getrennten und sicher aufbewahrtem, virenfreien Rechner mit Zugriffsschutz vor Unbefugten.

Inhaltsverzeichnis

Allgemeine Erläuterungen

DIGITTRADE Smartcard Manager 2

Der DIGITTRADE Smartcard Manager 2 ermöglicht Ihnen einen zentralen Überblick über Ihre gesamten DIGITTRADE High Security Festplatten, Smartcards und kryptografischen Schlüssel. Mit dieser umfangreichen Verwaltungssoftware können Sie diese High Security Festplatten komplett erfassen. Durch die Darstellung einer Unternehmensstruktur lassen sich Mitarbeiter, Abteilungen und Standorte zu den jeweiligen Informationen zuordnen. Damit können Sie die Festplatten und Smartcards den jeweiligen Mitarbeitern sowie den jeweiligen Abteilungen hinzufügen. Bereits vorhandene Informationen können aktualisiert werden.

Zudem erhalten Sie die Möglichkeit, Ihre Smartcards direkt am PC zu verwalten. Dabei können die Smartcards synchronisiert, kryptografische Schlüssel neu erstellt, geändert und gelöscht, sowie die Smartcard-PIN geändert werden.

Hinweis: *Beachten Sie, dass bei 8-maliger Fehleingabe der PIN die Smartcard unwiderruflich zerstört wird. Nach korrekter Eingabe wird der Zähler wieder zurückgesetzt.*

Shortcuts und Symbole

Shortcuts:
Zur einfachen Bedienung des Smartcard Manager 2 können Sie die folgenden Shortcuts verwenden.

[Strg] + [W]	*Besitzer hinzufügen:* Drücken Sie die Taste „Strg“ („Ctrl“ bei amerikanischen Tastaturen) und den Buchstaben „W“ gleichzeitig, um zum Menüpunkt „Besitzer hinzufügen“ zu gelangen.
[Strg] + [E]	*Smartcard hinzufügen:* Drücken Sie die Taste „Strg“ („Ctrl“ bei amerikanischen Tastaturen) und den Buchstaben „E“ gleichzeitig, um zum Menüpunkt „Smartcard hinzufügen“ zu gelangen.
[Strg] + [R]	*Festplatte hinzufügen:* Drücken Sie die Taste „Strg“ („Ctrl“ bei amerikanischen Tastaturen) und den Buchstaben „R“ gleichzeitig, um zum Menüpunkt „Festplatte hinzufügen“ zu gelangen.

Symbolerläuterung:


Eingabe bestätigen


Eingabe verwerfen


Fenster schließen


hinzufügen


zurück


Element löschen


bearbeiten


Krypto-Schlüssel sperren


Smartcard hinzufügen


Karte auslesen, Krypto-Schlüssel in der Datenbank hinzufügen


AES-Schlüssel auf Smartcard kopieren


Kartenlesegerät neu einlesen


Festplatte hinzufügen

1. Installation

1.1 Systemanforderungen

Betriebssystem:	Windows Vista®, Windows® 7, Windows® 8, Windows® 10
Prozessor:	*Mindestens:* x86-Prozessor: 1,0 GHz oder x64-Prozessor: 1,4 GHz
Arbeitsspeicher:	*Mindestens:* 512 MB RAM
Software:	*Mindestens:* Treiber für den Administrator-Token (beiliegend auf der CD) Microsoft® SQL Server 2012 Express LocalDB Microsoft® .NET Framework 4.5 *Empfohlen:* PDF-Reader

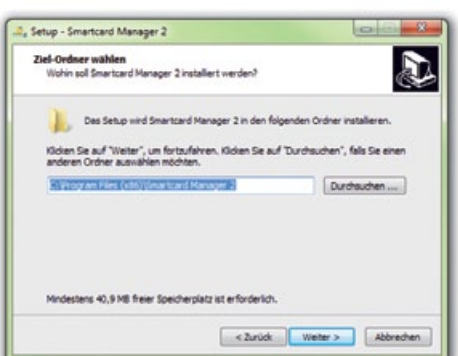
Zur Installation des DIGITTRADE Smartcard Manager 2 werden mindestens 100 MB freier Festplattenspeicherplatz benötigt.

1.2 Installation der Software

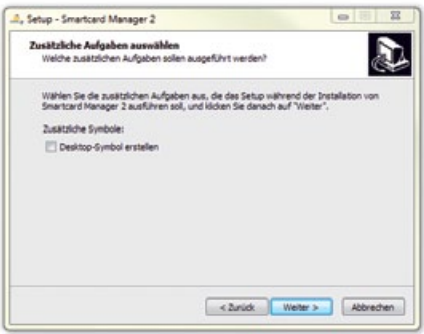
Starten Sie den DIGITTRADE Smartcard Manager 2 Installer (DIGITTRADE Smartcard Manager 2 Installer.msi). Es erscheint ein Fenster mit einer Sprachauswahl. Wählen Sie Ihre Sprache und klicken Sie auf „OK“.

Zum Fortfahren der Installation lesen Sie die Bedingungen der Lizenzvereinbarung und stimmen diesen zu. Klicken Sie anschließend auf „Weiter“.

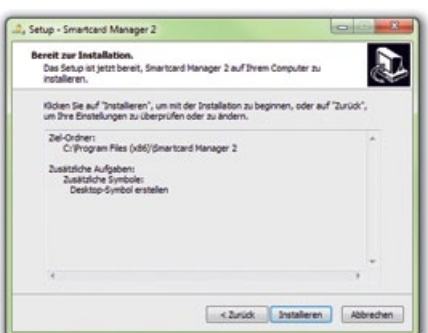
Wählen Sie Ihren Zielpfad für die Installation der Software aus und klicken Sie dann auf „Weiter“.



Wenn Sie ein Desktop-Symbol erstellen wollen, klicken Sie bitte auf „Desktop-Symbol erstellen“und danach auf „Weiter“.



Klicken Sie nun auf „Installieren“.



Klicken Sie zum Abschluss der Installation auf „Fertig stellen“.

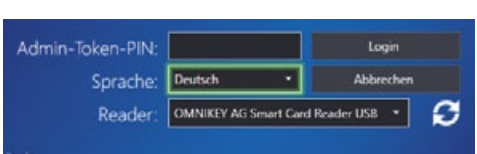
Achten Sie vor dem ersten Start der Software darauf, dass die Treiber für den Administrator-Token installiert wurden.

Hinweis: *Der DIGITTRADE Smartcard Manager 2 Installer erkennt Ihre Spracheinstellungen im System automatisch (Deutsch oder Englisch).*

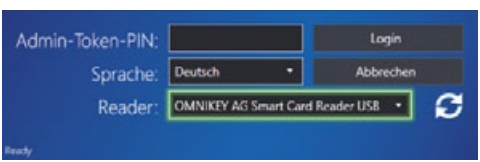
2. Starten der Software

2.1 Erstmaliger Start der Software

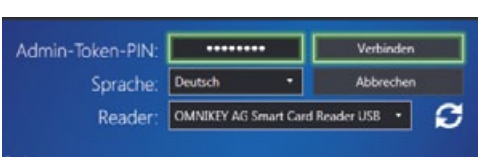
Sobald Sie die Software zum ersten Mal starten, wählen Sie zuerst Ihre Sprache.



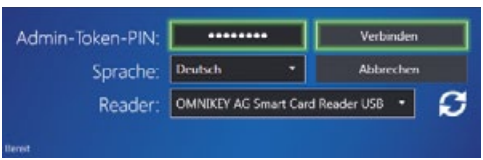
Vergewissern Sie sich, dass Ihr Smartcard Reader ausgewählt ist. Klicken Sie, wenn nötig, auf ↻.



Verbinden Sie den Token mit dem DIGITTRADE Smartcard Manager 2, stecken Sie hierzu den Token in einen freien USB-Steckplatz. Danach geben Sie Ihre Admin-Token-PIN ein und wählen „Verbinden“.



Jetzt können Sie sich einloggen. Dazu geben Sie die Admin-Token-PIN nochmals ein und klicken dann auf „Verbinden“. Mit Klick auf „Abbrechen“ schließen Sie das Programm.

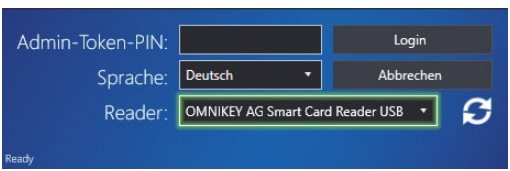


Hinweis: *Sollte der Admin-Token bereits vorher bei einer Installation des Smartcard Manager 2 verwendet worden sein, so kann auf die alte Installation nach diesem Schritt nicht mehr zugegriffen werden.*

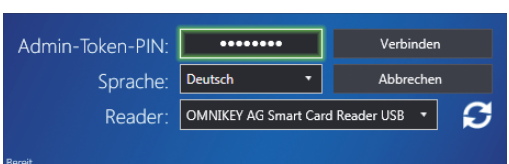
Beachten Sie außerdem, dass aus Sicherheitsgründen der Token während der gesamten Zeit, in der Sie die Software verwenden, mit dem System verbunden sein muss.

2.2 Regulärer Start der Software

Zur Authentifizierung stecken Sie bitte den Token in einen freien USB-Steckplatz. Vergewissern Sie sich, dass Ihr Smartcard Reader ausgewählt ist.



Geben Sie Ihre Token-PIN ein und klicken Sie auf „Verbinden".

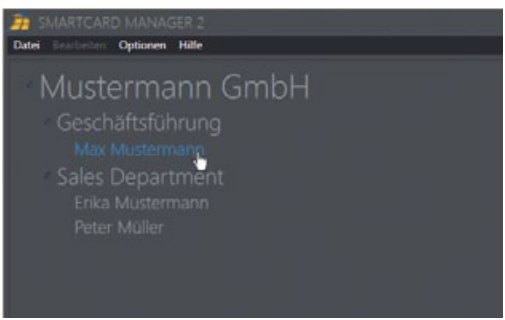


Hinweis: *Achten Sie aus Sicherheitsgründen äußerst darauf, dass der Token ununterbrochen mit dem System verbunden bleibt, während Sie die Software verwenden.*

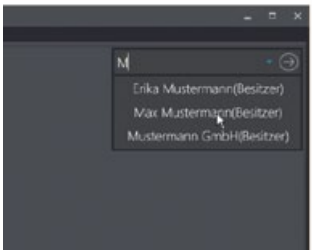
3. Elemente suchen und auswählen

3.1 Besitzer suchen und auswählen

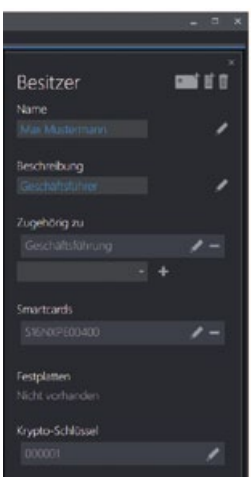
Besitzer sind mit einem Klick auf den Namen über die Liste auf der linken Seite anwählbar.



Optional kann die Suche verwendet werden, welche sich oben rechts im Listenfeld befindet. Mit Klick in das Suchfeld öffnet sich eine neue Liste, aus welcher der gewünschte Besitzer ausgewählt werden kann. Der Name des gesuchten Besitzers kann auch in das Suchfeld eingegeben werden. Um die Besitzer-Detailansicht zu öffnen, wird die Suchauswahl mit dem Rechtspfeil bestätigt.

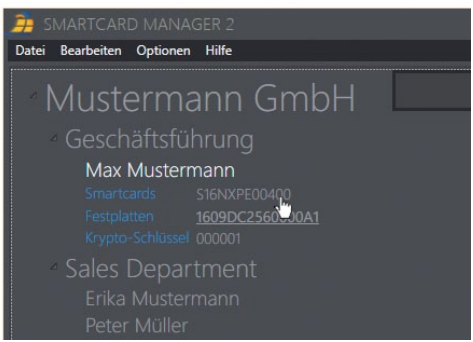


Beide Möglichkeiten öffnen die Besitzer-Detailansicht, in welcher die eingetragenen Informationen einsehbar sind und Änderungen vorgenommen werden können.

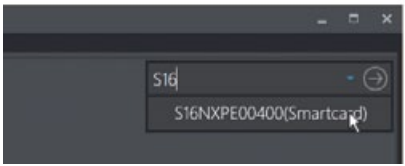


3.2 Smartcards suchen und auswählen

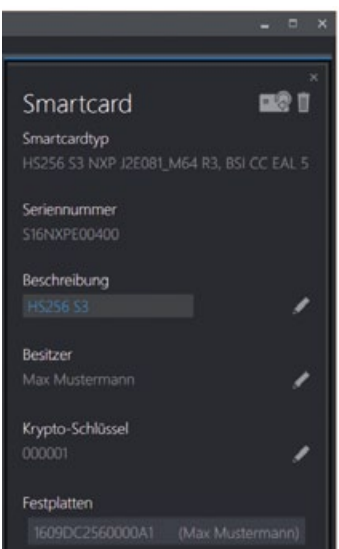
Sofern der Besitzer bekannt ist, können Smartcards über Ihren Besitzer ausgewählt werden. Klicken Sie hierzu auf den entsprechenden Namen des Besitzers in der Liste auf der linken Seite.



