ANLEITUNG ZU EINRICHTUNG DER SMARTY® VERSCHLÜSSELUNG

Version 1.1

New Media Company GmbH & Co. KG
Donnerschweer Straße 398
26123 Oldenburg
Telefon: 0441 - 390 112 00
Fax: 0441 - 390 112 10
Email: info@newmediacompany.de
www.smarty-online.de

Inhaltsverzeichnis

1. Informationen

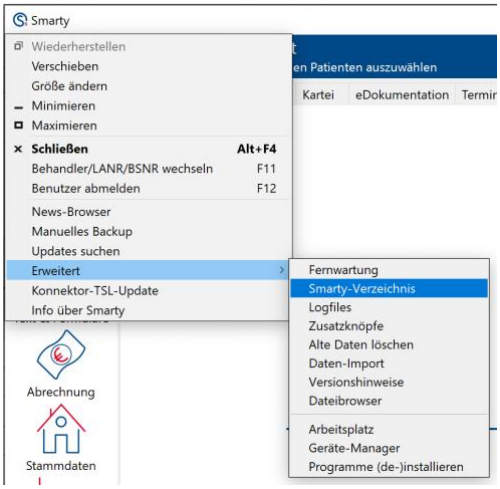
Mit unserer Lizenz *Verschlüsselung* können Sie Ihren gesamten Patienten- und Dokumentenbestand verschlüsseln und somit vor einem Fremdzugriff oder Diebstahl schützen. Ihre Daten werden mit AES256 verschlüsselt, einer der sichersten Verschlüsselungsmethoden, die es gibt.

Für die Einrichtung der Smarty® Verschlüsselung wird das Datenbank-managementsystem Firebird in der Version 3 vorausgesetzt. Für die Einzelplatzversion von Smarty® stellen wir Ihnen diese kostenfrei zur Verfügung und haben Ihnen auch die Einrichtung wieder so einfach wie möglich gestaltet.

2. Einrichtung der Verschlüsselung am Einzelplatz

2.1 Installation von Firebird 3

Um Firebird 3 auf Ihrem Computer zu installieren, klicken Sie bitte links oben in Smarty® auf das kleine Smarty®-Icon, gehen dort auf *Erweitert* und wählen das *Smarty-Verzeichnis* aus.



Gehen Sie bitte in den Ordner *Module*, dort in den Ordner *Installer* und öffnen Sie den Ordner *Firebird*. Starten Sie die *Firebird3Install.bat* als Administrator (ggf. Rechtsklick auf die Datei und „Als Administrator ausführen“ auswählen) und folgen Sie den Anweisungen um Firebird 3 und den ODBC-Treiber zu installieren. Alle weiteren im Ordner befindlichen Dateien müssen und sollten nicht installiert werden.

Alternativ finden Sie die notwendige Datei bei der Standardinstallation von Smarty® unter folgender Adresse:

C:\Smarty\Module\Installer\Firebird
Datei: Firebird3Install.bat

2.2 Backup erstellen

Bevor Sie nun mit der Einrichtung fortfahren, erstellen Sie bitte noch ein manuelles Backup. Hierzu klicken Sie bitte in Smarty® links oben auf das kleine Smarty®-Icon und wählen dort *Manuelles Backup* aus. Speichern Sie das Backup (Datensicherung) an einem beliebigen Ort, auf den Sie im Notfall jederzeit zugreifen können.

2.3 Eingabe der neuen Lizenznummer

Nachdem Firebird 3 installiert und ein Backup (Datensicherung) erstellt wurde, können Sie Smarty® starten und die Lizenznummer unter *Stammdaten* und dem Reiter *Praxis* eingeben. Hierfür klicken Sie bitte rechts unten auf *Lizenznummer* und geben die von uns zugesendeten Lizenzdaten aus der E-Mail ein. Die Eingabe bestätigen Sie dann mit „Speichern & Beenden“.

