

Dokumentation

sidoku[®] Secure Mail Connector SE

Einrichtungsassistent

Release 1.0

erstellt von:

EXEC IT Solutions GmbH
Südstraße 24
56235 Ransbach-Baumbach
www.exec.de

Inhalt

1 Einleitung	1
2 Technik/Sicherheit	1
2.1 Betrieb	1
3 Installation des Einrichtungsassistenten des sidoku® Secure Mail Connector SE	2
4 sidoku® Secure Mail Connector SE Einrichtungsassistent	5
4.1 Schlüsselpaar-Erzeugung	5
5 Inbetriebnahme des sidoku® Secure Mail Connector SE Einrichtungsassistenten	7
5.1 Einstellungen Proxy-Server	7
5.2 Zugangsdaten	8
5.3 E-Mail-Server	12
5.4 E-Mail-Texte	12
5.5 Fehlerbenachrichtigung	13
5.6 Einstellungen überprüfen	14
5.7 Schlüsselübertragung	15
5.8 Abschluss	16
6 Schlüsselverwaltung	16
7 Installation auf einem Linux-Betriebssystem	17
7.1 Installation der Dateien	17
7.2 Start des Konfigurationsassistenten	18
7.3 Einrichtung des Dienstes	18
7.4 Start der Schlüsselverwaltung	19

1 Einleitung

Der Einrichtungsassistent hilft Ihnen bei der Einrichtung des sidoku® Secure Mail Connector SE innerhalb Ihres Netzwerkes.

Der sidoku® Secure Mail Connector SE ist eine für den Endbenutzer unsichtbare Verbindung zwischen der bestehenden E-Mail-Kommunikation und dem sidoku®-System. Nachrichten, die an Ihre „sidoku®-E-Mail-Adresse geschickt werden, wandelt der sidoku® Secure Mail Connector SE in E-Mails um und stellt sie dem Empfänger auf der gewohnten E-Mail-Oberfläche zur Verfügung. Die Anmeldung an das sidoku® Portal und der damit verbundene Zeitaufwand entfallen. Das Prinzip funktioniert auch in die andere Richtung. Der Benutzer schreibt eine E-Mail an eine „sidoku®“- Adresse, der sidoku® Secure Mail Connector SE wandelt sie in eine sidoku®-E-Mail um und sendet diese an das sidoku® Postfach des Empfängers.

Ziel des sidoku® Secure Mail Connector SE ist es, dem Benutzer von sidoku® den sicheren Dokumentenaustausch zu ermöglichen und trotzdem die gewohnte Arbeitsweise zu erhalten. Die für das Unternehmen wichtige Sicherheit beim Austausch elektronischer Nachrichten kann auf diese Weise ohne erhöhten Arbeitsaufwand für den einzelnen Mitarbeiter umgesetzt werden. Außerdem hat der Nutzer den Vorteil, dass alle empfangenen E-Mails, ob via sidoku® oder nicht in nur einer E-Mail-Integration gespeichert werden.

Dieses Handbuch soll Sie während der gesamten Installation des sidoku® Secure Mail Connector SE unterstützen.

2 Technik/Sicherheit

Im Rahmen der Einrichtung des sidoku® Secure Mail Connector SE wird ein Schlüsselpaar für asymmetrische Verschlüsselung erstellt. Dieses Schlüsselpaar bildet die Grundlage für die Nutzung des sidoku® Secure Mail Connector SE. Bei der Einrichtung der einzelnen Benutzer des Unternehmens wird für jeden Benutzer ebenfalls ein Schlüsselpaar für asymmetrische Verschlüsselung erstellt.

Dabei ist zu beachten, dass die öffentlichen Schlüssel der Benutzer beim Einrichtungsvorgang automatisch im zentralen sidoku®-System abgespeichert und für die Verschlüsselung von Nachrichten verwendet werden. Die privaten Schlüssel der Benutzer werden immer kennwortgeschützt im Unternehmen gespeichert und für die Entschlüsselung der Nachrichten benötigt.

Da der sidoku® Secure Mail Connector SE zur Entschlüsselung von eingehenden Nachrichten für die Benutzer des Unternehmens den privaten Teil des Schlüssels benötigt, muss beim Start des sidoku® Secure Mail Connector SE das Passwort für diesen privaten Schlüssel eingegeben werden, erst dann kann der sidoku® Secure Mail Connector SE arbeiten. Zur Eingabe dieses Kennwortes wird nach dem Start des sidoku® Secure Mail Connector SE -Dienstes ein Programm gestartet(siehe Abschnitt 6 Schlüsselmanagement), in welchem das Kennwort eingegeben und dann an den sidoku® Secure Mail Connector SE -Dienst weitergegeben wird.

2.1 Betrieb

Der sidoku® Secure Mail Connector SE läuft als Dienst innerhalb des Netzwerkes des Unternehmens und kommuniziert mit dessen Mailserver. In regelmäßigen Abständen werden sidoku® Nachrichten für das Unternehmen bzw. die konfigurierten Benutzer abgerufen und auf dem Mailserver des Unternehmens verteilt.

Die Konfiguration des Mailservers des Kunden muss daher dahingehend angepasst werden, dass alle intern versendeten Emails, welche an die Domain "*.sidoku.de" gerichtet sind, per SMTP an den sidoku® Secure Mail Connector SE weitergeleitet werden. Der sidoku® Secure Mail Connector SE fungiert in diesem Fall als E-Mailserver. Er nimmt die Nachricht an und überträgt sie an das sidoku®-System.

Die Zuordnung von Sender/Empfänger einer E-Mail zu einem sidoku®-Benutzer erfolgt über den Benutzernamen, deshalb müssen der Benutzername und die E-Mail-Adresse des jeweiligen Benutzers identisch sein. Erhält der sidoku® Secure Mail Connector SE vom Mailserver z.B. eine Nachricht von m.mustermann@muster.de, wird im zentralen System nachgeschlagen, welcher sidoku®-Benutzer dieser E-Mail zugeordnet ist und dieser Benutzer wird dann im sidoku®-System als Sender der Nachricht eingetragen. Erhält der sidoku® Secure Mail Connector SE eine Nachricht vom zentralen sidoku®-System, wird für den Empfänger der Nachricht der Benutzername ermittelt und die Nachricht intern an dessen E-Mail-Adresse verschickt.

3 Installation des Einrichtungsassistenten des sidoku® Secure Mail Connector SE

Den Einrichtungsassistenten für den sidoku® Secure Mail Connector SE bekommen Sie in der jeweils aktuellen Fassung auf Anfrage von uns zur Verfügung gestellt. Bitte setzen Sie sich dazu mit uns über die auf der Seite www.sidoku.de genannten Kontaktdaten in Verbindung.

Nach dem Start des Einrichtungsassistenten öffnet sich das folgende Fenster.

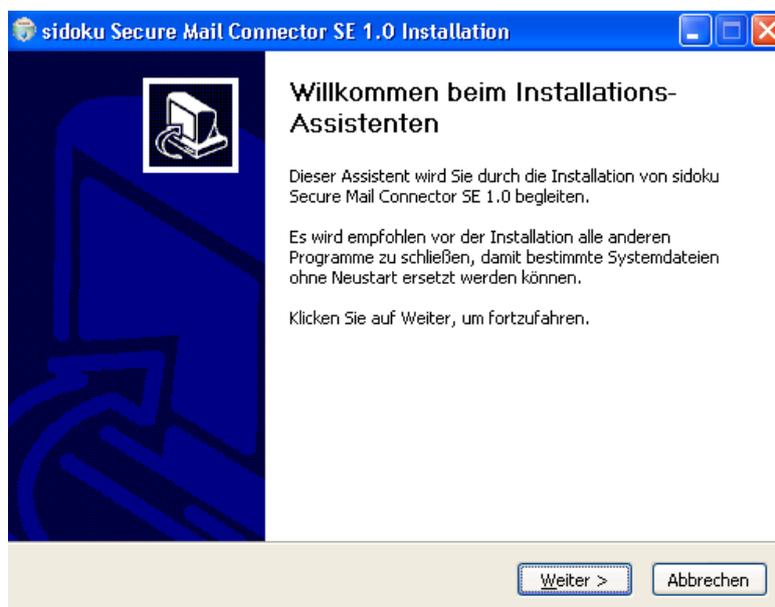


Abbildung 1: Installationsassistent

Bitte folgen Sie den Anweisungen des Installationsassistenten klicken die Schaltfläche „Weiter“.

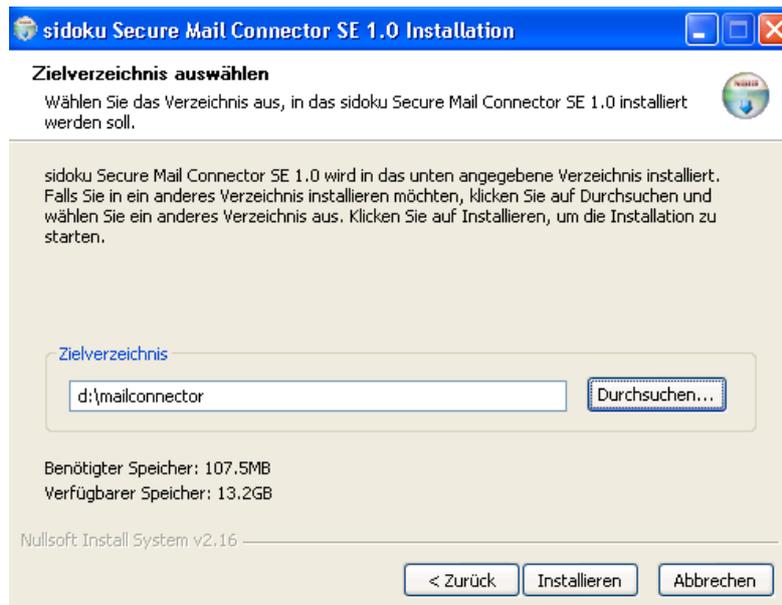


Abbildung 2: Zielverzeichnis wählen

Bitte geben Sie das Zielverzeichnis für die Datei an und klicken auf die Schaltfläche „Installieren“.