In der Liste unterhalb des Namens stehen alle diesem Besitzer zugeordneten Smartcards. Mit Klick auf die Seriennummer der gewünschten Smartcard öffnet sich die Smartcard-Detailansicht. Optional kann die Smartcard auch über die Eingabe ihrer Seriennummer in das Suchfeld gefunden werden. Nach korrekter Auswahl der Seriennummer kann die Smartcard-Detailansicht durch Klick auf den Rechtspfeil geöffnet werden.

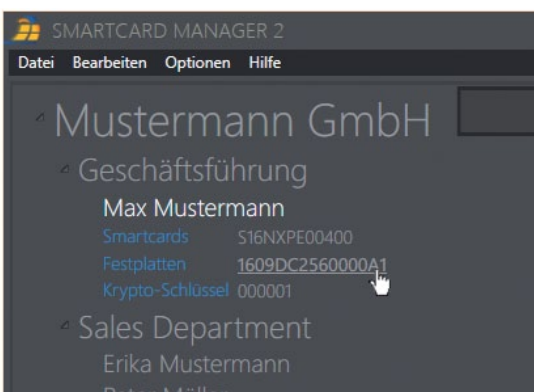


In der Smartcard-Detailansicht können Sie alle eingetragenen Informationen einsehen und Änderungen vornehmen.

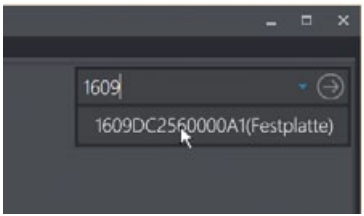


3.3 Festplatte suchen und auswählen

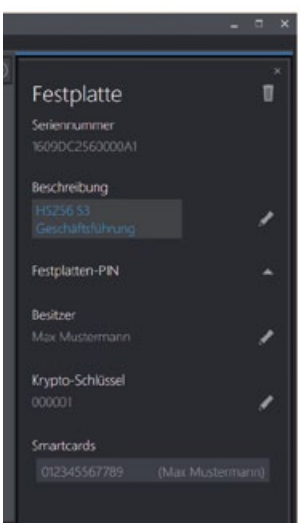
Sofern der Besitzer bekannt ist, können Festplatten über Ihren Besitzer ausgewählt werden. Klicken Sie hierzu auf den entsprechenden Namen des Besitzers in der IListe auf der linken Seite. In der Liste unterhalb des Namens befinden sich alle diesem Besitzer zugeordneten Festplatten. Mit Klick auf die gewünschte Festplatte öffnet sich die Festplatten-Detailansicht.



Optional kann die Festplatte auch über die Eingabe ihrer Seriennummer in das Suchfeld gefunden werden. Nach korrekter Auswahl der Seriennummer kann die Festplatten-Detailansicht durch Klick auf den Rechtspfeil geöffnet werden.

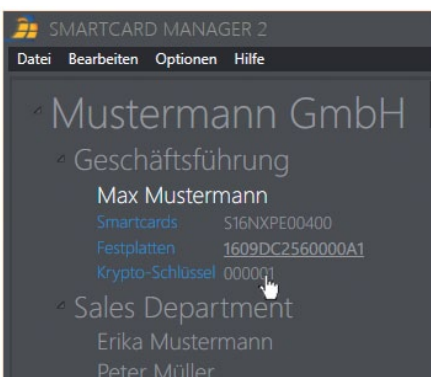


In der Festplatten-Detailansicht können Sie alle eingetragenen Informationen einsehen und Änderungen vornehmen.

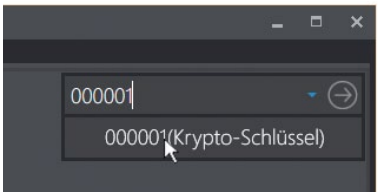


3.4 Krypto-Schlüssel suchen und auswählen

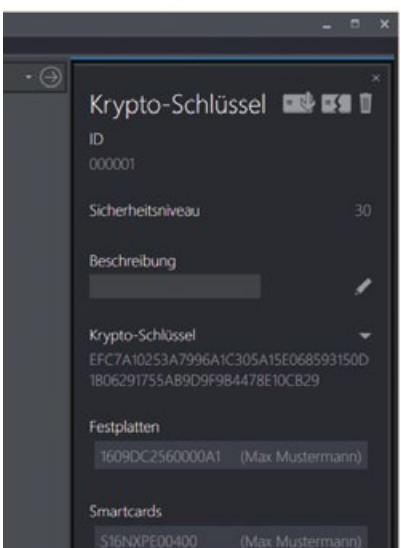
Sofern der Besitzer bekannt ist, können Krypto-Schlüssel über Ihren Besitzer ausgewählt werden. Klicken Sie hierzu auf den entsprechenden Namen des Besitzers in der Liste auf der linken Seite. In der Liste unterhalb des Namens befinden sich alle vom Besitzer verwendeten Krypto-Schlüssel. Mit Klick auf die gewünschten Krypto-Schlüssel öffnet sich die Krypto-Schlüssel-Detailansicht.



Optional kann der Krypto-Schlüssel auch über die Eingabe seiner Nummer in das Suchfeld gefunden werden. Nach korrekter Auswahl der Nummer kann die Krypto-Schlüssel-Detailansicht durch Klick auf den Rechtspfeil geöffnet werden.



Die Detailansicht zeigt alle den Krypto-Schlüssel betreffenden Informationen.

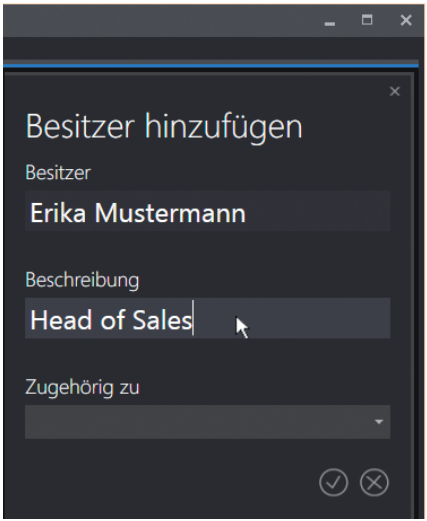


4. Besitzer

4.1 Besitzer hinzufügen

Zum Eintragen eines neuen Besitzers klicken Sie über den Reiter „Datei“ auf das Feld „Besitzer hinzufügen“

In der folgenden Detailansicht tragen Sie die Angaben zum neuen Besitzer ein. Die Beschreibung der Person (z.B. Position im Unternehmen) ist optional. Im Feld „Zugehörig zu“ können Sie den Besitzer einem übergeordneten Element (z.B. Besitzer oder Gruppe) zuordnen. Wenn Sie den neuen Besitzer als Hauptelement erstellen wollen, lassen Sie dieses Feld einfach frei. Ihre Eingaben können Sie nun mit ⓥ bestätigen oder mit ⓧ verwerfen. Es besteht die Möglichkeit, eine organigramm-ähnliche Struktur anzulegen.

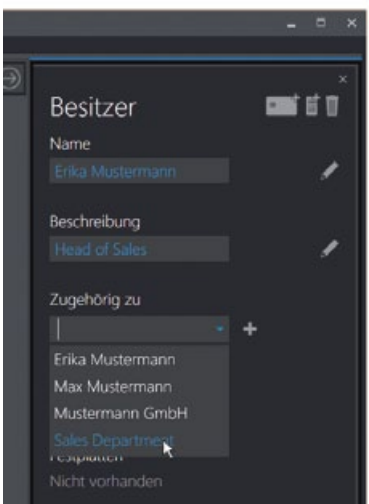


Hinweis: *Bevor ein Besitzer einem Hauptelement zugeordnet werden kann, muss dieses Hauptelement bereits existieren. Ein Hauptelement kann nicht dem Unterbesitzer als weiteren Unterbesitzer zugeordnet werden, da diese Verknüpfung bereits besteht. Ein Besitzer kann mehreren Hauptelementen zugeordnet werden.*

4.2 Besitzer-Zugehörigkeit nachtragen

Wählen Sie den zu bearbeitenden Besitzer aus (siehe „3.1 Besitzer suchen und auswählen“).

Im Feld „Zugehörig zu“ der Besitzer-Detailansicht wählen Sie das gewünschte Hauptelement aus und bestätigen Sie Ihr Auswahl mit +.

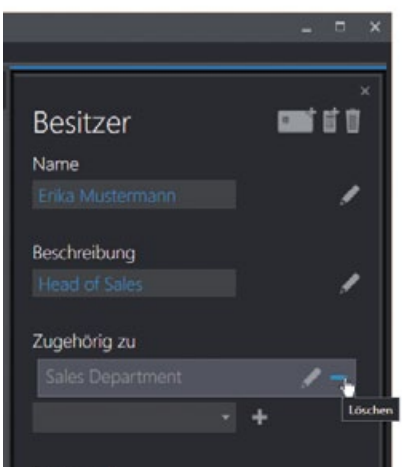


Hinweis: *Ein Besitzer kann mehrere Zugehörigkeiten haben.*

4.3 Hauptelementverknüpfung entfernen

Wählen Sie den zu bearbeitenden Besitzer aus (siehe „3.1 Besitzer suchen und auswählen“).

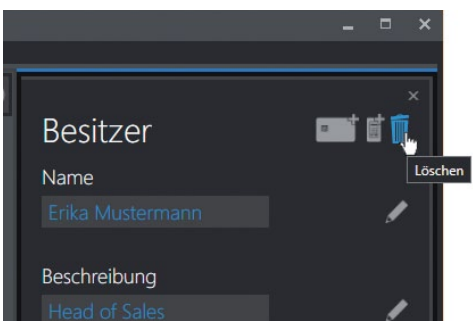
In der Liste „Zugehörig zu“ sehen Sie alle zugeordneten Hauptelemente. Die Verknüpfungen können mit Klick auf das Zeichen − einzeln gelöscht werden. Im Dialog „Besitzerverbindung“ können Sie den Löschvorgang mit ⓥ bestätigen oder mit ⓧ abbrechen.



4.4 Besitzer entfernen

Wählen Sie den zu löschenden Besitzer aus (siehe „3.1 Besitzer suchen und auswählen“).

Klicken Sie in der Besitzer-Detailansicht das Symbol an. Im folgenden Dialog „Besitzer löschen“ wählen Sie unbedingt aus, wem die Smartcards und Festplatten des gelöschten Besitzers zugeordnet werden. Bestätigen Sie mit ⓥ.

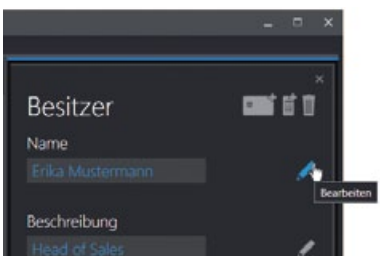


Hinweis: *Die einem gelöschten Besitzer zugeordneten Festplatten und Smartcards werden ebenfalls gelöscht, sofern kein neuer Besitzer in der Liste ausgewählt wird. Alle Besitzer, die dem entfernten Besitzer untergeordnet waren, müssen anschließend neu zugeordnet werden.*

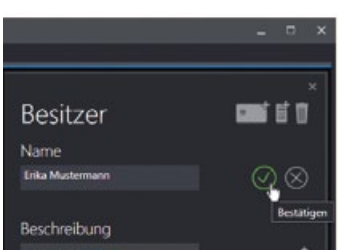
4.5 Namen ändern

Wählen Sie den zu bearbeitenden Besitzer aus (siehe „3.1 Besitzer suchen und auswählen“).

Klicken Sie auf das Symbol neben dem Namensfeld.



Klicken Sie in das Namensfeld, ändern Sie den Besitzernamen und bestätigen Sie die Änderung mit ⓥ.

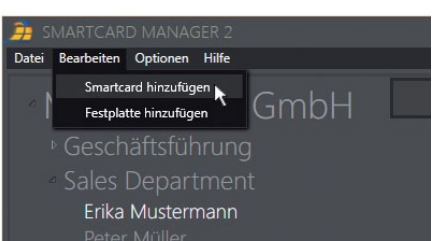


5. Smartcard

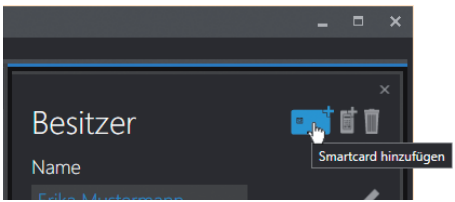
5.1 Smartcard hinzufügen

Stecken Sie die gewünschte Smartcard in den Smartcard Reader. Wählen Sie einen Besitzer aus.