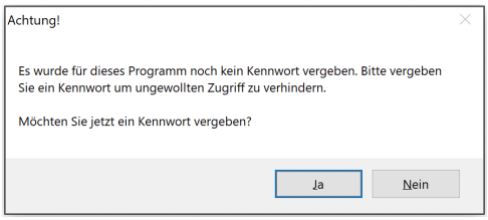
Nachdem die Lizenz erfolgreich eingegeben wurde, wird nach einem Hinweis die Access-Datenbank zu Firebird 3 konvertiert. Der erfolgreiche Abschluss der Konvertierung wird Ihnen am Ende vom System rückgemeldet.

2.4 Aktivierung des Wartungsmodus

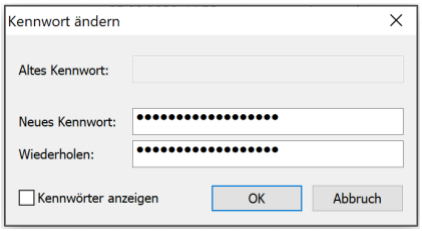
Um das Programm für Verschlüsselung zu starten, klicken Sie bitte links oben in Smarty® auf das kleine Smarty®-Icon, gehen dort auf *Erweitert* und wählen das *Smarty-Verzeichnis* aus. Smarty® muss daraufhin geschlossen werden!

Gehen Sie bitte in den Ordner *Module* und öffnen den Ordner *Installer*. Starten Sie dort bitte die Datei *DBCryptTool.exe*.

Um das Programm vor unerlaubtem Zugriff zu schützen, können Sie für den Start ein Passwort vergeben.

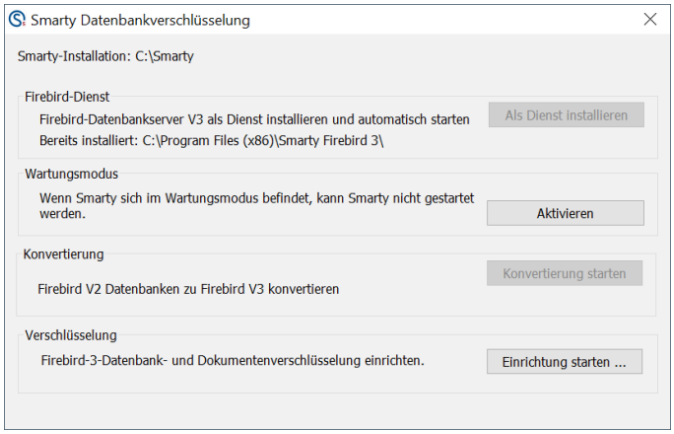


Bitte vergeben Sie ein Kennwort, das Groß- und Kleinschreibung, sowie Zahlen und Sonderzeichen enthält und ausreichend lang ist.



Bevor die Verschlüsselung nun gestartet werden kann, muss das System in den Wartungsmodus versetzt werden. Hierzu klicken Sie im Bereich Wartungsmodus bitte auf die Schaltfläche *Aktivieren.*

Während der Einrichtung ist es wichtig, dass Smarty® nicht gestartet ist/wird!

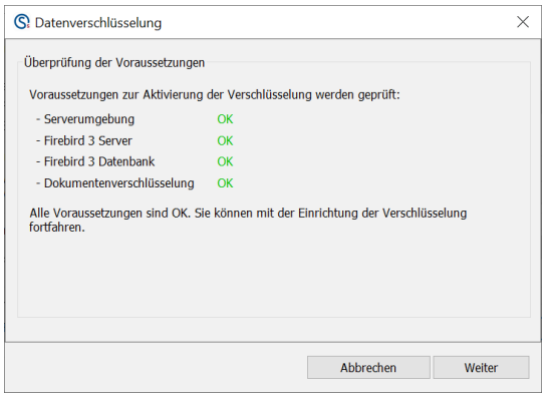


2.5 Starten der Datenverschlüsselung

Starten Sie die Einrichtung der Datenverschlüsselung nun bitte über die Schaltfläche *Einrichtung starten*.