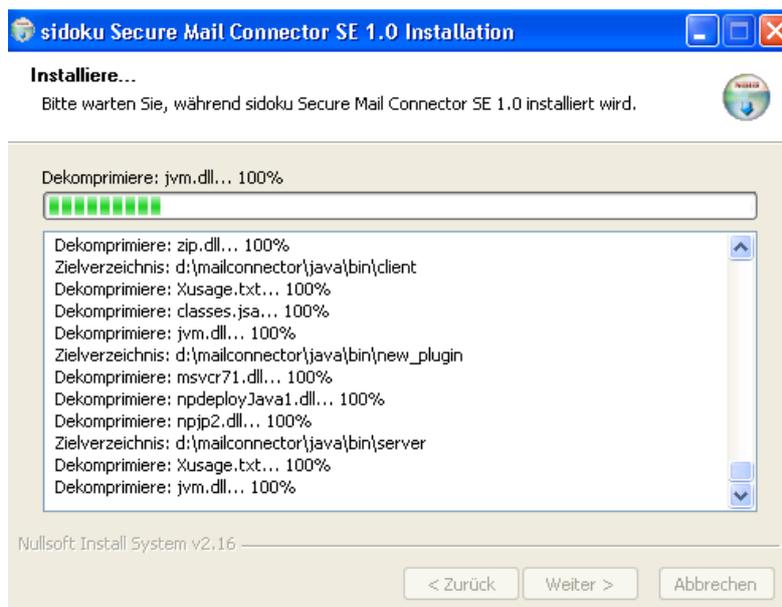


Abbildung 3: Installation

Der sidoku® Secure Mail Connector SE wird nun installiert. Bitte warten Sie bis die Installation abgeschlossen ist.

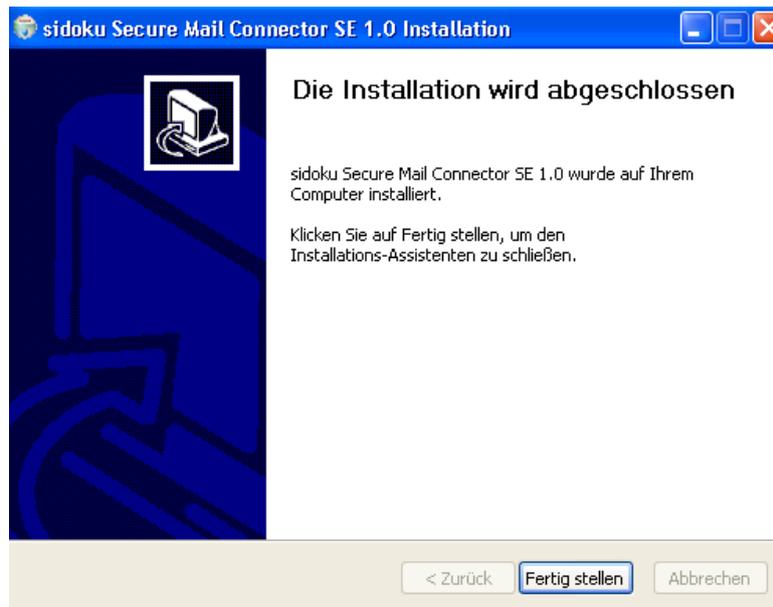


Abbildung 4: Installation abgeschlossen

Der sidoku® Secure Mail Connector SE ist fertig installiert, sobald Sie die Schaltfläche „Fertig stellen“ betätigen.

Der Einrichtungsassistent öffnet sich nach dem Download selbständig.

Sie können den Einrichtungsassistenten auch manuell starten, bspw. wenn Sie nach der Einrichtung noch Änderungen an den Eingaben vornehmen möchten.

Bitte klicken Sie dazu im Startmenü auf „sidoku® Secure Mail Connector SE/Einrichtungsassistent“.

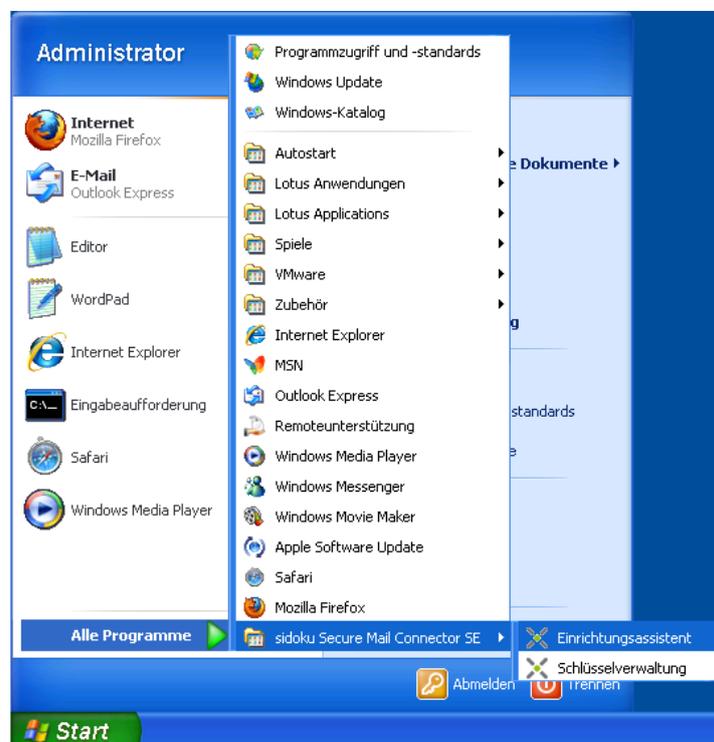


Abbildung 5: Einrichtungsassistent im Startmenü

4 sidoku® Secure Mail Connector SE Einrichtungsassistent

Hinweis:

Um eine einwandfreie Installation des sidoku® Secure Mail Connector SE sicher zu stellen, ist während des gesamten Einrichtungsprozesses eine Internetverbindung notwendig.

Nach dem Start des sidoku® Secure Mail Connector SE Einrichtungsassistenten erscheint das folgende Informationsfenster. Bitte folgen Sie den Anweisungen des Assistenten. Den nächsten Bearbeitungsschritt erreichen Sie immer über die Schaltfläche „weiter“.

Bitte klicken Sie nun auf die Schaltfläche „weiter“ und wechseln damit in die Registerkarte „Schlüsselpaar-Erzeugung“.



Abbildung 6: Start Einrichtungsassistent

4.1 Schlüsselpaar-Erzeugung

Die Erstellung des Systemschlüsselpaares bildet die Grundlage für die Nutzung des sidoku® Secure Mail Connector SE. Nur mit diesem Schlüsselpaar können die sidoku® Nachrichten ver- bzw. entschlüsselt werden. Das Schlüsselpaar besteht zum Einen aus einem öffentlichen Schlüssel, der am Ende des Einrichtungsassistenten an sidoku® übermittelt wird. Zum Anderen besteht es aus dem privaten Schlüssel, der ausschließlich auf dem Computer des sidoku® Secure Mail Connector SE abgelegt ist. Nur mit dem privaten Schlüssel können die Nachrichten entschlüsselt und gelesen werden.

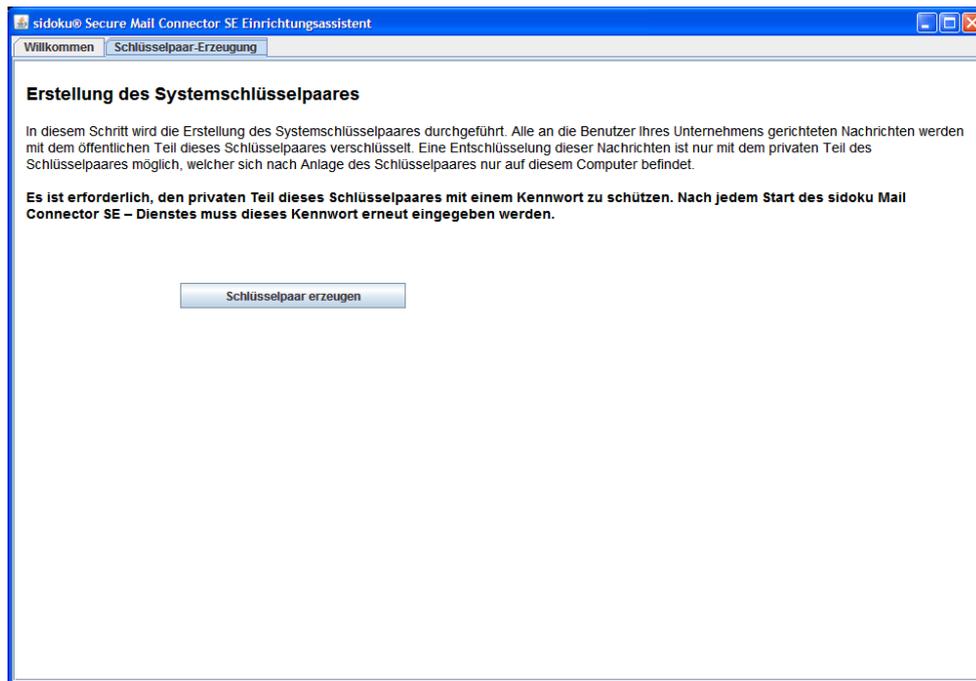


Abbildung 7: Schlüsselpaar-Erzeugung

Nach dem Betätigen der Schaltfläche „Schlüsselpaar erzeugen“ werden Sie darauf hingewiesen, dass ein Kennwort zum Schutz des Schlüssels vergeben werden muss.