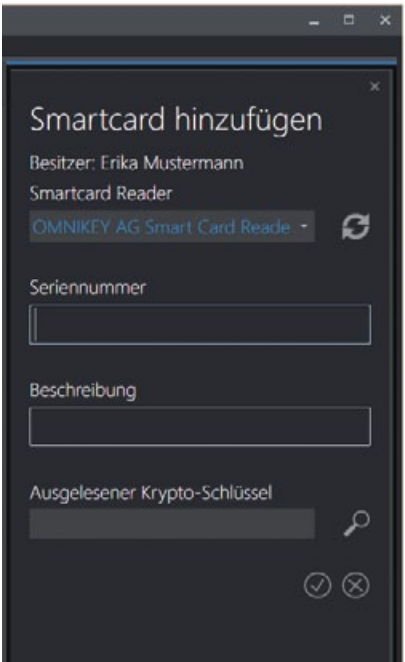
Klicken Sie anschließend auf „Bearbeiten“ ▸ „Smartcard hinzufügen“.



Alternativ können Sie in der Besitzer-Detailansicht auf das Symbol klicken.



Wählen Sie den verwendeten Smartcard Reader im Feld „Smartcard Reader“ aus. Klicken Sie dazu auf das Symbol . Optional kann die Smartcard im entsprechenden Feld beschrieben werden. Geben Sie die Seriennummer ein und klicken Sie auf das Symbol neben dem Feld „ausgelesener AES-Schlüssel“. Geben Sie die 8-stellige PIN der verwendeten Smartcard ein. Bestätigen Sie mit . Bestätigen Sie in der Detailansicht Ihre Angaben folgend mit . Der Krypto-Schlüssel wird, sofern bereits vorhanden, automatisch zugeordnet.

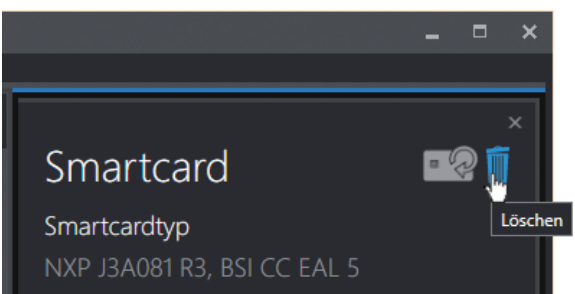


Hinweis: *Sind noch keine Daten auf der Smartcard vorhanden, müssen diese zunächst erstellt werden. Hierzu werden Sie von der Software aufgefordert. Bestätigen Sie diese Aufforderung mit ✓, geben Sie die PIN erneut ein und bestätigen Sie diese mit ✓.*

5.2 Smartcard löschen

Wählen Sie die zu löschende Smartcard aus (siehe „3.2 Smartcards suchen und auswählen“).

In der Smartcard-Detailansicht klicken Sie auf das Symbol und bestätigen mit ✓.



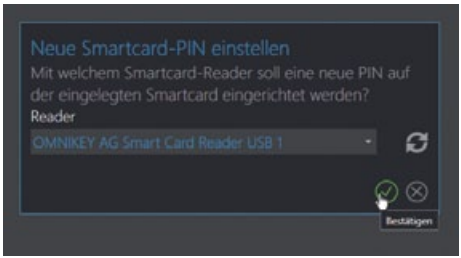
5.3 Smartcard-PIN ändern

Stecken Sie die gewünschte Smartcard in den Smartcard Reader.

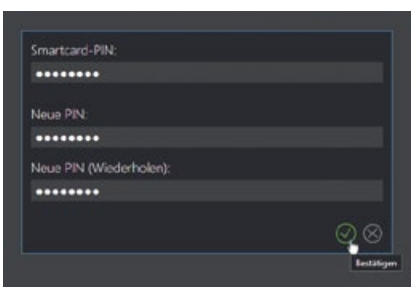
Wählen Sie die zu bearbeitende Smartcard aus (siehe „3.2 Smartcards suchen und auswählen“).

Gehen Sie nun auf „Bearbeiten“ ▸ „PIN ändern“.

Wählen Sie im folgenden Dialogfenster den Smartcard Reader aus (ggf. mit ↻ aktualisieren), in dem sich die zu bearbeitende Smartcard befindet.



Nach Bestätigung durch ⓥ geben Sie die alte Smartcard-PIN und danach zwei Mal die neue Smartcard-PIN ein. Bestätigen Sie abermals mit ⓥ.

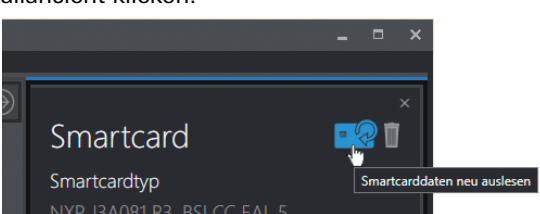


Hinweis: *Sollten Sie nicht wissen in welchem Smartcard Reader sich die zu bearbeitende Smartcard befindet, so empfiehlt es sich, alle zusätzlichen Smartcard Reader von dem PC zu trennen. Der Admin-Token muss jedoch weiterhin am PC verbleiben.*

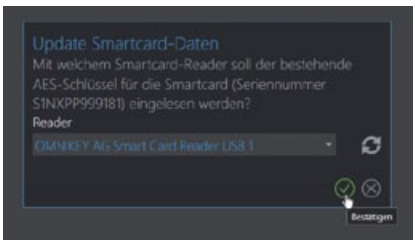
5.4 Smartcard mit Datenbank synchronisieren

Sollten die Informationen auf der Smartcard außerhalb des Smartcard Manager 2 geändert werden, so besteht die Möglichkeit die neuen Smartcard-Daten in die Datenbank des Smartcard Manager 2 zu übernehmen. Wählen Sie die gewünschte Smartcard aus (siehe 3.2 Smartcards suchen und auswählen) und gehen Sie auf „Bearbeiten“ ▸ „Daten einlesen“.

Optional können Sie auf das Symbol in der Smartcard-Detailansicht klicken.



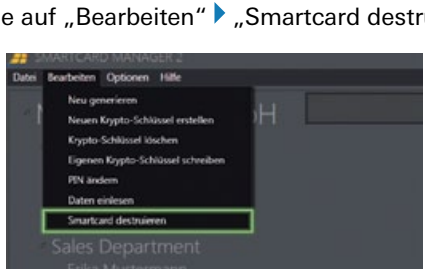
Wählen Sie im folgenden Dialogfenster den entsprechenden Smartcard Reader aus. Klicken Sie ggf. auf das Symbol ↻ und bestätigen Sie mit ✓. Es erscheint die Mitteilung „Neuer Schlüssel wurde zugeordnet“. Bestätigen Sie mit ✓.



5.5 Smartcard destruieren

Wählen Sie die zu bearbeitende Smartcard aus (siehe „3.2 Smartcards suchen und auswählen“).

Klicken Sie auf „Bearbeiten“ ▸ „Smartcard destruieren“.



Wählen Sie im Feld „Smartcard Reader“ den genutzten Smartcard Reader aus. Klicken Sie ggf. auf ↻ und bestätigen Sie mit ⓥ.

Hinweis: *Sollten Sie nicht wissen, in welchem Smartcard Reader sich die zu bearbeitende Smartcard befindet, so empfiehlt es sich, alle zusätzlichen Smartcard Reader von dem PC zu entfernen. Der Admin-Token muss jedoch weiterhin am PC verbleiben.*

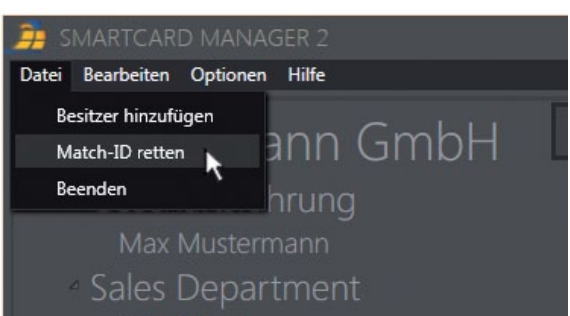
Die Smartcard wird bei diesem Vorgang unwiderruflich zerstört.

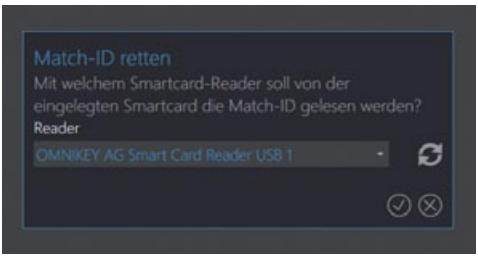
5.6 Match-ID retten

Damit Sie die Festplatte auch bei vergessener Geräte- und Smartcard-PIN sowie bei allen gesperrten Smartcards weiterhin sicher verwenden können, soll die Match-ID der alten Smartcard gerettet und auf eine neue Smartcard mit bekannter Smartcard-PIN und einem bereits generierten neuen Krypto-Schlüssel kopiert werden.

Nach der Formatierung kann die zugeordnete Festplatte mit dieser neuen Smartcard verwendet werden. Der Zugriff auf die alten Daten ist dabei nicht mehr möglich.

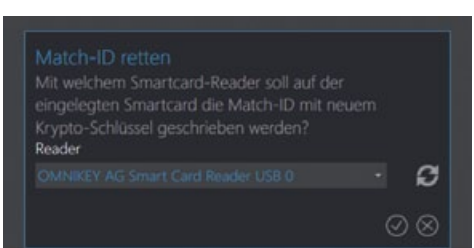
Legen Sie hierzu die Smartcard mit der zu rettenden Match-ID in einen Smartcard Reader ein und klicken Sie auf Datei ▸ Match-ID retten.

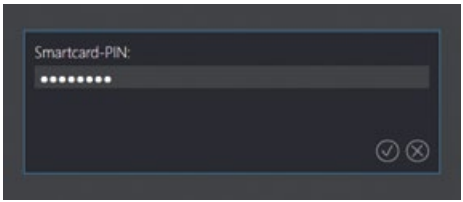




Wählen Sie nun den entsprechenden Smartcard Reader aus, in welchem sich die Smartcard befindet. Kicken Sie dazu gegebenenfalls auf . Bestätigen Sie Ihre Eingabe mit .

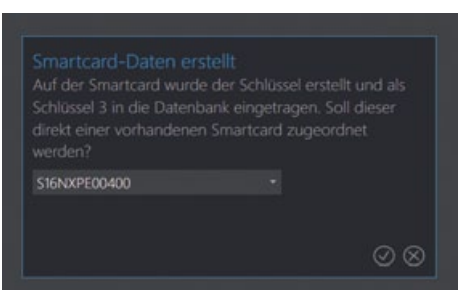
Entfernen Sie nun die alte Smartcard aus dem Reader und ersetzen Sie diese durch die neue Smartcard, auf welche die Match-ID kopiert werden soll. Wählen Sie erneut den entsprechenden Reader aus.





Authentifizieren Sie sich mit der Smartcard-PIN der neuen Smartcard.

Schließen Sie den Vorgang ab, indem Sie die Smartcard einer Vorhandenen zuordnen. Bestätigen Sie mit ⓥ. Danach ist es möglich, die zur alten Smartcard gehörige Festplatte mit der neuen Smartcard, wie ober beschrieben, zu verwenden.

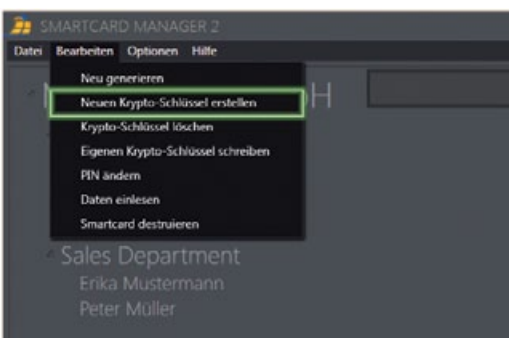


Hinweis: *Beachten Sie, dass der Zugriff auf die alten Daten dadurch nicht mehr möglich ist.*

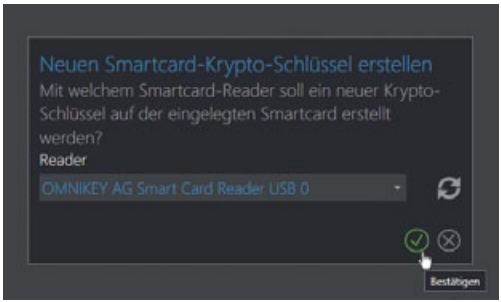
6. Kryptografischer Schlüssel

6.1 Neuen AES-Schlüssel erstellen

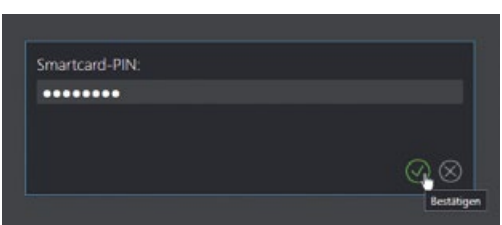
Stecken Sie die gewünschte Smartcard in den Smartcard Reader und wählen Sie diese Smartcard aus (siehe „3.2 Smartcards suchen und auswählen“). Klicken Sie auf „Bearbeiten“ ▸ „Neuen AES-Schlüssel erstellen“.