2.5.1 Überprüfung der Voraussetzungen

Zunächst müssen die Voraussetzungen überprüft werden, damit die Verschlüsselung gestartet werden kann.

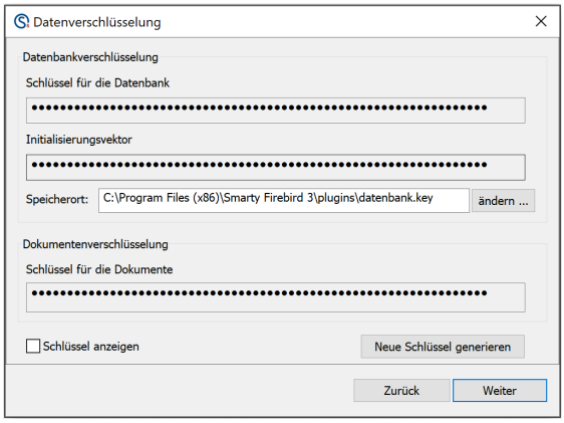


Sind die Voraussetzungen erfüllt, können Sie auf die Schaltfläche *Weiter* klicken und gelangen so zur Einrichtung der Datenbankverschlüsselung.

2.5.2 Datenbank- und Dokumentenverschlüsselung

Der Schlüssel für die Datenbankverschlüsselung wird automatisch generiert, so dass sichergestellt ist, dass das Kennwort für die Erzeugung des Schlüssels ausreichend Zeichen enthält.

Als nächstes können Sie einen Speicherort für die Schlüsseldatei festlegen, sofern Sie den vorhandenen nicht übernehmen möchten. Dieser sollte nicht im Smarty-Verzeichnis liegen.

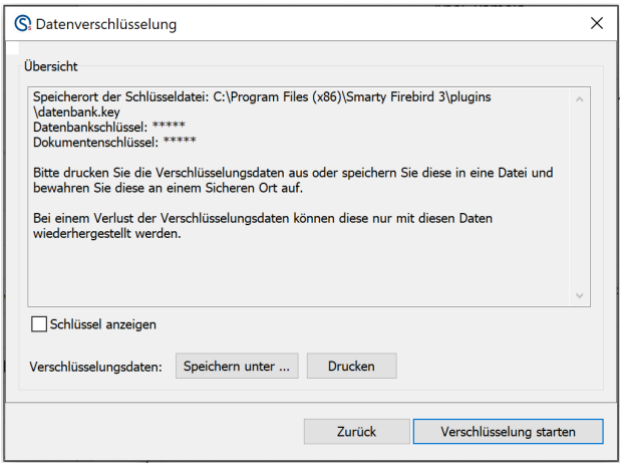


Sie können die Schlüsseldatei alternativ auch auf einem externen Speichermedium, wie z. B. einer externen Festplatte, einem USB-Stick oder einer SD-Karte, abspeichern.

Bitte beachten Sie, dass Smarty® dann nur gestartet werden kann, wenn das Speichermedium mit dem Schlüssel auch an den Computer angeschlossen ist!

2.5.3 Übersicht der Verschlüsselungsdaten

Bevor die Verschlüsselung der Daten beginnt, erhalten Sie noch einmal eine Übersicht über die festgelegten Daten.



Technische Informationen:

Der Schlüssel ist Hexadezimal kodiert und umfasst die Zahlen von 0-9 und Buchstaben von A-F. Wenn dieser als String zurückkodiert wird, enthält dieser alle möglichen 256 Zeichen.

Wenn die Schlüsseldatei verloren geht, haben Sie keine Möglichkeit mehr auf die Daten in Smarty® zuzugreifen!

Im Notfall kann die Schlüsseldatei mit den festgelegten Kennwörtern wiederhergestellt werden. Es wird daher dringend empfohlen die Verschlüsselungsdaten auszudrucken oder in eine gesonderte Textdatei zu speichern!

Die Verschlüsselungsdaten sollten an einem sicheren Ort aufbewahrt werden!

Sie können dann mit der Verschlüsselung der Daten über die Schaltfläche *Verschlüsselung starten* beginnen.