Bitte bestätigen Sie dieses Informationsfenster mit „OK“.

Hinweis:

Dieses Kennwort muss bei jedem neuen Start des sidoku® Mail Connector SE-Dienstes eingegeben werden (siehe dazu Kapitel 6 Schlüsselverwaltung).

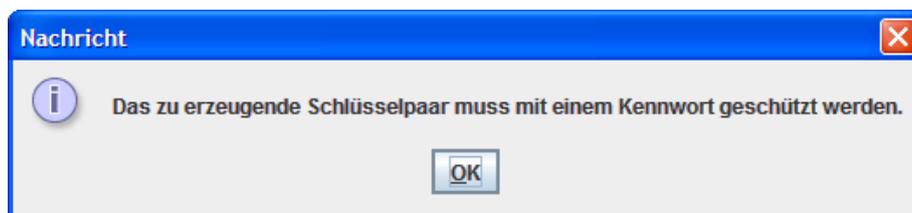


Abbildung 8: Information Kennwortvergabe

Sie werden jetzt zweimal aufgefordert das Kennwort einzugeben. Das Kennwort muss mindestens 8 Zeichen lang sein.

Die Eingaben werden jeweils mit „OK“ bestätigt.

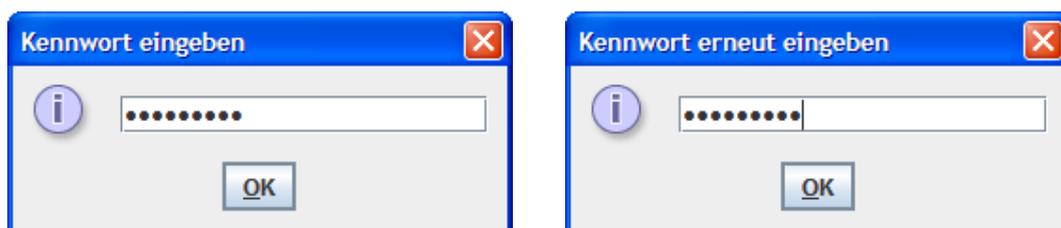


Abbildung 9: Kennworteingabe/Kennwortbestätigung

Im Anschluss an die Kennwortvergabe erhalten Sie die Bestätigung, dass der Systemschlüssel erfolgreich erstellt wurde.

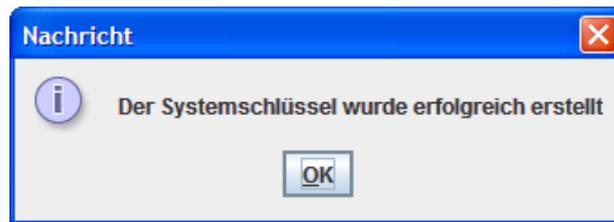


Abbildung 10: Systemschlüssel erstellt

Nach der Erstellung des Systemschlüssels öffnet sich der Einrichtungsassistent für die Inbetriebnahme des sidoku® Secure Mail Connector SE.

5 Inbetriebnahme des sidoku® Secure Mail Connector SE Einrichtungsassistenten

Mit Hilfe des Einrichtungsassistenten (*Abbildung 11*) kann jetzt die Inbetriebnahme des sidoku® Secure Mail Connector SE vorgenommen werden. Bitte folgen Sie weiterhin den Anweisungen des Assistenten. Während des gesamten Eingabevorgangs ist ein Wechsel zwischen den einzelnen Registerkarten möglich, ohne die bisher gemachten Eingaben zu verwerfen.

Den nächsten Arbeitsschritt erreichen Sie jeweils mit der Schaltfläche „weiter“, Sie können aber auch direkt auf die Registerkarten klicken. Bitte beachten Sie, dass für die einwandfreie Installation die vorgegebene Reihenfolge bei der Dateneingabe eingehalten werden muss.

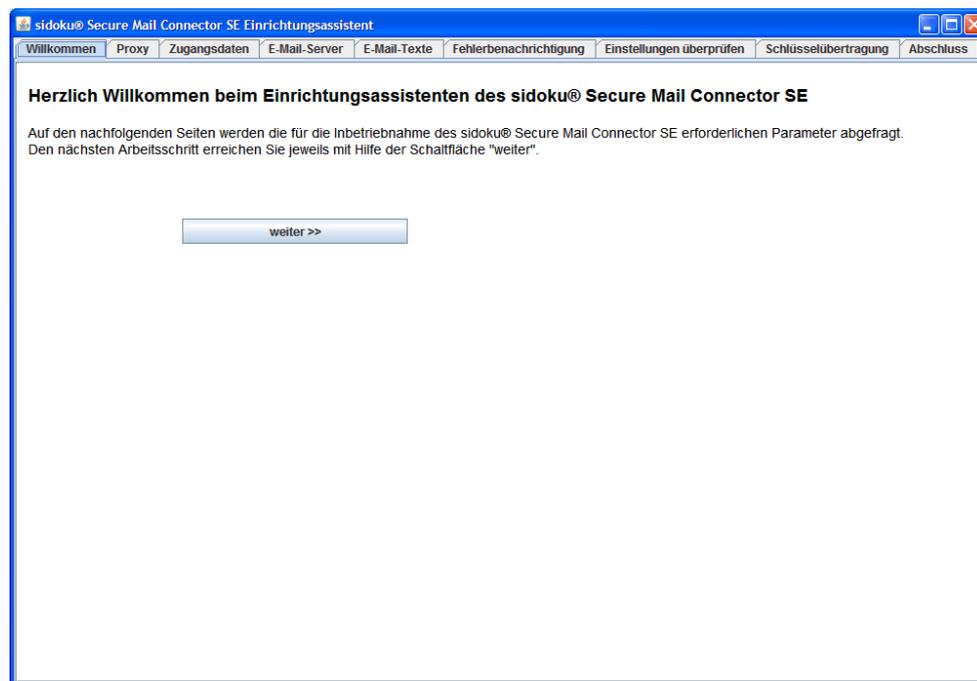


Abbildung 11: Einrichtungsassistent Inbetriebnahme

5.1 Einstellungen Proxy-Server

Wenn für den Zugriff auf das Internet ein Proxy-Server verwendet werden soll, geben Sie bitte an dieser Stelle die dazu notwendigen Daten ein. Wird kein Proxy-Server verwendet, lassen Sie die Felder leer und gehen direkt über die Schaltfläche „weiter“ zum nächsten Eingabeschritt. Die Schaltfläche  bietet Ihnen eine kleine Erläuterung zum jeweiligen Feld (*Abbildung 13*).

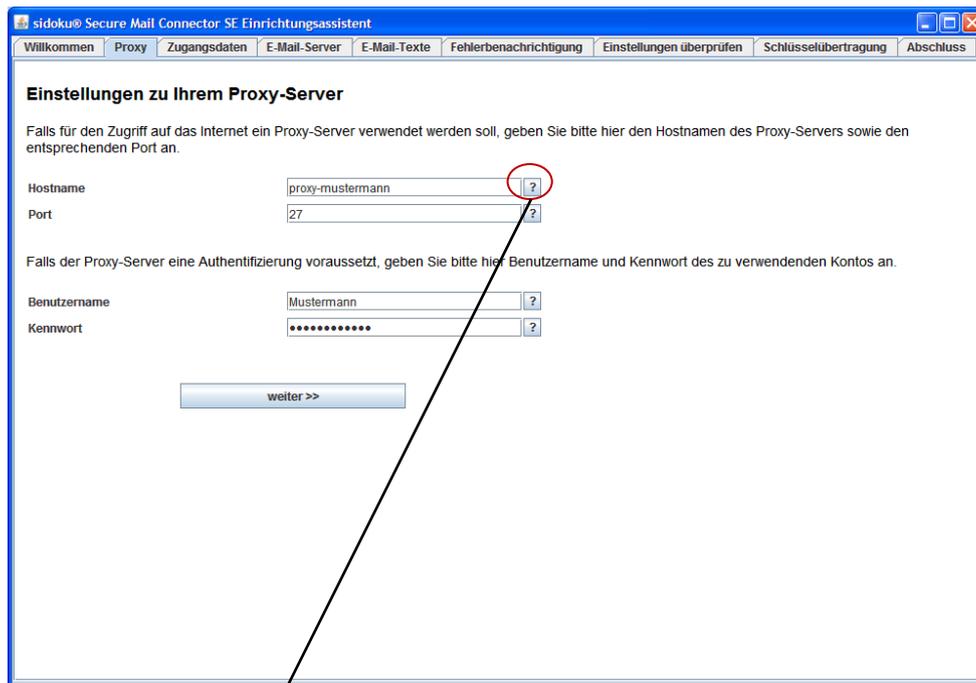


Abbildung 12: Einstellungen Proxy-Server



Abbildung 13: Anzeige Hilfetext

5.2 Zugangsdaten

Im Rahmen der Registrierung im zentralen sidoku® System haben Sie für die Synchronisierung Zugangsdaten für das sidoku®-Replikationskonto erhalten.