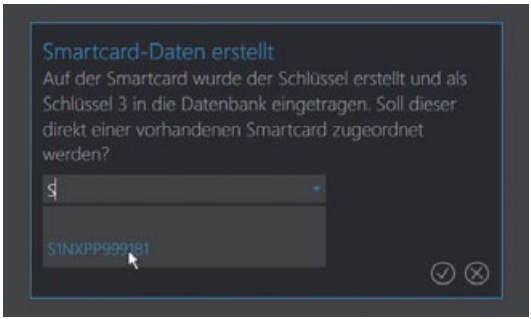
Wählen Sie den Smartcard Reader im entsprechenden Feld aus. Aktualisieren Sie gegebenenfalls mit Klick auf ↻ und bestätigen Sie Ihre Auswahl mit ✓.



Geben Sie die PIN der eingesteckten Smartcard ein und bestätigen Sie mit ⓥ.



Ordnen Sie den Krypto-Schlüssel einer im System vorhandenen Smartcard mit Klick in das entsprechende Feld zu und bestätigen Sie wieder mit ⓥ.



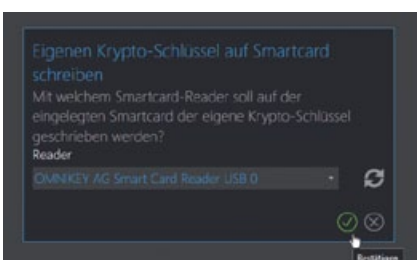
Hinweis: *Der neue Krypto-Schlüssel wird automatisch in der Datenbank mit einer neuen Identifikationsnummer hinterlegt.*

6.2 Eigenen AES-Schlüssel schreiben

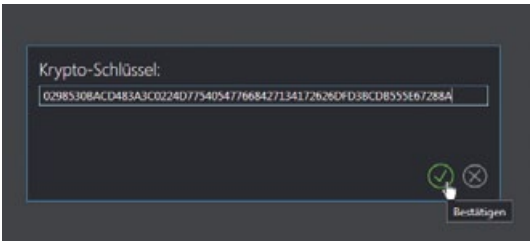
Stecken Sie die gewünschte Smartcard in den Reader und wählen Sie die entsprechende Smartcard aus (siehe „3.2 Smartcards suchen und auswählen“).

Gehen Sie nun auf „Bearbeiten“ ▸ „Eigenen AES-Schlüssel schreiben“.

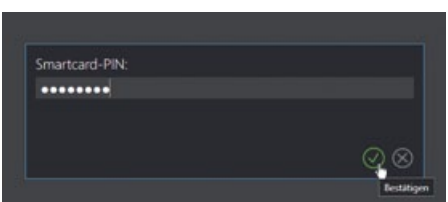
Wählen Sie den verwendeten Reader ggf. mit Klick auf ⟳ aus und bestätigen Sie mit ♡.



Geben Sie nun die 64-stellige Zeichenkette ein. Die Zeichen müssen hexadezimal eingegeben werden. Dies bedeutet, dass ausschließlich die Zahlen 0 bis 9 und die Buchstaben A bis F legitim sind, wobei Groß- und Kleinschreibung keine Rolle spielt. Sonderzeichen sind nicht erlaubt. Bestätigen Sie abschließend Ihre Eingabe mit ♡.



Geben Sie nun im folgendem Dialogfenster die PIN der eingesteckten Smartcard ein und bestätigen Sie mit ♡.



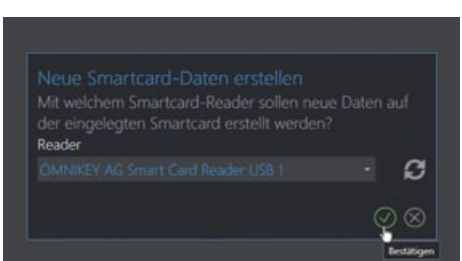
Hinweis: *Es wird dringend davon abgeraten, frei gewählte Zeichen zu verwenden. Diese Funktion sollten Sie nur verwenden, wenn Sie den* Krypto-Schlüssel *durch einen kryptogrisch sicheren Zufallszahlengenerator (RNG) generieren können. Sollten Sie nicht über einen solchen RNG verfügen, empfehlen wir die Verwendung der integrierten, zertifizierten RNGs der Smartcard. Folgen Sie hierzu dem Punkt „6.1 Neuen AES-Schlüssel erstellen“*

6.3 Smartcard neu generieren

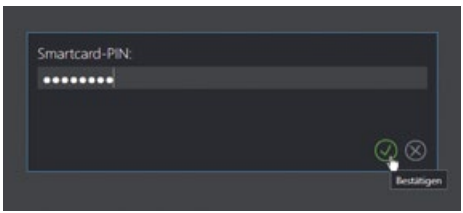
Stecken Sie die gewünschte Smartcard in den Reader und wählen Sie die entsprechende Smartcard aus (siehe „3.2 Smartcards suchen und auswählen“).

Klicken Sie auf „Bearbeiten“ ▸ „Neu generieren“.

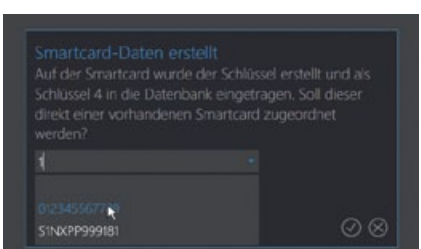
Wählen Sie nun den Smartcard Reader im entsprechenden Feld aus. Aktualisieren Sie gegebenenfalls mit Klick auf ↻ und bestätigen mit ✓.



Geben Sie die Smartcard-PIN ein und bestätigen Sie mit ✓.



Abschließend haben Sie die Möglichkeit die Auswahl der gewünschten Smartcard zu überprüfen und ggf. mit Klick in das entsprechende Feld zu ändern. Bestätigen Sie diesen Dialog mit ✓, um den Vorgang abzuschließen.

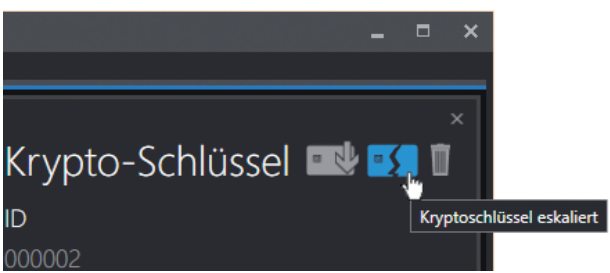


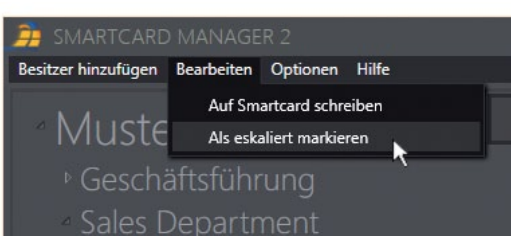
Hinweis: *Mit dieser Funktion werden neben einem neuen AES-Schlüssel auch alle weiteren Werte auf der Smartcard neu generiert.*

6.4 Kryptografischen Schlüssel als eskaliert markieren

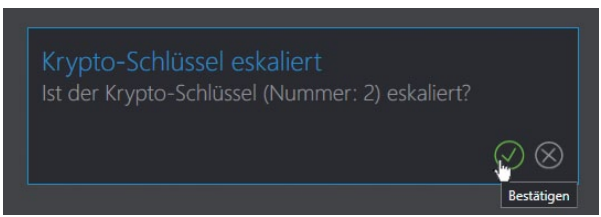
Stecken Sie die gewünschte Smartcard in den Reader und wählen Sie die entsprechende Smartcard aus (siehe „3.2 Smartcards suchen und auswählen“).

Anschließend können Sie auf in der Detailansicht klicken oder über „Bearbeiten“ ▸ „Als eskaliert melden“ das nächste Dialogfenster öffnen.





Bestätigen Sie dieses mit ⓥ, wird der Krypto-Schlüssel unwiderruflich markiert.

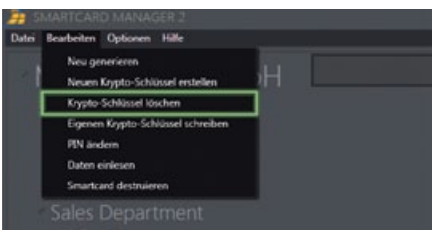


Hinweis: *Dieser Vorgang sollte sofort nach Verlust einer Smartcard durchgeführt werden. Der Krypto-Schlüssel wird dabei unwiderruflich als gefährdet markiert und sollte nicht weiter verwendet werden. Weiterhin sollten alle Smartcards und Festplatten, die diesen Krypto-Schlüssel verwenden, mit einem neuen Krypto-Schlüssel beschrieben werden.*

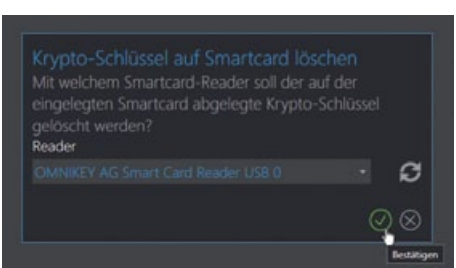
6.5 AES-Schlüssel von Smartcard löschen

Stecken Sie die gewünschte Smartcard in den Reader und wählen Sie die entsprechende Smartcard aus (siehe „3.2 Smartcards suchen und auswählen“).

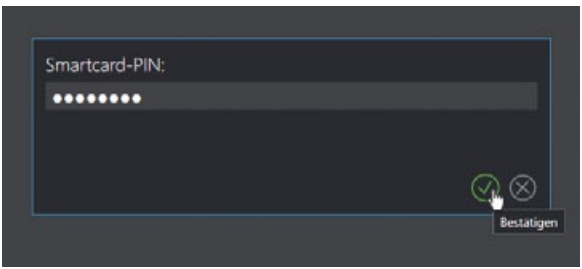
Klicken nun Sie auf „Bearbeiten“ ▸ „AES-Schlüssel löschen“.



Im folgenden Dialogfeld wählen Sie den Smartcard Reader aus. Klicken Sie wenn nötig auf ⟳ und bestätigen Sie mit ⓥ.



Geben Sie nun die PIN ein und bestätigen Sie abschließend mit ⓥ. Der alte Krypto-Schlüssel wird nun durch die automatische Vergabe eines neuen Schlüssels gelöscht.

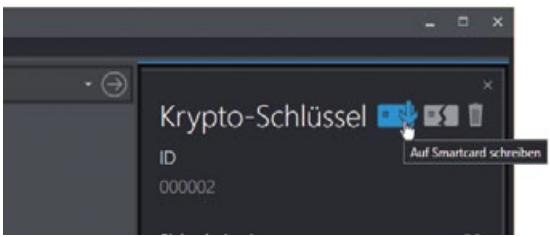


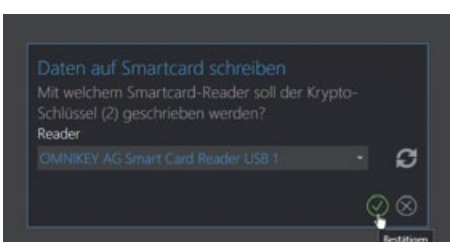
6.6 Kryptografischen Schlüssel kopieren

Stecken Sie die gewünschte Smartcard in den Reader und wählen Sie die entsprechende Smartcard aus (siehe „3.2 Smartcards suchen und auswählen“).

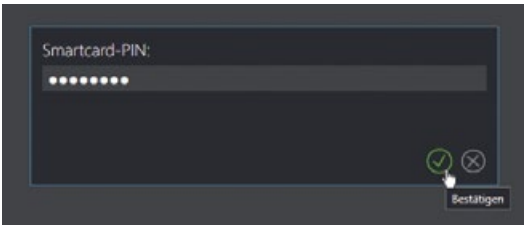
Wählen Sie den gewünschten Krypto-Schlüssel über den jeweiligen Benutzer oder durch die Eingabe in das Suchfeld aus (geben Sie 6 für Krypto-Schlüssel 000006 ein).

Klicken Sie auf und wählen Sie den Smartcard Reader im entsprechenden Feld aus. Aktualisieren Sie wenn nötig mit und bestätigen Sie mit ⓥ.

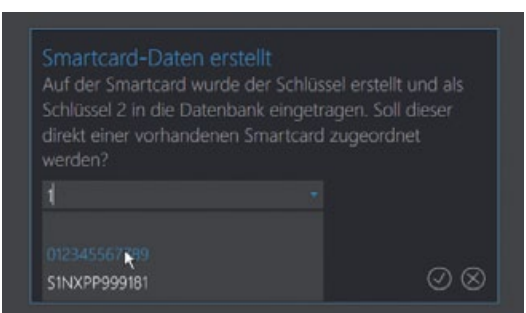




Geben Sie die entsprechende Smartcard-PIN ein und bestätigen Sie diese mit ⓥ.