2.5.4 Fortschritt der Verschlüsselung

Während der Verschlüsselung erhalten Sie eine Übersicht über den Fortschritt der Verschlüsselung. Dieses kann je nach Menge der Daten und Geschwindigkeit der Festplatte mehrere Minuten dauern.

Nach der erfolgreichen Verschlüsselung können Sie das Fenster über die Schaltfläche *Beenden* schließen.

2.6 Beenden des Wartungsmodus

Als letzten Schritt deaktivieren Sie nun bitte noch den Wartungsmodus über die Schaltfläche *Deaktivieren*. Daraufhin können Sie Smarty® starten und die Arbeit wieder aufnehmen.

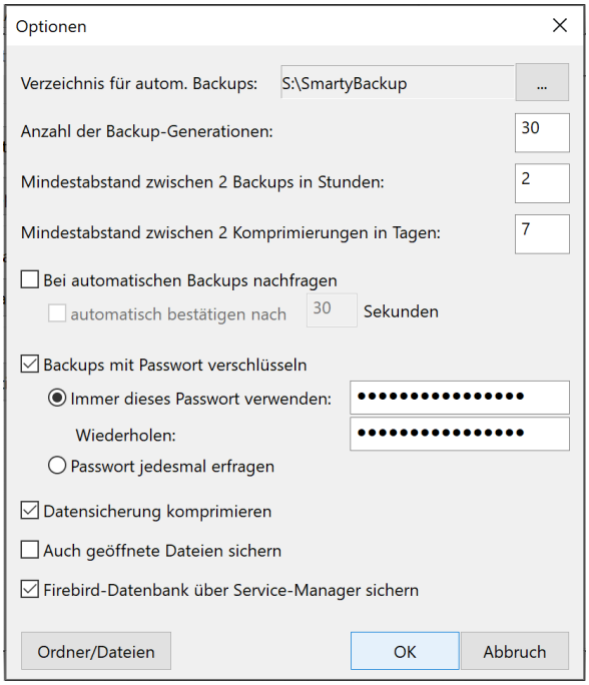
2.7 Verschlüsselung des Backups

Wenn Ihr Smarty® verschlüsselt ist, dann wird auch die Verschlüsselung des Backups zur Pflicht! Darauf weist Smarty® Sie beim Erstellen eines Backups hin, sollte vorher kein Passwort vergeben worden sein.

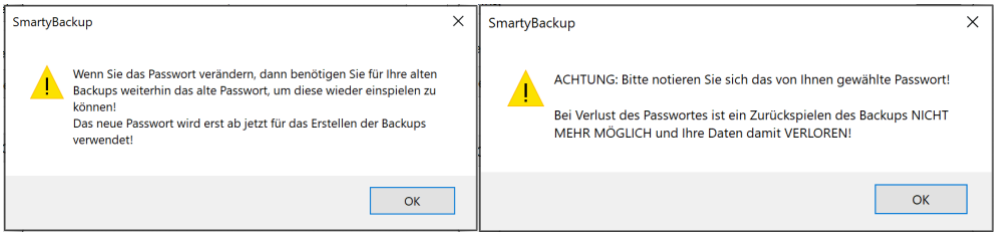
Wir empfehlen Ihnen diese Einstellungen aber bereits vorher vorzunehmen, damit es im regulären Betrieb nicht zu Irritationen kommt.

Klicken Sie in Smarty® bitte links unten auf *Erweitert* und wählen dort *Smarty-Backup* aus. Klicken Sie auf der linken Seite bitte auf *Optionen*. In den Optionen haben Sie jetzt die Möglichkeit ein Passwort anzugeben, mit dem die Backups verschlüsselt werden. Aktivieren Sie bitte *Backups mit Passwort verschlüsseln* durch das Setzen des Häkchens und vergeben Sie ein Passwort. Um die Sicherheit zu erhöhen, sollte das

Passwort different zu allen anderen verwendeten Passwörtern sein. Das Passwort für die Backups sollten Sie sich notieren und genau wie die weiteren Verschlüsselungsdaten an einem sicheren Ort aufbewahren!