An dieser Stelle ist es notwendig zwischen Unternehmensbezogener Synchronisierung und Kontobezogener Synchronisierung zu unterscheiden.

5.2.1 Unternehmensbezogene Synchronisierung

Die unternehmensbezogene Synchronisierung ist die bevorzugte Betriebsart, wenn Sie über ein eigenes Unternehmenskonto im sidoku®-System verfügen. Über dieses Konto sind alle Ihre Mitarbeiter an sidoku® angeschlossen und mit ihren E-Mail-Adressen eingetragen. Innerhalb des sidoku® Secure Mail Connector SE wird ein Replikationsbenutzer des Unternehmens konfiguriert. Die Kommunikation und Verschlüsselung des sidoku®-Systems erfolgt über diesen Replikationsbenutzer. Der einzelne Mitarbeiter des Unternehmens schaltet sich selbst mit Hilfe des Profil-Vorgangs im sidoku®-Portal für die Replikation frei (siehe Handbuch „Replikation mit sidoku® Secure Mail Connector freischalten“). Ab diesem Zeitpunkt kann der Benutzer über seinen E-Mail-Client Nachrichten an die sidoku®-Mail-Adressen seiner Geschäftspartner verschicken. Eingehende Nachrichten werden für diese Benutzer vom sidoku® Secure Mail Connector SE abgerufen und intern per Email zugestellt.

Das hat den Vorteil, dass kein weiterer Administrationsaufwand am sidoku® Secure Mail Connector SE bei der Anlage neuer Benutzer notwendig ist.

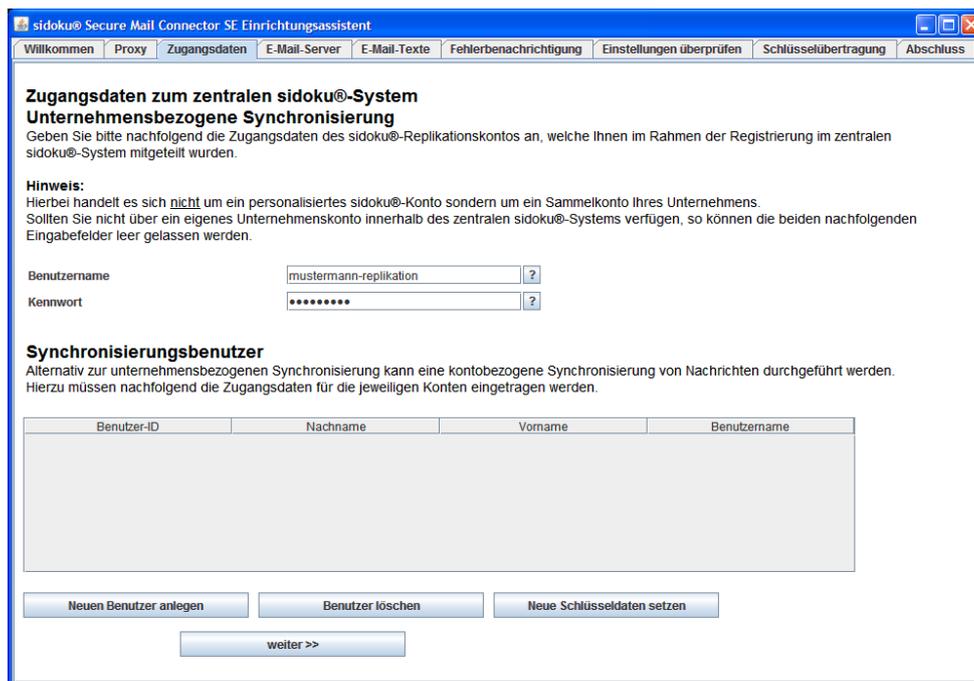


Abbildung 14: Zugangsdaten

5.2.2 Kontobezogene Synchronisierung

Die Kontobezogene Synchronisierung wird gewählt, wenn Sie kein Unternehmenskonto im sidoku®-System haben, sondern als Geschäftspartner eines Unternehmens am sicheren Dokumentenaustausch teilnehmen. Die kontobezogene Synchronisierung bietet Ihnen als Geschäftspartner die Möglichkeit, sidoku® in Ihre gewohnte E-Mail-Anwendung zu integrieren.

Dafür ist es erforderlich jeden Synchronisierungsbenutzer einzeln als Benutzer einzutragen. Mit der Schaltfläche „Benutzer löschen“ kann ein angelegter Benutzer jederzeit wieder aus dem System entfernt werden.

Um einen neuen Benutzer anzulegen, klicken Sie bitte auf die Schaltfläche „Neuen Benutzer anlegen“. Es öffnet sich ein Fenster zur Eingabe des Benutzernamens und eines Kennwortes (Abbildung 15). Bitte beachten Sie dabei, dass Benutzername und die intern verwendete E-Mail-Adresse identisch sein müssen.

Nach der Eingabe betätigen Sie bitte die Schaltfläche „Benutzerdaten abrufen“ (Abbildung 15). Damit wird der neue Synchronisierungsbenutzer in den Benutzerbestand des sidoku® Secure Mail Connector SE hinzugefügt (Abbildung 16). Bitte bestätigen Sie die Angaben mit der Schaltfläche „Ja“.

Im Anschluss daran erhalten Sie vom System noch eine Nachricht über die erfolgreiche Anlage des neuen Benutzers (Abbildung 17), die Sie bitte mit der Schaltfläche „OK“ bestätigen.

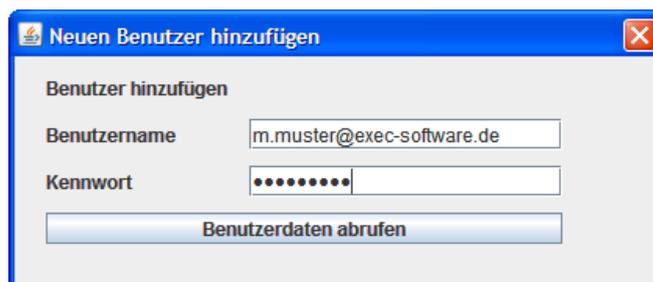


Abbildung 15: Neuen Benutzer anlegen

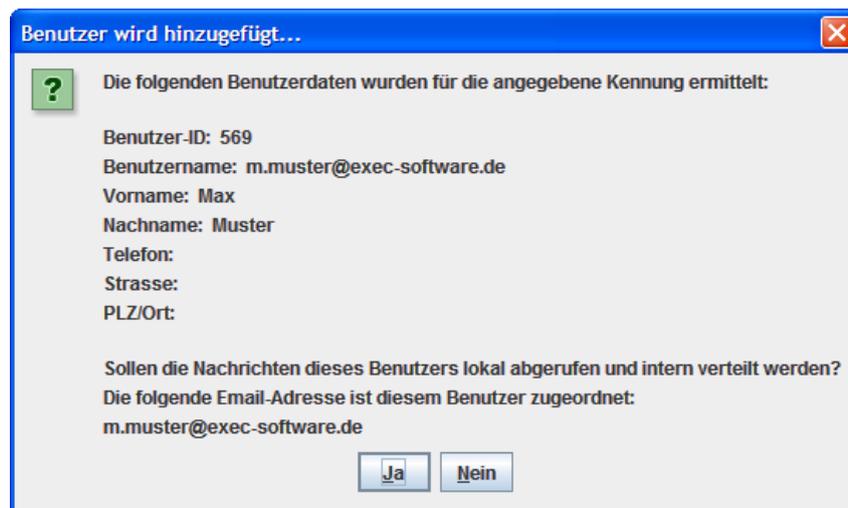


Abbildung 16: Benutzer wird hinzugefügt

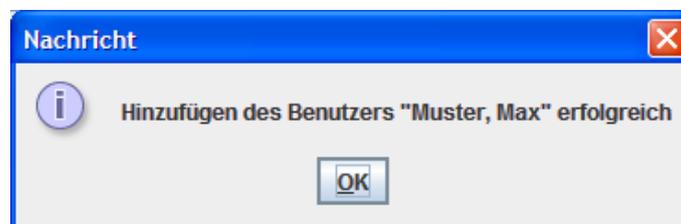


Abbildung 17: Benutzer erfolgreich hinzugefügt

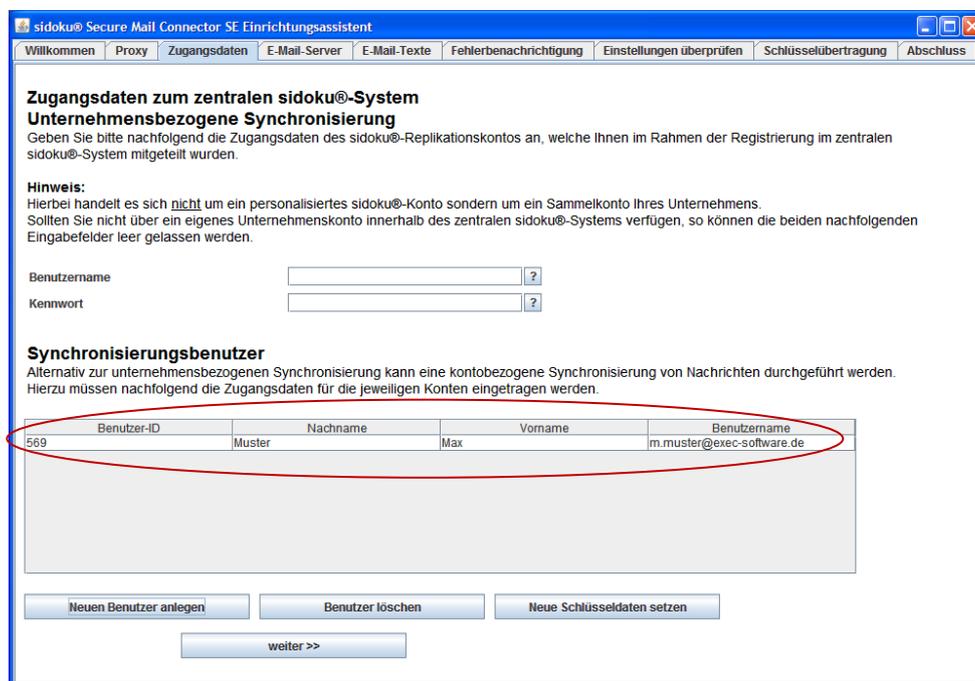


Abbildung 18: Synchronisierungsbutzer Tabelleneintrag

Diesen Vorgang wiederholen Sie bis alle Synchronisierungsbutzer angelegt sind.