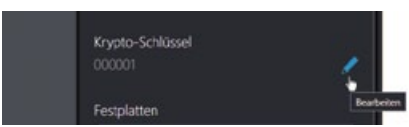
Sie können nun den Krypto-Schlüssel einer bereits vorhandenen Smartcard zuordnen und den Vorgangmit einem weiteren Klick auf ⓥ abschließen.

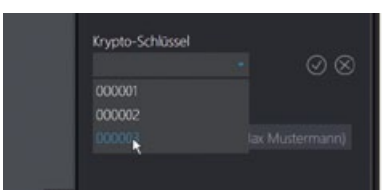


6.7 Smartcard neuen kryptografischen Schlüssel zuordnen (datenbankintern)

Stecken Sie die gewünschte Smartcard in den Reader und wählen Sie die entsprechende Smartcard aus (siehe „3.2 Smartcards suchen und auswählen“).

Klicken Sie auf ✎ neben dem Feld „Krypto-Schlüssel“ und wählen Sie aus der Liste, welche mit Klick in das Feld erscheint, den gewünschten Krypto-Schlüssel aus. Bestätigen Sie die Eingabe mit ⓥ.

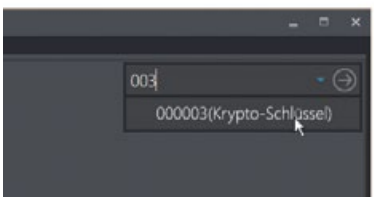




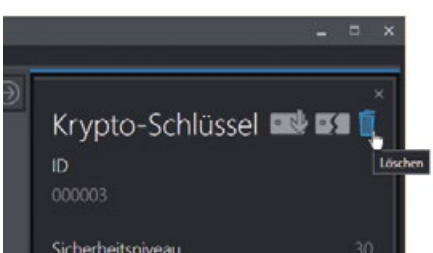
Hinweis: *Beachten Sie, dass der Krypto-Schlüssel dabei nur datenbankintern zugeordnet wird. Um den Krypto-Schlüssel auf die Smartcard zu kopieren, befolgen Sie den Punkt „6.6 Kryptografischen Schlüssel kopieren“.*

6.8 Kryptografischen Schlüssel aus Datenbank löschen

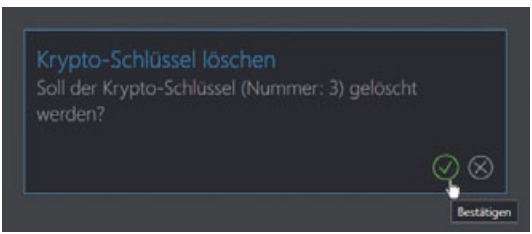
Wählen Sie den gewünschten Krypto-Schlüssel über die Suche (geben Sie „6“ ein für den Krypto-Schlüssel mit der Nummer 000006) aus.



In der Krypto-Schlüssel-Detailansicht klicken Sie auf 🗑 und bestätigen mit ⓥ.



Bestätigen Sie die Eingabe mit ⓥ.



Hinweis: *Beachten Sie, dass der Schlüssel keiner Festplatte oder Smartcard zugeordnet sein darf. Alle Verknüpfungen mit Besitzern, Smartcards und Festplatten müssen zuvor aufgelöst worden sein. Daher ist das Auswählen ausschließlich über die Suche möglich.*

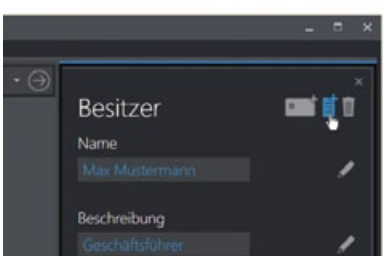
7. Festplatten

Hinweis: *Festplatten können mehreren Besitzern zugewiesen werden, welche dabei in Nutzungsberechtigte unterteilt werden können. Die Festplatte des Hauptbesitzers wird dabei fett und unterstrichen angezeigt, während bei weiteren Nutzungsberechtigten die Festplatte ohne Hervorhebung angezeigt wird.*

Eine Teilung erfolgt, sobald Besitzer mit einer Smartcard arbeiten, die den gleichen Krypto-Schlüssel besitzt wie die Festplatte des Hauptbesitzers.
Ist ein Teilen der Festplatte nicht erwünscht, muss mit unterschiedlichen Krypto-Schlüsseln gearbeitet werden. Dies wird auch empfohlen, um eine höchstmögliche Vertraulichkeit der Daten zu gewährleisten.

7.1 Festplatten hinzufügen

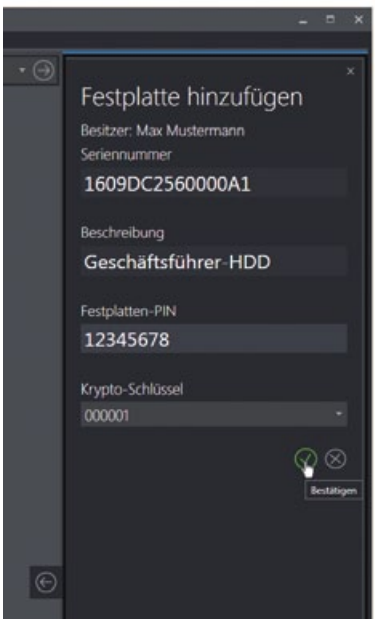
Um eine Festplatte hinzuzufügen, klicken Sie in der Detailansicht des gewünschten Besitzers auf .



Die Vergabe einer Beschreibung sowie Angabe der Festplatten-PIN sind optional.
Geben Sie nun die Seriennummer ein. Diese finden Sie auf

der Rück- der Festplatte sowie auf der Verpackung.

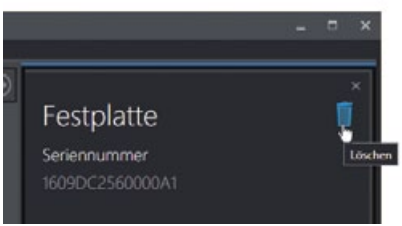
Wählen Sie den verwendeten Krypto-Schlüssel über die Liste aus und bestätigen Sie mit ⓥ.

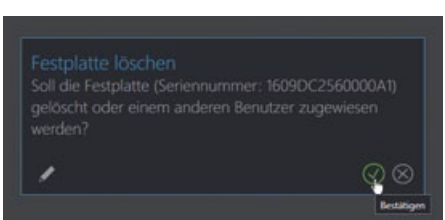


7.2 Festplatten entfernen

Wählen Sie die gewünschte Festplatte aus (siehe „3.3 Festplatte suchen und auswählen“).

In der Festplatten-Detailansicht klicken Sie auf 🗑 und bestätigen Sie mit ♡.



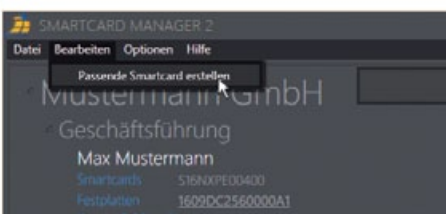


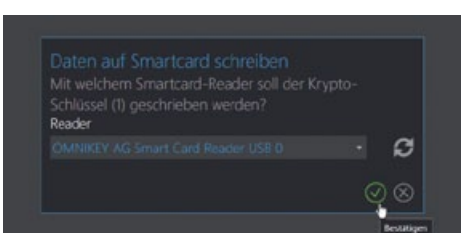
Hinweis: *Bei mehreren Besitzern bedeutet das Löschen der Festplatte über einen der beiden Besitzer das vollständige Löschen der gewählten Festplatte aus der Datenbank.*

7.3 Zur Festplatte passende Smartcard erstellen

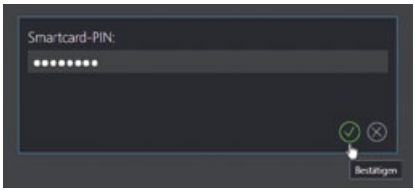
Wählen Sie die gewünschte Festplatte aus (siehe „3.3 Festplatte suchen und auswählen“) und stecken Sie die gewünschte Smartcard in den Reader.

Klicken Sie auf „Bearbeiten“ ▸ „Passende Smartcard erstellen“und wählen Sie den Smartcard Reader aus. Aktualisieren Sie wenn nötig mit ⟳.

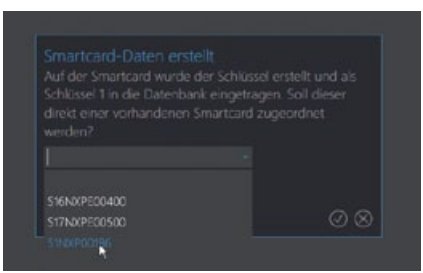




Geben Sie nun die Smartcard-PIN ein und bestätigen Sie mit ✓.



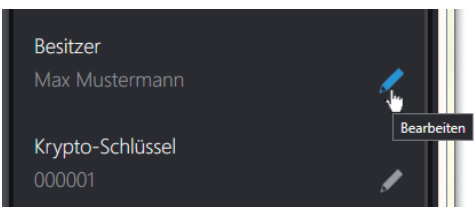
Sie haben nun die Möglichkeit, die Daten einer bereits vorhanden Smartcard zuzuordnen. Bestätigen Sie dann mit ⓥ.

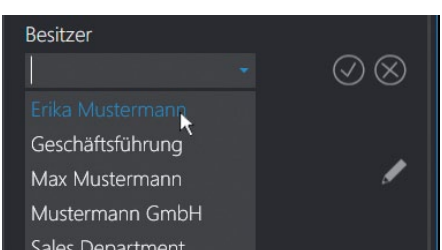


7.4 Festplatten-Besitzer ändern

Wählen Sie die gewünschte Festplatte aus („3.3 Festplatte suchen und auswählen“).

In der Festplatten-Detailansicht klicken Sie auf neben dem Besitzer und wählen Sie einen neuen Besitzer durch Klick auf das Feld aus der Liste aus. Bestätigen Sie mit .

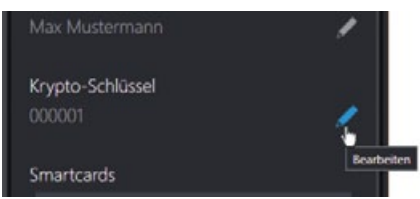


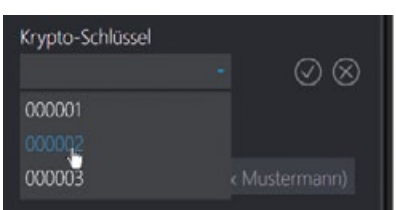


7.5 Festplatte neuen kryptografischen Schlüssel zuordnen (datenbankintern)

Wählen Sie die Festplatte aus („3.3 Festplatte suchen und auswählen“).

In der Festplatten-Detailansicht klicken Sie auf neben dem Krypto-Schlüssel. Wählen Sie einen neuen Krypto-Schlüssel aus der Liste und bestätigen Sie mit .





8. Backups

8.1 Hinweise zu Möglichkeiten der Erstellung und des Zurückspielens von Backups

Admin-Token:
Mit dem Admin-Token lassen sich Backups sowohl erstellen als auch zurückspielen. Dabei wird das Backup durch den Token verschlüsselt gespeichert.

Dies bedeutet jedoch auch, dass ein Zurückspielen des Backups bei Verlust des Tokens nicht möglich ist, da ein neuer Admin-Token eine andere Verschlüsselung benutzt. Um ein Zurückspielen des Backups trotz Verlust zu ermöglichen, wird ein seperat zu erwerbender Backup-Token benötigt.

Backup-Passwort:
Backups können auch ohne Token zurückgespielt werden, sofern bei Erstellung des Backups ein Passwort vergeben wurde. Lesen Sie hierzu mehr in „8.3 Datenbank-Backup mit eigenem Passwort erstellen“. Das Passwort ist weder auf bestimmte Zeichen noch auf eine Länge beschränkt, muss aber mindestens 1 Zeichen enthalten.

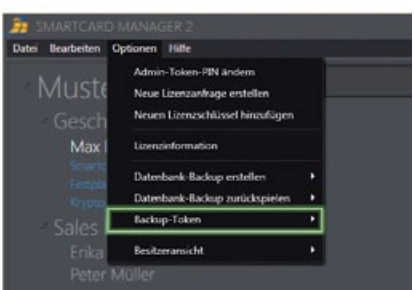
Da mittels Passwort erstellte Backups unsicherer sind, als mittels Token erstellte, wird dringend dazu geraten ein Passwort mit 8 Zeichen oder mehr zu wählen. Dabei sollte

auf die Verwendung von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen geachten werden.