Nachdem Sie Ihr Passwort eingegeben und das Fenster mit OK bestätigt haben, erhalten Sie die beiden nachfolgenden Hinweise:



3. Einrichtung der Verschlüsselung im Netzwerk-/Serverbetrieb

Die Einrichtung der Verschlüsselung im Netzwerk-/Serverbetrieb muss am Server erfolgen und dabei sichergestellt werden, dass Smarty® an keinem Client gestartet ist und auch nicht gestartet wird.

3.1 Backup erstellen

Bevor Sie nun mit der Einrichtung fortfahren, erstellen Sie bitte noch ein manuelles Backup. Hierzu klicken Sie bitte in Smarty® links oben auf das kleine Smarty®-Icon und wählen dort *Manuelles Backup* aus. Speichern Sie das Backup (Datensicherung) an einem beliebigen Ort, auf den Sie im Notfall jederzeit zugreifen können.

3.2 Eingabe der neuen Lizenznummer

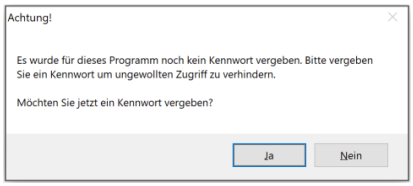
Zur Eingabe der Lizenznummer gehen Sie bitte unter *Stammdaten* auf den Reiter *Praxis*. Klicken Sie bitte rechts unten auf *Lizenznummer* und geben Sie die von uns zugesendeten Lizenzdaten aus der E-Mail ein. Die Eingabe bestätigen Sie dann mit „Speichern & Beenden“. Sollte die Eingabe erfolgreich gewesen sein, erhalten Sie kein gesondertes Feedback und können mit Punkt 3.2 weitermachen.

3.3 Aktivierung des Wartungsmodus

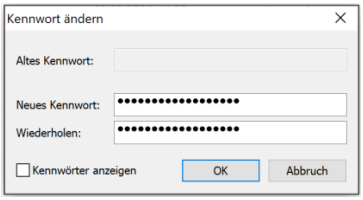
Um das Programm für Verschlüsselung zu starten, gehen Sie bitte in das lokale Installationsverzeichnis (nicht das freigegebene Netzlaufwerk wie z. B. S:) von Smarty® auf dem Server. Im Ordner *Module* öffnen Sie bitte den Ordner *Installer* und starten dort die Datei *DBCryptTool.exe*.

C:\Smarty\Module\Installer
Datei: DBCryptTool.exe

Um das Programm vor unerlaubtem Zugriff zu schützen, können Sie für den Start ein Passwort vergeben.

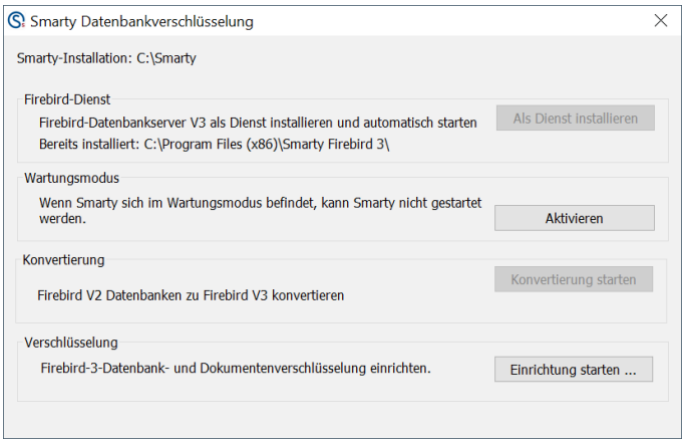


Bitte vergeben Sie ein Kennwort, das Groß- und Kleinschreibung, sowie Zahlen und Sonderzeichen enthält und ausreichend lang ist.