5.2.2.1 Neue Schlüsseldaten setzen

Das Schlüsselpaar für jeden Synchronisierungsbutzer wird im Rechenzentrum der EXEC Software Team GmbH abgelegt, der private Teil des Schlüssels ist mit Ihrem Kennwort verschlüsselt. Für den Fall, dass Ihnen diese Sicherheit nicht ausreichend erscheint, können Sie mit Hilfe der Schaltfläche

„Neue Schlüsseldaten setzen“ (Abbildung 19) für jeden Synchronisierungsbenutzer einzeln neue Schlüsseldaten generieren. Sie erreichen damit eine Ende-zu-Ende-Verschlüsselung. Der private Teil des neuen Schlüssels wird dann bei Ihnen auf dem internen Mailserver, auf dem der sidoku® Secure Mail Connector SE Dienst installiert ist, abgelegt. Der Schutz des privaten Schlüssels/des Kennwortes erfolgt über den Systemschlüssel. Der öffentliche Teil des Schlüssels wird an das zentrale sidoku®-System übermittelt.

Hinweis:

Bitte beachten Sie, dass das Setzen neuer Schlüsseldaten zur Folge hat, dass der sichere Dokumentenaustausch ausschließlich über den sidoku® Secure Mail Connector SE erfolgen kann. Die Benutzer können keine Nachrichten mehr über das sidoku®-Portal versenden bzw. erhalten.

Zum Setzen neuer Schlüsseldaten markieren Sie bitte den jeweiligen Benutzer in der Tabelle und klicken dann auf die Schaltfläche „Neue Schlüsseldaten setzen“ (Abbildung 19).

Sie erhalten daraufhin eine Systemabfrage, ob für den betreffenden Benutzer ein neues Schlüsselpaar generiert werden soll (Abbildung 20). Nachdem Sie diese Abfrage mit der Schaltfläche „Ja“ bestätigt haben, erhalten Sie eine Systemnachricht, dass der öffentliche Teil des neu generierten Schlüsselpaares erfolgreich übertragen wurde (Abbildung 21).

Die neuen Schlüsseldaten sind nun gesetzt, die bisher gültigen Schlüsseldaten wurden im System gelöscht.

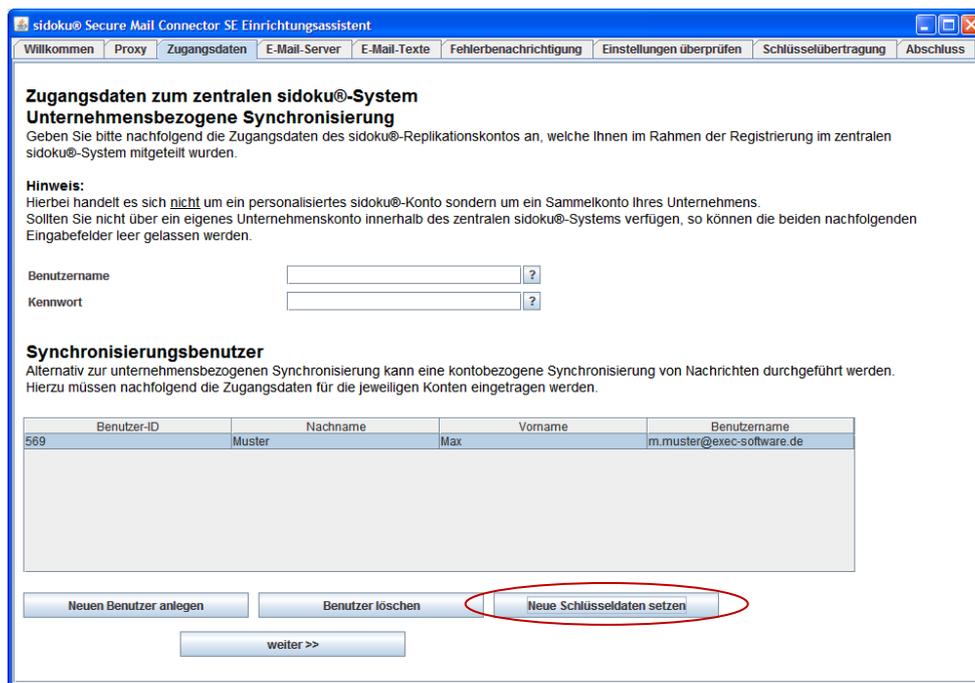


Abbildung 19: Neue Schlüsseldaten setzen

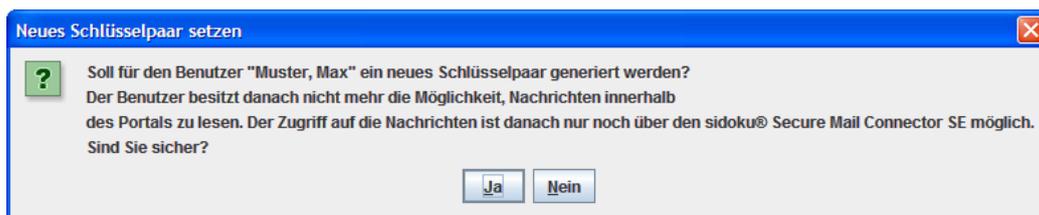


Abbildung 20: Neues Schlüsselpaar setzen

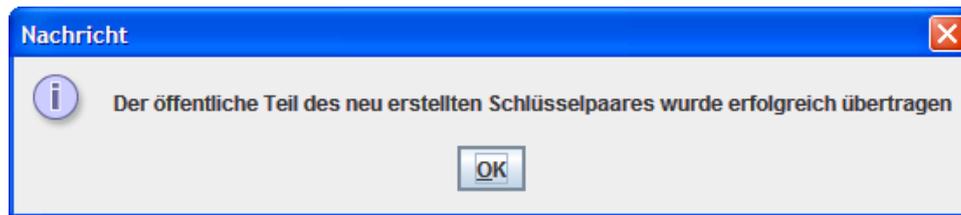


Abbildung 21: Erfolgreiche Übertragung

5.3 E-Mail-Server

An dieser Stelle werden die Daten zu Ihrem Unternehmens-Mailserver abgefragt. Bitte geben Sie den Hostnamen und den Port des Servers an, über welchen die eingehenden Nachrichten im internen Netzwerk verteilt werden sollen. Desweiteren wird die E-Mail-Domain Ihres Unternehmens benötigt. Sollten Sie mehrere Domains für Ihr Unternehmen haben, werden diese durch ein Semikolon getrennt hintereinander eingetragen.

Der Port zur lokalen SMTP-Schnittstelle ist standardmäßig auf den TCP-Port 25 eingestellt. Sollte der Port auf diesem Rechner bereits durch einen anderen Dienst belegt sein, haben Sie an dieser Stelle die Möglichkeit, einen anderen, freien TCP-Port einzutragen.

Bitte denken Sie daran, dass für den Versand der sidoku Nachrichten der interne E-Mailserver dahingehend konfiguriert werden muss, dass E-Mails, die an die Domain *.sidoku.de versendet werden, an den Server weitergeleitet werden, auf dem der sidoku® Secure Mail Connector SE betrieben wird.

Falls Sie also einen anderen als den standardmäßig vorgesehenen TCP-Port eintragen, stellen Sie bitte sicher, dass auch an Ihrem internen E-Mailserver der neue TCP-Port konfiguriert ist.