Backup-Token:

Um Backups auch nach Verlust des Admin-Tokens zurückspielen zu können, wird zum Erwerb des Backup-Tokens geraten. Dieser stellt sicher, dass mittels Admin-Token erstellte Backups zurückspielbar sind, sollte der Admin-Token entwendet werden, verloren gehen oder beschädigt sein. Hierzu muss jedoch sicher gestellt werden, dass Admin-Token und der Backup-Token miteinandern verbunden sind. Folgen Sie hierzu der Anleitung in „".

Alleinige Aufgabe dieses Tokens ist es, mittels Admin-Token erstellte Backups zurückzuspielen. Jedoch können über Optionen ▸ Backup-Token Funktionen wie Backup-Token-PIN ändern, verbinden und Verbindung entfernen aufgerufen werden.



Allgemeiner Hinweis zu Backups: *Prinzipiell wird zur Erstellung eines Backups sowohl mittels Token als auch mittels Passwort geraten. So stellen Sie sicher, dass die Backups jederzeit einspielbar sind. Aufgrund des niedrigen Sicherheitsniveaus von mittels Passwort erstellten Backups, ist es empfehlenswert, eben dieses Backup auf mehrere DIGITTRADE High Security Festplatten zu hinterlegen.*

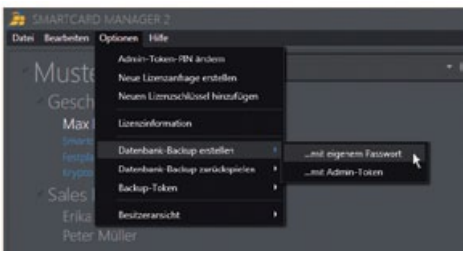
Beachten Sie, dass mittels Admin-Token erstellte Backups durch den Backup-Token nur einspielbar sind, wenn diese beiden Token vorher verbunden wurden.
Beachten Sie außerdem die Hinweise unter „8.4 Datenbank-Backup mit eigenem Passwort zurückspielen“, „8.5 Datenbank-Backup mit Admin-Token erstellen“ sowie „“. Erstellen Sie regelmäßig Backups, um Datenverlust zu umgehen.

8.2 Kontext zwischen Art der Erstellung und Möglichkeit der Einspielung eines Backups

Art des erstellten Backups	**Auswirkung auf Zurückspielen**
mittels Passwort	• nur mit entsprechendem Passwort
mittels unverknüpftem Admin-Token	• nur mit entsprechendem, unverknüpften Admin-Token (ggf. Verbindung entfernen)
mittels mit Backup-Token verknüpftem Admin-Token	• *bestehende Verknüpfung:* Backup kann sowohl von Admin-Token als auch Backup-Token zurückgespielt werden • *nach entfernter Verknüpfung:* Backup nur noch mit Backup-Token zurückspielbar; um mit Admin-Token zurückspielen zu können, müssen erneut entsprechender Admin- und Backup-Token miteinander verknüpft werden

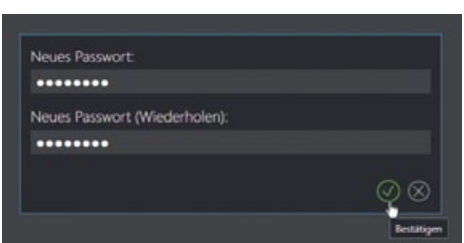
8.3 Datenbank-Backup mit eigenem Passwort erstellen

Klicken Sie auf „Optionen“ ▸ „Datenbank Backup erstellen“ ▸ „ … mit eigenem Passwort“.



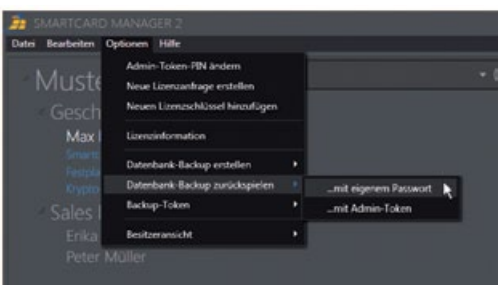
Wählen Sie nun einen Namen und einen Speicherort für die Backup-Datei und klicken Sie auf „Speichern“.

Vergeben Sie das gewünschte Passwort, wiederholen Sie dieses und bestätigen Sie die Eingabe mit ⓥ.



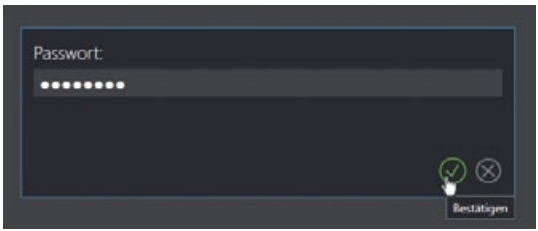
8.4 Datenbank-Backup mit eigenem Passwort zurückspielen

Zum Einspielen eines Backups mit eigenem Passwort benötigen Sie das Passwort, mit welchem dieses Backup erstellt wurde. Es ist nicht möglich, ein durch Token erstelltes Backup mit eigenem Passwort zurückzuspielen. Gehen Sie zunächst auf „Optionen“ ▸ „Datenbank Backup zurückspielen“ ▸ „ … mit eigenem Passwort“.



Im folgenden Dialogfeld können Sie ihr System nach dem Backup mit der Endung „.dtdb“ durchsuchen. Wählen Sie das gewünschte Backup aus und gehen Sie auf „Öffnen“.

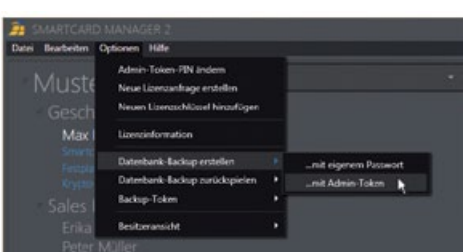
Geben Sie nun das Passwort ein, welches Sie bei der Erstellung des Backups vergeben haben und bestätigen Sie die Eingabe mit ⏎.



Hinweis: *Bitte beachten Sie, dass beim Einspielen des Backups alle aktuellen Daten vollständig durch die Backup-Daten ersetzt werden.*

8.5 Datenbank-Backup mit Admin-Token erstellen

Klicken Sie auf „Optionen“ ▸ „Datenbank Backup erstellen“ ▸ „ … mit Token“.



Wählen Sie nun einen Namen und Speicherort für die Backup-Datei und klicken Sie auf „Speichern“. Bestätigen Sie die Eingabe mit ⓥ.

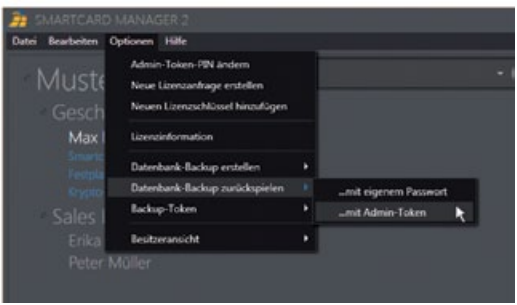
Hinweis: *Beachten Sie, dass das Datenbank-Backup an den Token gebunden ist. Bei Verlust oder Defekt des Tokens lässt sich das Backup auch mit neuem Token nicht zurückspielen.*

Um einen Verlust des Backups zu vermeiden, wird der Erwerb eines Backup-Tokens und eine Verknüpfung dessen mit Ihrem Admin-Token empfohlen. Mit verknüpftem Admin-Token erstellte Backups lassen sich sowohl mit verknüpftem Admin-Token als auch zusätzlich mit dem jeweiligen Backup-Token zurückspielen.

8.6 Datenbank-Backup mit Admin-Token zurückspielen

Das Einspielen eines Backups mittels Admin-Token ist nur möglich, wenn dieses Backup auch mit eben diesem Token erstellt wurde. Es ist nicht möglich ein mittels eigenem Passwort erstelltes Backup mit Token zurückzuspielen.

Gehen Sie zunächst auf „Optionen“ ▸ „Datenbank Backup zurückspielen“ ▸ „ … mit Token“.

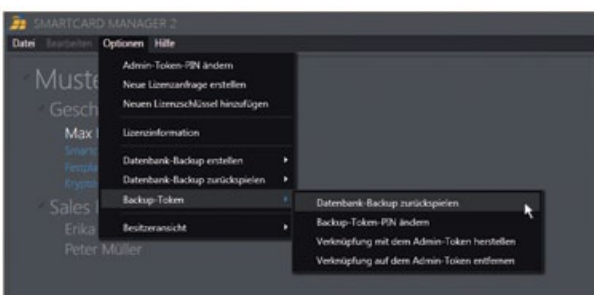


Im folgenden Dialogfeld können Sie Ihr System nach dem Backup mit der Endung „.dtdb“ durchsuchen. Wählen Sie das gewünschte Backup aus und gehen Sie auf „Öffnen“. Bestätigen Sie mit ⓥ.

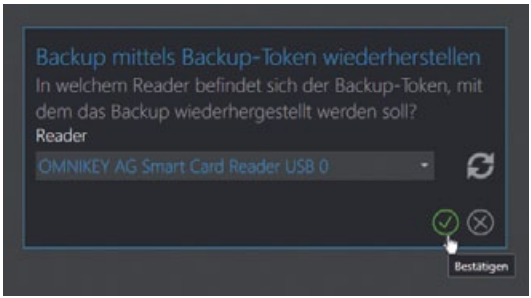
Hinweis: *Alle aktuellen Daten werden gelöscht, wenn das Datenbank-Backup zurückgespielt wird. Dabei ist es irrelevant, ob das Backup fehlerhaft ist oder nicht.*

8.7 Datenbank-Backup mittels Backup-Token zurückspielen

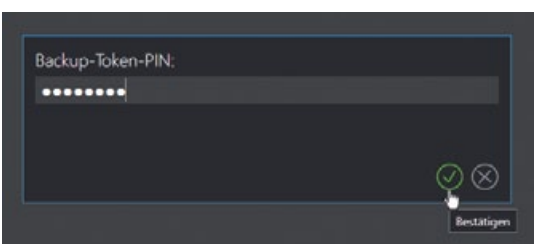
Diese Funktion lässt sich nur ausführen, sofern das Backup mit einem mit dem Backup-Token verknüpftem Admin-Token erstellt wurde. Gehen Sie über „Option“ ▸ „Backup-Token“ auf „Datenbank zurückspielen“.



Wählen Sie den Backup-Token im Smartcard Reader Feld, ggf. mit Klick auf ↻ aus und bestätigen Sie die Eingabe mit ✓.



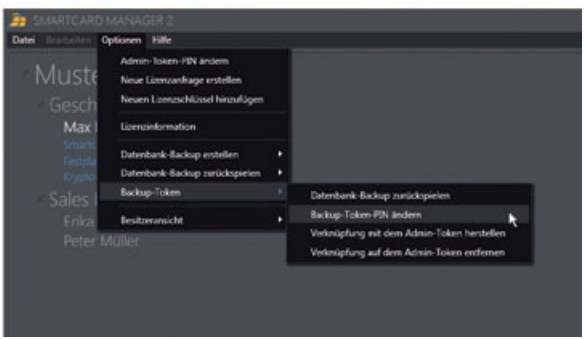
Geben Sie nun die PIN des Backup-Tokens ein und bestätigen Sie mit ⓥ.



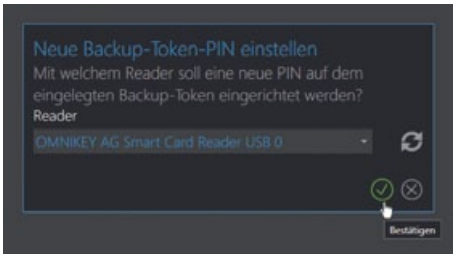
Durchsuchen Sie im darauf folgenden Fenster Ihr System nach dem Backup, welches Sie zuvor mit dem verknüpften Admin-Token erstellt haben. Nachdem Sie das Backup mit der Endung „.dtdb“ geöffnet haben, bestätigen Sie mit ⓥ.

8.8 Backup-Token-PIN ändern

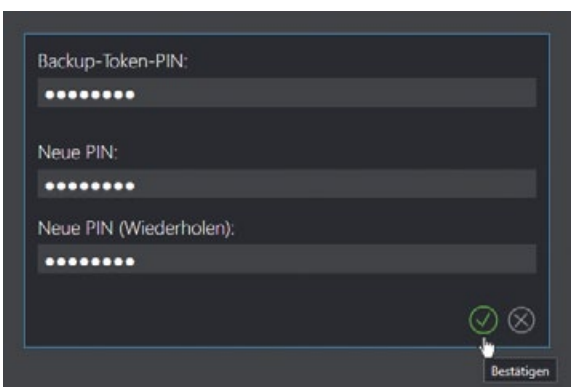
Gehen Sie über „Option“ ▸ „Backup-Token“ auf „Backup-Token-PIN ändern“.



Wählen Sie den Backup-Token im Smartcard Reader Feld, ggf. mit Klick auf ↻ aus und bestätigen Sie die Eingabe mit ✓.