Bevor die Verschlüsselung nun gestartet werden kann, muss das System in den Wartungsmodus versetzt werden. Hierzu klicken Sie im Bereich Wartungsmodus bitte auf die Schaltfläche *Aktivieren.*

Während der Einrichtung ist es wichtig,
dass Smarty® weder am Server, noch an den Clients gestartet ist und auch nicht gestartet wird!

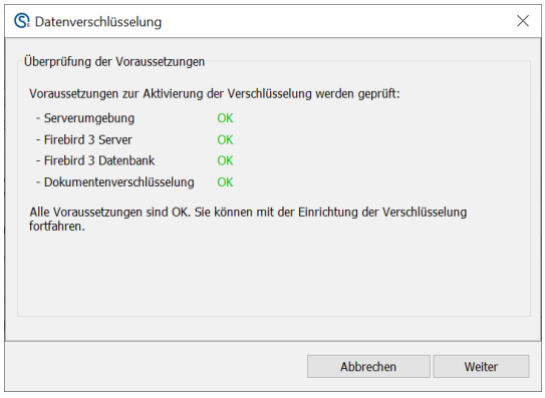


3.4 Starten der Datenverschlüsselung

Starten Sie die Einrichtung der Datenverschlüsselung nun bitte über die Schaltfläche *Einrichtung starten*.

3.4.1 Überprüfung der Voraussetzungen

Zunächst müssen die Voraussetzungen überprüft werden, damit die Verschlüsselung gestartet werden kann.

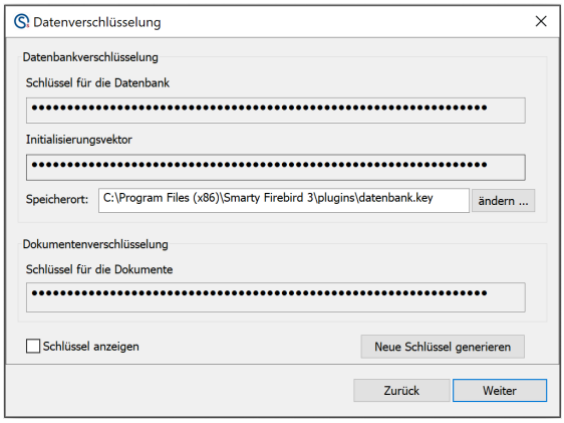


Sind die Voraussetzungen erfüllt, können Sie auf die Schaltfläche *Weiter* klicken und gelangen so zur Einrichtung der Datenbankverschlüsselung.

3.4.2 Datenbank- und Dokumentenverschlüsselung

Der Schlüssel für die Datenbankverschlüsselung wird automatisch generiert, so dass sichergestellt ist, dass das Kennwort für die Erzeugung des Schlüssels ausreichend Zeichen enthält.

Als nächstes können Sie einen Speicherort für die Schlüsseldatei festlegen, sofern Sie den vorhandenen nicht übernehmen möchten. Dieser sollte nicht im Smarty-Verzeichnis liegen.

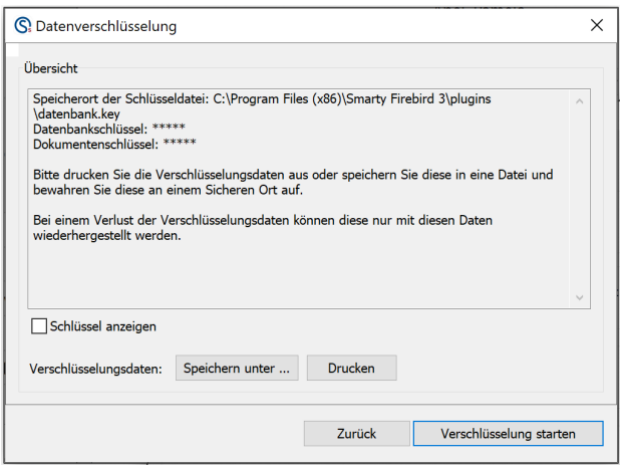


Sie können die Schlüsseldatei alternativ auch auf einem externen Speichermedium, wie z. B. einer externen Festplatte, einem USB-Stick oder einer SD-Karte, abspeichern.