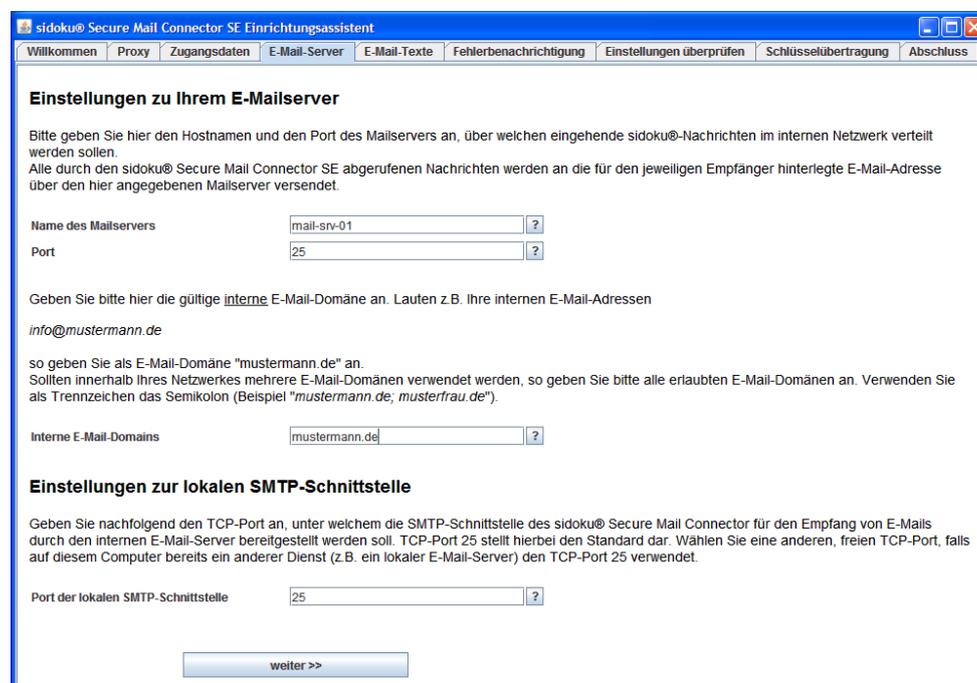


Abbildung 20: Einstellungen Mailserver / lokale SMTP Schnittstelle

5.4 E-Mail-Texte

Sie können alle E-Mails, die über den sidoku® Secure Mail Connector SE an den internen Mailserver weitergeleitet werden mit einem festgelegten Begleittext versehen. Dies gibt dem Benutzer beim

Öffnen der E-Mail auf den ersten Blick die Information, dass es sich bei der erhaltenen Nachricht um eine sidoku®-Nachricht handelt. Diesen Informationstext können Sie selber konfigurieren.

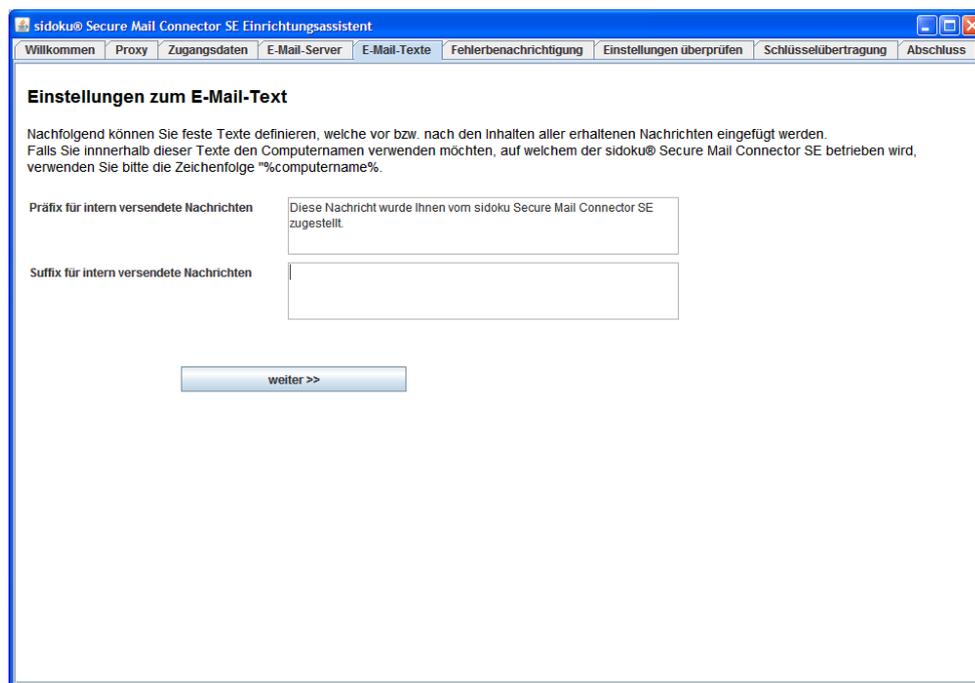


Abbildung 21: Einstellungen zum E-Mail Text

5.5 Fehlerbenachrichtigung

Der sidoku® Secure Mail Connector SE protokolliert Fehler und Warnungen in Logdateien. Zusätzlich besteht die Möglichkeit Fehler bzw. Warnungen per E-Mail zu versenden. Es wird empfohlen diesen Dienst in Anspruch zu nehmen.

Wenn Sie diese Benachrichtigungen wünschen, setzen Sie bitte das Häkchen in der Zeile „Fehlermeldungen per E-Mail versenden“. Desweiteren werden nochmals die Daten zum Mailserver sowie der Port des Mailservers benötigt.

In der Zeile „Absenderadresse“ können Sie eine E-Mail-Adresse kreieren, die ausschließlich für diese Warnmeldungen verwendet wird. Das ermöglicht Ihnen beim Umgang mit dem sidoku® Secure Mail Connector SE die eindeutige Zuordnung der Mails auf einen Blick. Anhand der Absenderadresse können Sie in Ihrer E-Mail-Integration auf den ersten Blick bereits sehen, dass es sich um Fehlermeldungen handelt.

In der Zeile „Empfängeradresse“ sollte die E-Mail des Administrators eingetragen werden.

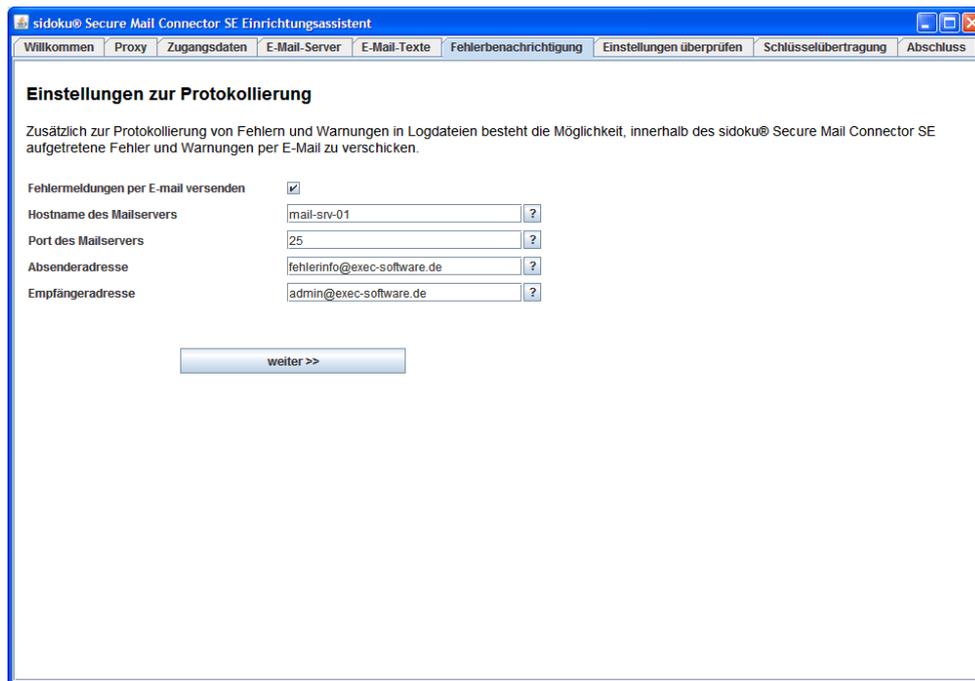


Abbildung 22: Einstellungen Protokollierung

5.6 Einstellungen überprüfen

Mit der Schaltfläche „Einstellungen überprüfen“ werden folgende Eintragungen überprüft:

- Verbindungsaufbau zum sidoku®-Webservice
- Verbindungsaufbau zu den konfigurierten E-Mailservern
- Prüfung der Verfügbarkeit des konfigurierten lokalen SMTP-Ports

Bitte beachten Sie, dass die Verbindungsprüfung nur dann erfolgreich durchgeführt werden kann, wenn eine Internetverbindung aufgebaut ist.

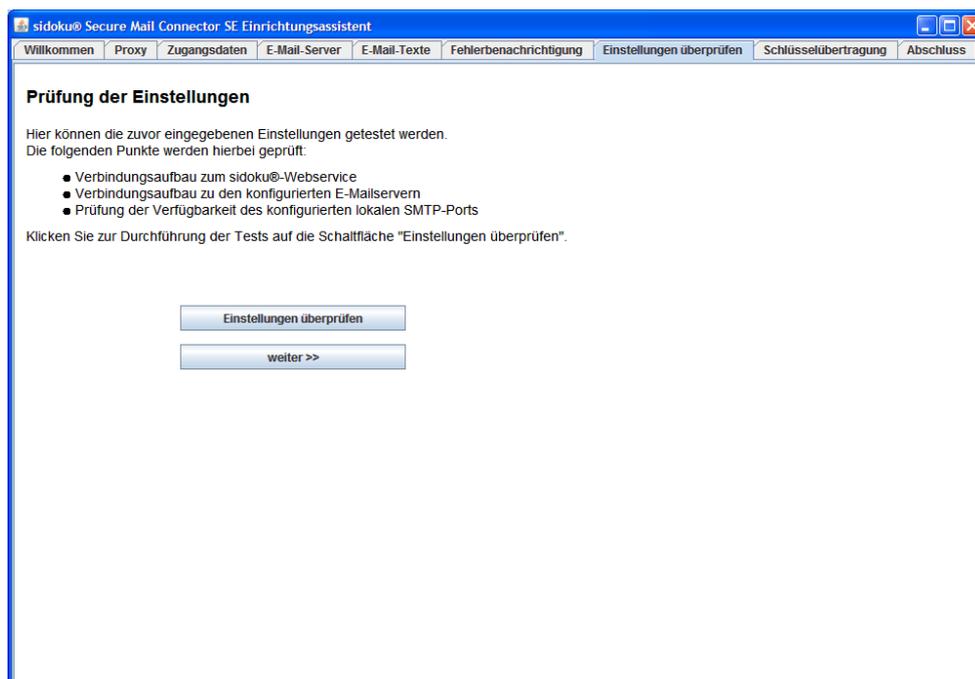


Abbildung 23: Einstellungen überprüfen

Nach der Verbindungsprüfung erscheint ein Fenster mit den Ergebnissen. Sollte hierbei ein Fehler aufgetreten sein, können Sie direkt in die jeweilige Registerkarte zurückgehen und den Eintrag dort überprüfen und korrigieren. Danach ist eine erneute Verbindungsprüfung möglich. Bitte wiederholen Sie diesen Vorgang gegebenenfalls solange bis die Verbindungsprüfung alle Parameter erfolgreich geprüft hat. Der sidoku® Secure Mail Connector SE kann nur dann erfolgreich gestartet werden, wenn alle Eingaben korrekt sind.