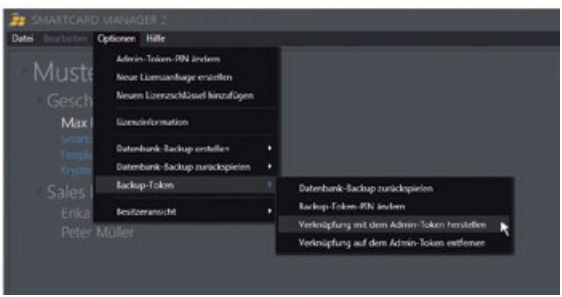


Geben Sie nun die PIN des Backup-Tokens ein. In die letzten beiden Felder geben Sie die gewünschte neue PIN ein. Bestätigen Sie nun mit ⓥ.

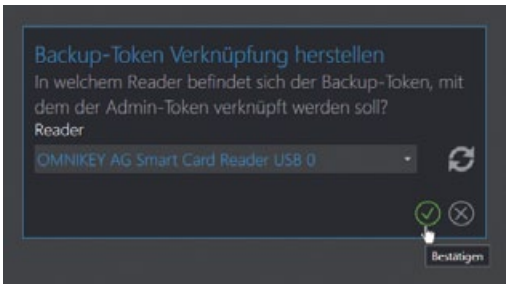


8.9 Verknüpfung mit dem Admin-Token herstellen

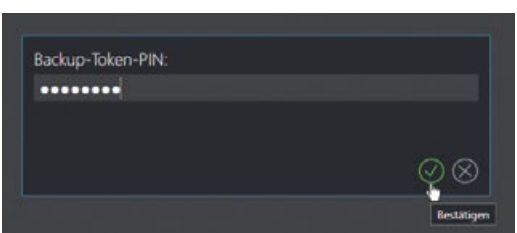
Gehen Sie über „Option“ ▸ „Backup-Token“ auf „Verknüpfung mit dem Admin-Token herstellen“.



Wählen Sie den Backup-Token im Smartcard Reader Feld ggf. mit Klick auf ⟳ aus und bestätigen Sie die Eingabe mit ⓥ.

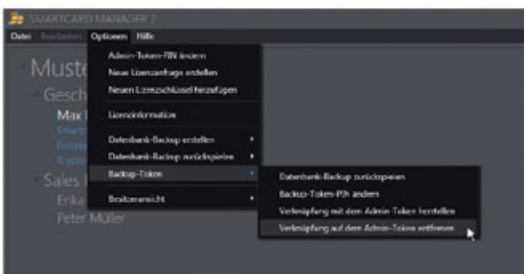


Geben Sie nun die PIN des Backup-Tokens ein und bestätigen Sie mit ⓥ.



8.10 Verknüpfung mit dem Backup-Token entfernen

Gehen Sie über „Option“ ▸ „Backup-Token“ auf „Verknüpfung mit dem Admin-Token entfernen“.

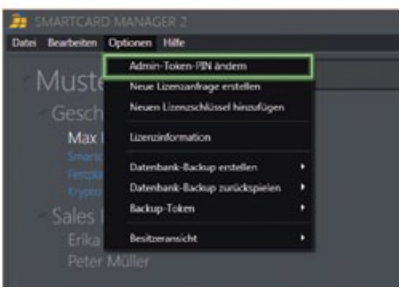


Bestätigen Sie die beiden nun erscheinenden Dialogfenster mit ⓥ.

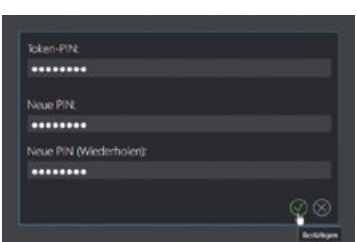
9. Optionen

9.1 Admin-Token-PIN ändern

Vergewissern Sie sich, dass der Admin-Token korrekt mit dem System verbunden ist. Gehen Sie nun auf „Optionen“ ▸ „Admin-Token-PIN ändern“.

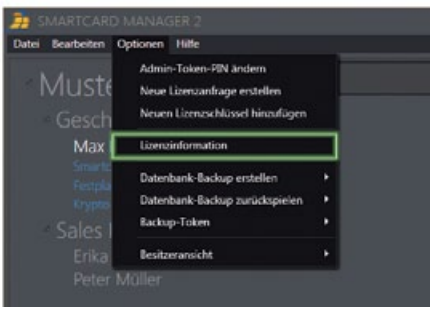


Sie können nun die alte Admin-Token-PIN und die neue Admin-Token-PIN eingeben und mit ♡ bestätigen.

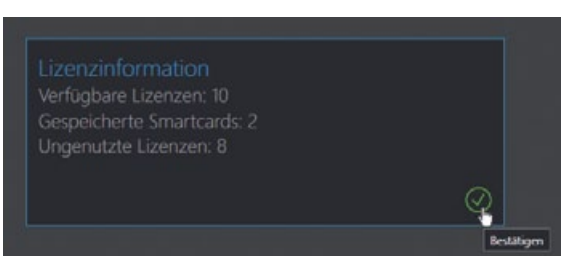


9.2 Lizenzinformationen einsehen

Klicken Sie auf Optionen“ ▸ „Lizenzinformation“.

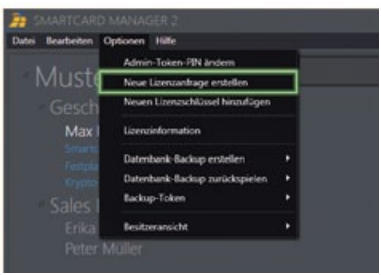


Im folgendem Fenster haben Sie Einsicht auf die verfügbaren Lizenzen, die gepeicherten Smartcards sowie die ungenutzten Lizenzen. Um das Fenster zu schließen, klicken Sie auf ⓥ.



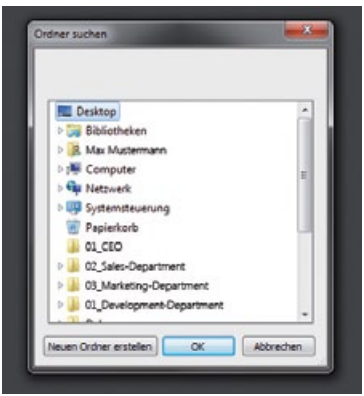
9.3 Neue Lizenzanfrage erstellen

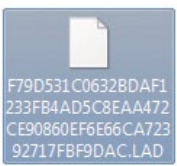
Um Ihr Kontingent an Lizenzen zur Verwaltung weiterer Smartcards in der Vollversion zu erhöhen, können Sie weitere Lizenzen bestellen. Für eine neue Lizenzanfrage öffnen Sie „Hilfe“ ▸ „neue Lizenzanfrage erstellen“.



Das nun angezeigte Eingabefeld muss vollständig ausgefüllt und die Angaben mit ⓥ bestätigt werden.

Danach wählen Sie den Speicherort der Lizenzanfrage aus. Der ausgewählte Speicherort der Datei (Endung .LAD) wird Ihnen in einem Fenster angezeigt.





Bestätigen Sie den nächsten Dialog mit ✓. Die Datei mit der Lizenzanfrage senden Sie an die DIGITTRADE GmbH unter folgender E-Mail-Adresse:

kundendienst@digittrade.de

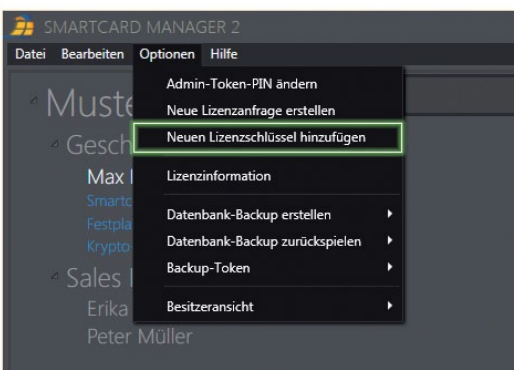
Lesen Sie bitte unter „9.4 Neuen Lizenzschlüssel hinzufügen“ nach, wie Sie die Lizenzen der Software hinzufügen.

Achtung: *Eine Veränderung des Dateinamens oder -inhaltes hat zur Folge, dass die Lizenzen ungültig werden.*

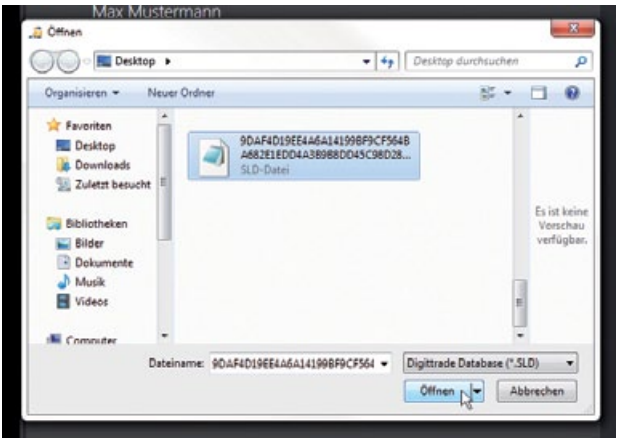
9.4 Neuen Lizenzschlüssel hinzufügen

Das freie Kontingent an 10 verwaltbaren Smartcards lässt sich durch eine Zubuchung von Lizenzen erweitern. Lesen Sie mehr dazu in „9.3 Neue Lizenzanfrage erstellen“.

Haben Sie die beantragten Lizenzen erhalten und auf Ihrem System gespeichert, so können Sie diese unter „Optionen“ ▸ „Neue Lizenzschlüssel hinzufügen“ in die Datenbank einspielen.



Suchen Sie hierzu in dem daraufhin erscheinenden Dialogfenster nach der Datei mit der Endung .SLD, wählen Sie diese aus und klicken Sie auf „Öffnen“.

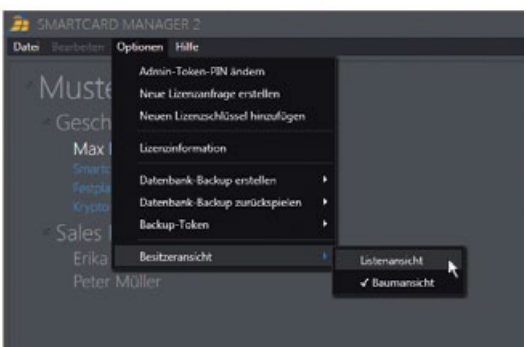


Hinweis: *Es lässt sich nur die beantragte und von DIGITTRADE freigegebene Anzahl an Lizenzen hinzufügen. Eine Aufteilung der Lizenzen ist nicht möglich und muss über die Bestellung geregelt werden.*

Achtung: *Eine Veränderung des Dateinamens oder -inhaltes hat zur Folge, dass die Lizenzen ungültig werden.*

9.5 Nutzeransicht ändern

Für die Verwaltung der Smartcards und Festplatten können Sie zwischen verschiedenen Ansichten wählen. Neben der standardmäßig eingestellten Baumansicht können Sie zudem die Listenansicht auswählen. Die Ansicht können Sie im Menüpunkt „Optionen“ ▸ „Ansicht“ ändern.



10. Hilfe

10.1 Benutzerhandbuch

Innerhalb der Software haben Sie die Möglichkeit das Benutzerhandbuch unter dem Menüpunkt „Hilfe“ ▸ „Benutzerhandbuch“ einzusehen.

10.2 Logbuch

Der Menüpunkt „Hilfe“ ▸ „Logbuch“ öffnet eine frei änderbare Textdatei, welche als Übersicht vorangegangener Aktionen dient. Bei auftretenden Problemen senden Sie das Logbuch, welches sich im Ordner des Smartcard Manager 2 auf Ihrem Rechner befindet, bitte an DIGITTRADE.

10.3 Info über DIGITTRADE Smartcard Manager 2

Über den Menüpunkt „Hilfe“ ▸ „Info über DIGITTRADE Smartcard Manager 2“ finden Sie Angaben darüber, um welche Version der Software es sich dabei handelt.

11. Hinweise

11.1 Hinweise zu Smartcard-Typen

Unter dem Gesichtspunkt der verschiedenen Smartcard-Typen befinden sich in der Krypto-Schlüssel-Detailansicht Angaben zum Sicherheitsniveau:

Schutzniveau	**kompatible Modelle**
10	HS128 / HS256
20	HS256S
30	HS256S
31	HS256S
32	HS256S
40	HS256 S3

Das Sicherheitsniveau des Krypto-Schlüssels richtet sich nach der Smartcard, welche diesen Krypto-Schlüssel verwendet und das niedrigste Sicherheitsniveau hat.

1. Smartcard Atmel CryptoMemory AT88SC014C
Sicherheitsniveau: 10
Diese Smartcard steht im Vergleich zu den anderen Smartcards im Hinblick auf das Sicherheitsniveau an letzter Stelle. Die Smartcard selber ist vom Anwender zwar auslesbar, jedoch nicht weiter beschreibbar.