Bitte beachten Sie, dass Smarty® dann nur gestartet werden kann, wenn das Speichermedium mit dem Schlüssel auch an den Computer angeschlossen ist!

3.4.3 Übersicht der Verschlüsselungsdaten

Bevor die Verschlüsselung der Daten beginnt, erhalten Sie noch einmal eine Übersicht über die festgelegten Daten.



Technische Informationen:

Der Schlüssel ist Hexadezimal kodiert und umfasst die Zahlen von 0-9 und Buchstaben von A-F. Wenn dieser als String zurückkodiert wird, enthält dieser alle möglichen 256 Zeichen.

Wenn die Schlüsseldatei verloren geht, haben Sie keine Möglichkeit mehr auf die Daten in Smarty® zuzugreifen!

Im Notfall kann die Schlüsseldatei mit den festgelegten Kennwörtern wiederhergestellt werden. Es wird daher dringend empfohlen die Verschlüsselungsdaten auszudrucken oder in eine gesonderte Textdatei zu speichern!

Die Verschlüsselungsdaten sollten an einem sicheren Ort aufbewahrt werden!

Sie können dann mit der Verschlüsselung der Daten über die Schaltfläche *Verschlüsselung starten* beginnen.

3.4.4 Fortschritt der Verschlüsselung

Während der Verschlüsselung erhalten Sie eine Übersicht über den Fortschritt der Verschlüsselung. Dieses kann je nach Menge der Daten und Geschwindigkeit der Festplatte mehrere Minuten dauern.

Nach der erfolgreichen Verschlüsselung können Sie das Fenster über die Schaltfläche *Beenden* schließen.

3.5 Beenden des Wartungsmodus

Als letzten Schritt deaktivieren Sie nun bitte noch den Wartungsmodus über die Schaltfläche *Deaktivieren*. Daraufhin kann Smarty® an allen Clients gestartet und die Arbeit wieder aufgenommen werden.

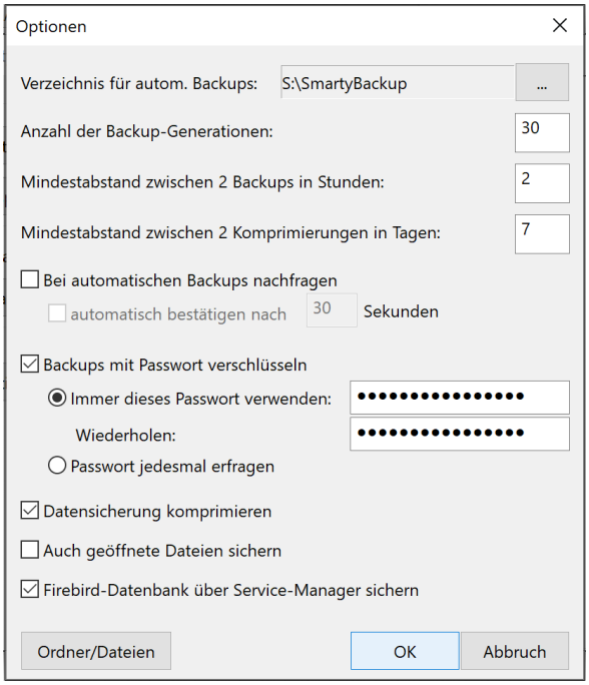
3.6 Verschlüsselung des Backups

Wenn Ihr Smarty® verschlüsselt ist, dann wird auch die Verschlüsselung des Backups zur Pflicht! Darauf weist Smarty® Sie beim Erstellen eines Backups hin, sollte vorher kein Passwort vergeben worden sein.

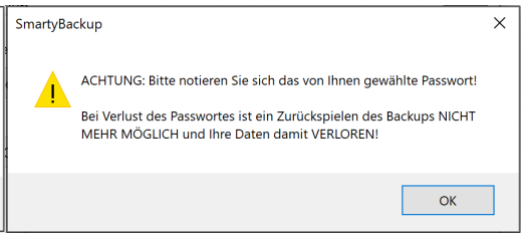
Wir empfehlen Ihnen diese Einstellungen aber bereits vorher vorzunehmen, damit es im regulären Betrieb nicht zu Irritationen kommt.