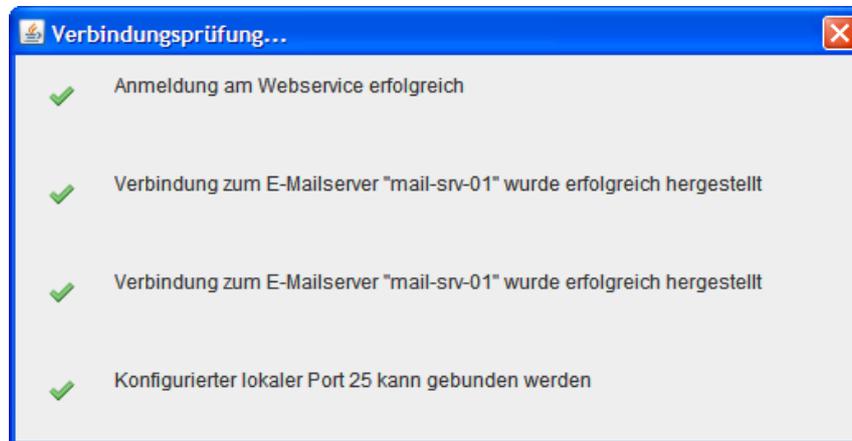


Abbildung 24: Verbindungsprüfung

5.7 Schlüsselübertragung

Der in Punkt „4.1 Schlüsselpaarerzeugung“ erzeugte öffentliche Teil des Schlüsselpaares muss an das zentrale sidoku®-System übertragen werden. Der öffentliche Teil des Systemschlüssels ermöglicht die Übertragung der Nachrichten mit Hilfe des sidoku® Secure Mail Connector SE.

Bitte stellen Sie sicher, dass eine Internetverbindung besteht und betätigen Sie die Schaltfläche „Öffentlichen Schlüssel übertragen“. Im Anschluss erhalten Sie eine Übertragungsbestätigung (Abbildung 26).

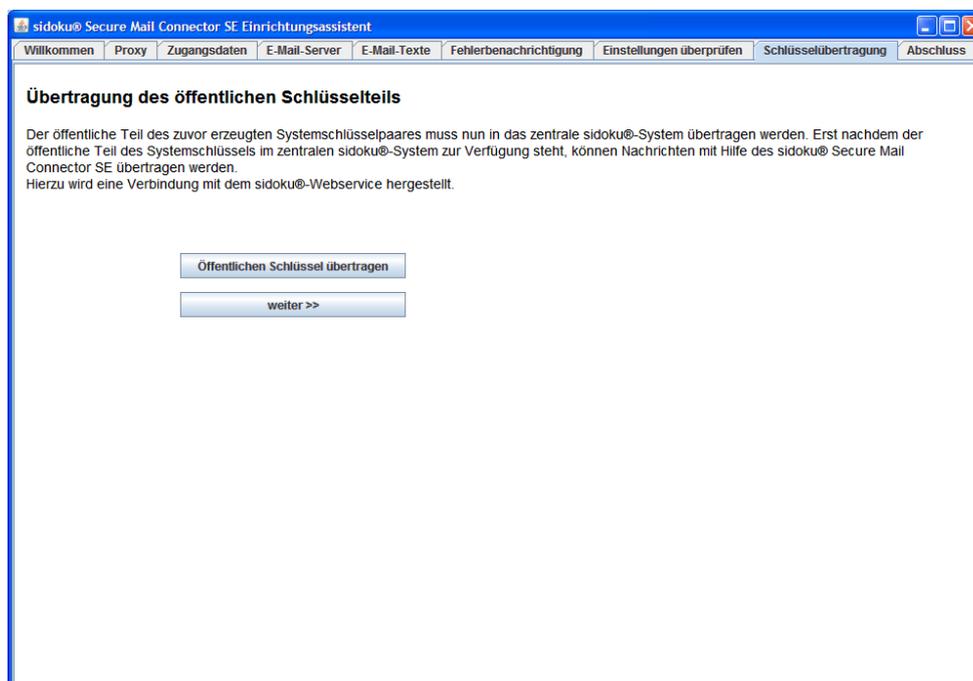


Abbildung 25: Schlüsselübertragung

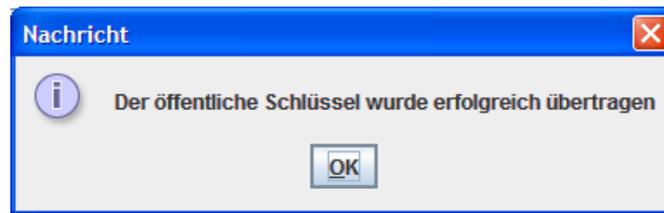


Abbildung 26: Erfolgreiche Schlüsselübertragung

5.8 Abschluss

Sie haben die letzte Registerkarte des Einrichtungsassistenten erreicht. Um die Einrichtung des sidoku® Secure Mail Connector SE abzuschließen, betätigen Sie bitte die Schaltfläche „Einstellungen speichern“. Alle vorgenommenen Einstellungen werden jetzt gespeichert. Sie erhalten eine Nachricht vom System über die erfolgreiche Speicherung (Abbildung 28).

Sollten im Nachhinein noch Änderungen an den Konfigurationsparametern notwendig sein, können diese mit dem Einrichtungsassistenten vorgenommen werden.

Sie können nun den sidoku® Secure Mail Connector SE Dienst mit der Schaltfläche „Dienst starten“ in Betrieb nehmen.

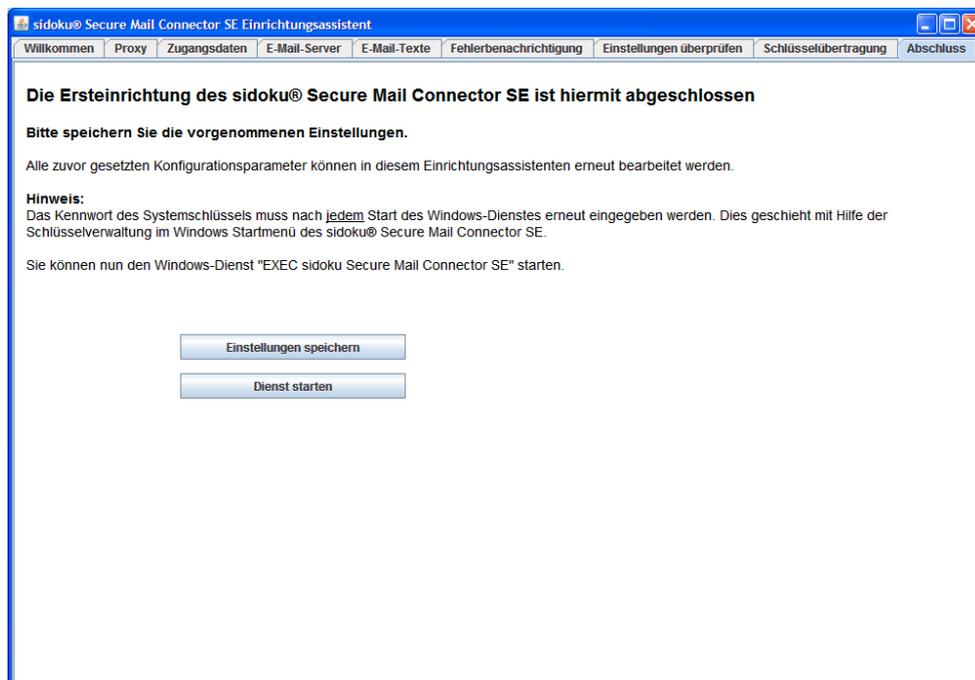


Abbildung 27: Ersteinrichtung abschließen

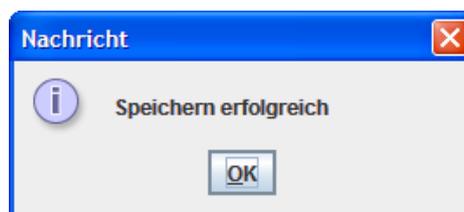


Abbildung 28: Einstellungen erfolgreich gespeichert

6 Schlüsselverwaltung

Wie bereits in Kapitel 4 Schlüsselpaar-Erzeugung erwähnt, ist es notwendig bei jedem Neustart des sidoku® Secure Mail Connector SE das Programm mit dem vergebenen Kennwort freizuschalten.