2. Smartcard Oberthur Cosmo 64 v5.4 FIPS-140-2 Level 3
Sicherheitsniveau: 20
Diese Smartcard ist im mittleren Bereich des Sicherheitsniveaus zu finden. Sie ist beliebig oft beschreibbar. Die Einlesezeit ist geringfügig länger als bei der NXP Smartcard. Die Smartcard-PIN kann mit dem Smartcard Manager 2 nicht geändert werden.

3. Smartcard NXP J3A081, BSI CC EAL5
Sicherheitsniveau: 30
Diese Smartcard wurde durch die EAL5 Zertifizierung durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) mit einem sehr hohen Maß an Sicherheit ausgewiesen. Alle Funktionen des Smartcard Manager 2 sind mit diesem Smartcard-Typ ausführbar.

4. Smartcard NXP J2D081, BSI CC EAL5
Sicherheitsniveau: 31

Diese Smartcard wurde durch die EAL5 Zertifizierung durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) mit einem sehr hohen Maß an Sicherheit ausgewiesen. Alle Funktionen des Smartcard Manager 2 sind mit diesem Smartcard-Typ ausführbar.

5. Smartcard NXP J2E081, BSI CC EAL5
Sicherheitsniveau: 32
Diese Smartcard wurde durch die EAL5 Zertifizierung durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) mit einem Höchstmaß an Sicherheit ausgewiesen. Dadurch bietet diese Smartcard das höchste Sicherheitsniveau. Alle Funktionen des Smartcard Manager 2 sind mit diesem Smartcard-Typ ausführbar.

5. Smartcard NXP J2E081, BSI CC EAL5
Sicherheitsniveau: 40
Diese Smartcard wurde durch die EAL5 Zertifizierung durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) mit einem Höchstmaß an Sicherheit ausgewiesen. Dadurch bietet diese Smartcard das höchste Sicherheitsniveau. Alle Funktionen des Smartcard Manager 2 sind mit diesem Smartcard-Typ ausführbar.

11.2 Hinweise zu den Lizenzen und deren Gültigkeitsdauer

In der Demoversion des Smartcard Manager 2 werden 4 Lizenzen für 30 Tage zur Verfügung gestellt. Die Demoversion ist nicht an den Token gebunden. Zwar sind bei der Demoversion alle wesentlichen Funktionen nutzbar, jedoch ist das Sicherheitsniveau wesentlich niedriger, als es bei Verwendung des Tokens – also bei der Vollversion – der Fall ist. Der Token stellt sicher, dass die Datenbank und der gesamte Inhalt inklusive aller AES-Schlüssel verschlüsselt gespeichert werden. Mit der Vollversion des Smartcard Managers 2 werden 10 Lizenzen ohne Einschränkung in der Gültigkeitsdauer erworben.

11.3 Hinweise zu verlorenen oder defekten Token

Im Falle von Verlust des Admin-Tokens erlischt aus lizenzrechtlichen Gründen auch der Anspruch auf die bisher erworbenen Lizenzen. Ein mittels Token erstelltes Backup lässt sich anschließend mit Hilfe des Backup-Token einzuspielen.
Sollte der Token defekt sein, ist es möglich, diesen an DIGITTRADE zurückzusenden und gegen eine Gebühr gegen einen neuen Token einzutauschen. In diesem Fall behält der Anwender die bisher erworbenen Lizenzen. Das Einspielen eines mittels altem Admin-Token erstellten Backups lässt sich ebenfalls mit Hilfe des Backup-Token einspielen.

12. Fehlerbehebung

Anzahl der Fehlversuche bei der PIN-Eingabe	Maximal 8 Eingabefehler hintereinander, danach ist die Smartcard zerstört. Bei richtiger Eingabe wird der Zähler für falsche PIN-Eingaben wieder zurückgesetzt
DIGITTRADE Smartcard Manager 2 startet nicht	Senden Sie die Log-Datei „log.txt“ per E-Mail an beratung@digittrade.de oder / und versuchen Sie eine Neuinstallation der Software.

Es ist keine Anmeldung am Smartcard Manager 2 möglich / Token-PIN wird nicht erkannt	Überprüfen Sie, ob • der Admin-Token korrekt verbunden, • die Token-PIN korrekt eingegeben, • der entsprechende Smartcard Reader korrekt ausgewählt wurde
Smartcard Reader wird nicht erkannt	Überprüfen Sie, ob der Treiber für den Smartcard Reader installiert wurde
Token-PIN wird nicht erkannt	• Überprüfen Sie, ob der richtige Smartcard Reader ausgewählt wurde • Überprüfen Sie Ihre Eingabe der Token-PIN

Smartcard wird nicht erkannt	• Sie verwenden einen anderen Smartcard-Typ als unter 10.1 aufgelistet oder • Sie haben 8 Mal die falsche PIN eingegeben oder • die Smartcard ist defekt Beachten Sie, dass Smartcards des Typs Oberthur Cosmo 64 v5.4 mehr Zeit zum Einlesen benötigen.
Besitzer wird nicht erkannt	Legen Sie den Besitzer neu an (siehe 4.1)
Smartcard Manager 2 reagiert nicht	Überprüfen Sie im Taskmanager die Auslastung Ihres Computers und beenden Sie nicht benötigte, performancelastige Prozesse

Neue PIN kann nicht verwendet werden	Gründe: • alte und neue PIN stimmen überein (bitte achten Sie darauf, dass sich die alte und die neue PIN unterscheiden) • die neuen PIN stimmen nicht überein Wiederholen Sie den Vorgang (siehe 5.3)
Smartcard-PIN vergessen	Übertragen Sie die Daten der alten Smartcard auf eine Smartcard, deren PIN Ihnen bekannt ist (siehe 5.6).
Datenbank-Backup kann nicht erstellt werden	Überprüfen Sie, ob Sie für den angegebenen Speicherort die benötigten Zugriffsrechte besitzen und ob genügend Speicherplatz vorhanden ist. Wählen Sie unter Umständen einen anderen Speicherort.

Datenbank-Backup kann nicht zurückgespielt werden.	• Überprüfen Sie Ihre Passworteingabe • Wählen Sie die korrekte Authentifizierungsmethode (mittels Passwort oder Token) • überprüfen Sie die Datei auf Beschädigungen • wenn die Anwendung bereits läuft, überprüfen Sie, ob der Smartcard Manager über die Taskleiste aufrufbar ist. Sollte dies nicht der Fall sein, rufen Sie den Taskmanager auf (Strg+Alt+Entf) und suchen Sie in den Prozessen „SmartcardManager2.exe“. Klicken Sie auf den Namen und beenden Sie die Anwendung durch Klick auf „Prozess beenden“
Nicht alle Lizenzen werden angezeigt	Überprüfen Sie im Log-Buch die Fehlermeldungen bezüglich der Lizenzen.

13. Datensicherheit und Haftungsausschluss

Wir empfehlen, die mit dem Smartcard Manager 2 erstellten Backups grundsätzlich auf mindestens zwei verschiedenen DIGITTRADE HIGH SECURITY FESTPLATTEN zu sichern. Die DIGITTRADE GmbH haftet nicht für den Verlust von Daten sowie dadurch entstehende Kosten und Schäden und trägt nicht die datenschutzrechtliche Verantwortlichkeit der gespeicherten Daten.

Der DIGITTRADE Smartcard Manager 2 sollte nur in einer absolut sicheren Umgebung verwendet werden. Die Verwendung sollte ausschließlich auf einem vom Netzwerk getrennten und sicher aufbewahrtem, virenfreien Rechner mit Zugriffsschutz vor Unbefugten erfolgen. Eine Verbindung zum Internet sollte unter allen Umständen ausgeschlossen werden.

Um Datenverluste zu vermeiden, sollten regelmäßig Backups sowohl mittels Passwort als auch mit dem Admin-Token erstellt werden.

Außerdem wird empfohlen, in regelmäßigen Abständen die Funktionalität des Backups und Backup-Token durch Einspielen der Daten zu überprüfen.

14. Lieferumfang

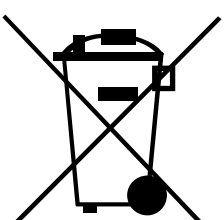
- CD mit Software DIGITTRADE Smartcard Manager 2
- Admin-Token
- Smartcard Reader
- Anleitung

15. Hinweis zum Schutz und Erhalt der Umwelt

Gemäß der EG-Richtlinie dürfen Elektro- und Elektronik-Altgeräte nicht mehr als kommunale Abfälle entsorgt werden.

Um die Verbreitung der enthaltenen Bausubstanzen in Ihrer Umgebung zu vermeiden und natürliche Ressourcen zu sparen, bitten wir Sie, dieses Produkt nach Ablauf seiner Lebensdauer ausschließlich an einer lokalen Altgerätesammelstelle in Ihrer Nähe abzugeben.

Dank dieser Maßnahmen können die Materialien Ihres Produktes umweltfreundlich wiederverwendet werden.



Glossar

Admin-Token:
Mitgeliefertes, USB-Stick ähnliches Kartenlesegerät zum Anschluss an den Rechner oder Laptop. Dient der Authentifizierung und ist nötig, um den Smartcard Manager uneingeschränkt nutzen zu können.

AES-Schlüssel:
Teil des kryptografischen Schlüssels. Parametrisiert die Art, Klartexte zu verschlüsseln und somit unleserlich zu machen.

Backup:
Gespeicherte, hinterlegte Datei mit den Werten, Informationen und Datensätzen, welche zum Zeitpunkt der Erstellung aktuell waren. Dient der Sicherheit, um im Falle von Datenverlust oder Fehlern die Software auf den Stand zum Zeitpunkt der Erstellung des Backups zurückzuführen.

Backup erstellen:
Erstellt und speichert eine Datei mit allen Werten, Informationen und Datensätzen, die die Software aktuell enthält.

Backup zurückspielen:
Setzt die Software mit allen Daten, Informationen und Werten auf den Stand zum Zeitpunkt der Erstellung zurück. Aktuelle Daten müssen mit einem neu erstellten Backup gesichert werden, da diese sonst nach Einspielen des Backups verloren gehen.

Backup-Token:
Dient als weitere Sicherheit einzig dem Einspielen von Backups, sofern diese mit miteinander verbunden Backup- und Admin-Token erstellt wurden.

Besitzer:
Person, der Festplatten und/oder Smartcards zugeordnet wurden.

Hauptelement:
Besitzer, der in der Liste linksbündig und in großer Schrift dargestellt ist. Ihm sind weitere Personen zugeordnet, aber keine Personen übergeordnet. Es ist möglich, mehrere Hauptelemente anzulegen.

Krypto-Schlüssel:
Besteht unter anderem aus AES-Schlüssel sowie anderen Werten. Dient der Ver- und Entschlüsselung.

Lizenzen:
Rechtliche Erlaubnis zur Verwaltung von Smartcards.

Lizenzschlüssel:
Von DIGITTRADE übersandte Datei zur Erhöhung Ihres Kontingents an Lizenzen.

Logbuch:
Automatisch erstellte Textdatei mit Erfassung aller ausgeführten Aktionen sowie (Fehler-)Meldungen. Datei befindet sich im Ordner „Smartcard Manager 2“.

Match-ID:
Regelt die Initialisierung in Bezug auf die Kompatibilität zwischen Smartcard und Festplatte.

Nutzeransicht:
Ändert Ansicht zwischen Listenansicht (alle Zuordnungendes Hauptelementes werden mit Klick auf eben diesen sofort angezeigt) und Baumansicht (Zuordnungen werden erst mit Klick auf den jeweiligen Überbesitzer angezeigt).

Nutzungsberechtigter:
Personen, die zumindest theoretisch über die Smartcard zur Nutzung der Festplatte berechtigt sind, da der Kryptoschlüssel von Smartcard und Festplatte identisch ist.

Passwort:
Frei wählbares Kennwort mit mindestens einem Zeichen zur Erstellung eines Backups. Es sind alle Zeichen erlaubt, jedoch muss das Passwort beim Zurückspielen des Backups identisch mit dem bei der Erstellung sein.

PIN:
Achtstellige Zahlenfolge, die zur Authentifizierung bei fast allen Funktionen bei Verwendung das Smartcard Managers benötigt wird. Die Standardeinstellung bei Auslieferung der Token und Smartcards lautet „1-2-3-4-5-6-7-8".

Shortcuts:
Tastenkombination zur schnelleren Erreichbarkeit bestimmter Funktionen.

Sicherheitsniveau:
Zeigt an, wie sicher die Verwendung des ausgewählten kryptografischen Schlüssels ist. Richtet sich nach dem Sicherheitsniveau der Smartcard, die den Schlüssel verwendet und das niedrigste Niveau aufweist.

Notizen

Ihre Fragen beantworten wir gerne telefonisch unter
0345/2317353

oder per E-Mail
beratung@digittrade.de

DIGITTRADE GmbH
Ernst-Thälmann-Str. 39
06179 Teutschenthal Germany

Fon	49 / 345 / 2317353
Fax	+49 / 345 / 6138697
E-Mail	beratung@digittrade.de
Web	www.digittrade.de