Klicken Sie in Smarty® bitte links unten auf *Erweitert* und wählen dort *Smarty-Backup* aus. Klicken Sie auf der linken Seite bitte auf *Optionen*. In den Optionen haben Sie jetzt die Möglichkeit ein Passwort anzugeben, mit dem die Backups verschlüsselt werden. Aktivieren Sie bitte *Backups mit Passwort verschlüsseln* durch das Setzen des Häkchens und vergeben Sie ein Passwort. Um die Sicherheit zu erhöhen, sollte das

Passwort different zu allen anderen verwendeten Passwörtern sein. Das Passwort für die Backups sollten Sie sich notieren und genau wie die weiteren Verschlüsselungsdaten an einem sicheren Ort aufbewahren!



Nachdem Sie Ihr Passwort eingegeben und das Fenster mit OK bestätigt haben, erhalten Sie die beiden nachfolgenden Hinweise:



4. FAQs

4.1 Warum muss das Backup verschlüsselt werden?

Es wird zwischen Datenbank- und Dokumentenverschlüsselung unterschieden. Der Datenbankschlüssel wird in einer Datei gespeichert. Der Schlüssel für die Dokumente in der Datenbank. Wenn Smarty® gebackupt wird, wird der Schlüssel für die Dokumente gesichert, da dieser in der Datenbank steht. Der Schlüssel für die Datenbank wird nicht gesichert. Die Datenbanken gelangen somit unverschlüsselt ins Backup (Datenbank-Backupdateien können nicht verschlüsselt werden). Deshalb muss das Backup passwortgeschützt sein! Dadurch sind Ihre Backups sicher.

4.2 Neuer Computer

Sollten Sie den Computer wechseln, muss auf dem neuen Computer die Datenbankverschlüsselung wieder aktiviert werden, da die Datenbanken unverschlüsselt wiederhergestellt werden (siehe 4.1). Auf dem neuen Computer muss das DBCryptTool (siehe 2.4 oder 3.3) erneut ausgeführt werden, um die Datenbanken wieder zu verschlüsseln (die Dokumente behalten ihre Verschlüsselung). Sobald auf dem neuen Computer die Datenbankverschlüsselung wieder aktiviert ist, werden die Datenbanken beim Zurückspielen des Backups wieder verschlüsselt.

4.3 Ich arbeite mit einem Computer in der Praxis und einem anderen Computer Zuhause. Was muss ich beachten?

Da die Datenbanken im Backup unverschlüsselt sind (siehe 4.1), muss am Computer Zuhause vorher einmalig die Verschlüsselung aktiviert werden. Dazu muss auf diesem Computer (Zuhause) das DBCryptTool (siehe 2.4 oder 3.3) erneut ausgeführt werden. Sobald auf dem Computer (Zuhause) die Datenbankverschlüsselung wieder aktiviert ist, werden die Datenbanken beim Zurückspielen des Backups wieder verschlüsselt.

4.4 Braucht mein Smarty® jetzt länger um zu starten oder zu schließen?

Zeitliche Differenzen zwischen einem verschlüsselten und einem nicht verschlüsselten Smarty® dürften beim Starten oder Beenden dürften nicht auftreten.

4.5 Kann ich die Schlüsseldatei auch verschieben?

Die Schlüsseldatei kann verschoben werden, muss beim Start von Smarty® aber dort liegen, wo sie mit dem Verschlüsselungstool gespeichert wurde. Wenn die Datei nachträglich verschoben wird, wird sie nicht mehr vom Firebird-Server-Dienst gefunden.

4.6 Werden auch meine mobilen Lösungen verschlüsselt?

Die Verschlüsselung gilt ausschließlich für Smarty® und nicht für die mobilen Lösungen.