Bitte rufen Sie im Windows Startmenü das Programm sidoku® Secure Mail Connector SE auf und wählen als nächsten Unterpunkt die Schlüsselverwaltung. Es öffnet sich ein Fenster zur Schlüsselaktivierung (*Abbildung 30*). Nach der Eingabe des Kennwortes bestätigen Sie bitte mit der Schaltfläche „OK“. Der Dienst ist nun freigeschaltet.



Abbildung 29: Schlüsselverwaltung



Abbildung 30: Schlüsselaktivierung

7 Installation auf einem Linux-Betriebssystem

Alternativ zur Installation auf einem Windows-Betriebssystem, kann der sidoku® Secure Mail Connector SE auch auf einem Linux-Betriebssystem installiert werden. Nachfolgend werden die Unterschiede zur Installation auf einem Windows-Betriebssystem beschrieben.

7.1 Installation der Dateien

Der Standard-Installationspfad des sidoku® Secure Mail Connector SE lautet `"/opt/exec/mc"`. Dieses Verzeichnis ist manuell zu erstellen. Innerhalb dieses Verzeichnisses ist das Installationsarchiv `"mc-tar.gz"` zu entpacken.

7.2 Start des Konfigurationsassistenten

Der Konfigurationsassistent des sidoku® Secure Mail Connector SE kann mit Hilfe des Skriptes "wizard.sh" gestartet werden. Bitte beachten Sie hierbei, dass für die Anzeige des Konfigurationsassistenten eine grafische Benutzeroberfläche (X-Windows) benötigt wird.

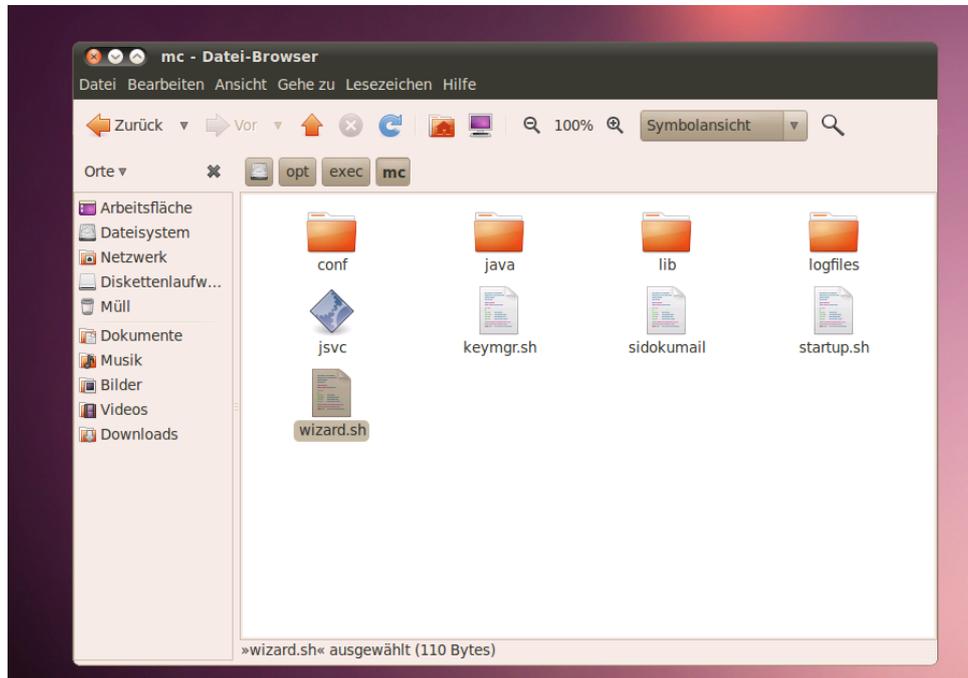


Abbildung 31: mc-Datei-Browser

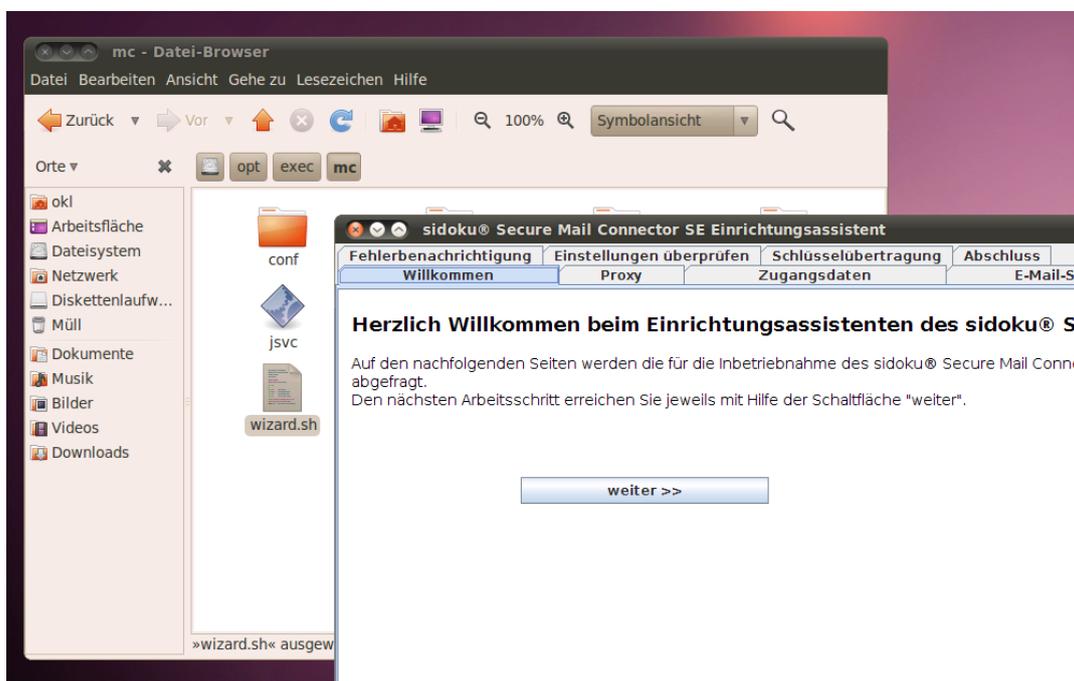


Abbildung 32: Start des sidoku® Secure Mail Connector SE

7.3 Einrichtung des Dienstes

Zur Ausführung des sidoku® Secure Mail Connector SE als Hintergrund-Prozess kann das mitgelieferte Shell-Skript "sidokumail" verwendet werden.

Der Start des sidoku® Secure Mail Connector SE erfolgt durch Aufruf des Shell-Skriptes mit dem Parameter "start":

```
./sidokumail start
```

Das Stoppen des Hintergrundprozesses erfolgt durch Aufruf des Shell-Skriptes mit dem Parameter "stop":

```
./sidokumail stop
```

Bitte beachten Sie, dass für das Starten und Stoppen des Dienstes über dieses Shell-Skript Administrator-Berechtigungen (root-Rechte) benötigt werden. Der Dienst selbst wird nach dem Start unter dem Betriebssystem-Benutzer "www-data" ausgeführt.

7.4 Start der Schlüsselverwaltung

Die Schlüsselverwaltungs-Applikation des sidoku® Secure Mail Connector SE kann mit Hilfe des Skriptes "keymgr.sh" innerhalb des Installationsverzeichnis gestartet werden. Für die Anzeige des Konfigurationsassistenten wird eine grafische Benutzeroberfläche (X-Windows) benötigt.

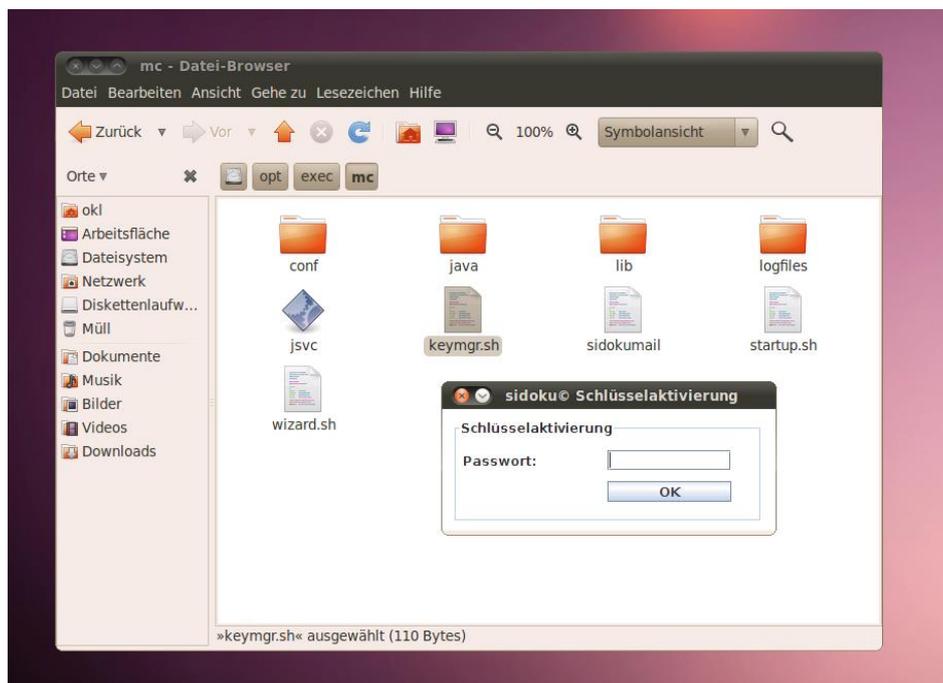


Abbildung 33: sidoku® Schlüsselaktivierung