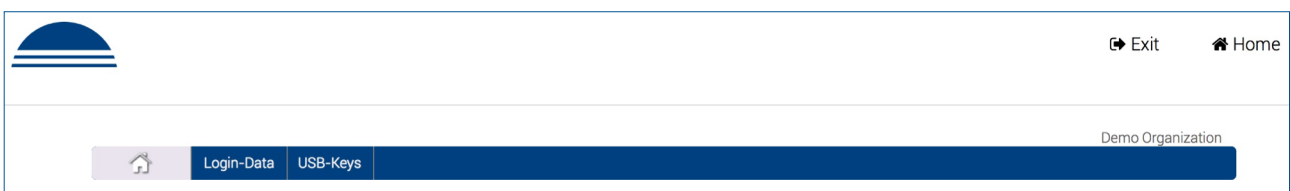




Phrase-Lock Enterprise-Services bieten eine sehr einfache Möglichkeiten, Login-Daten zu bearbeiten, zu verteilen und zu synchronisieren. Privatpersonen können damit für ihren USB-Key online sehr einfach Login-Daten anlegen und verwalten. Professionelle Anwender verfügen über eine



weit reichende Lizenz und verwalten damit eine beliebige Anzahl von USB-Keys.

Bitte lesen Sie diese Anleitung aufmerksam durch - es geht schließlich um Ihre Daten! Manche Details erscheinen etwas technisch, wir sehen uns aber der transparenten Darstellung verpflichtet um der Leserin/dem Leser zu vermitteln, dass wir in der Lage sind mit Geheimnissen - Ihren Login-Daten - umzugehen ohne diese inhaltlich kennen zu müssen.

***Bitte beachten Sie:** Phrase-Lock Enterprise-Services überschneiden sich teilweise mit den Backup- und Wiederherstellungsfunktionen. Sie stellen aber keinen Ersatz für aktuelle Backups dar.*

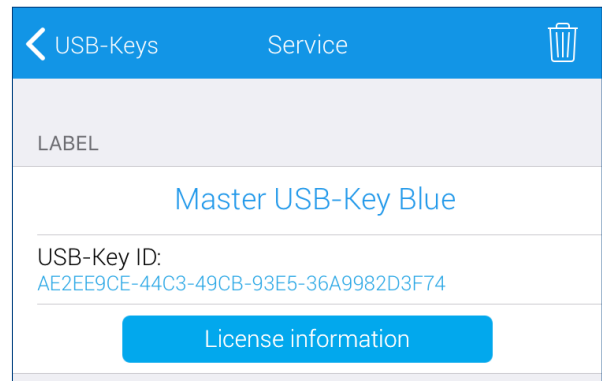
Aktivierung der Enterprise-Services

Die Enterprise-Services müssen zuerst mit einer Lizenzabfrage aktiviert werden. Danach wird ein Synchronisationsschlüssel mit PIN-Code, im folgenden Text als S-Key bezeichnet, angelegt. Dieser S-Key ist notwendig um Login-Daten für andere USB-Keys, bzw. deren Anwender, verfügbar zu machen.

Mit dem S-Key werden Login-Daten wie in einer Transportbox mit Schloss versperrt und nur jene Personen, die auch den PIN-Code kennen, sind in der Lage die Login-Daten einzulesen. Auf technischer Ebene ist das wesentlich komplexer und sicherer als die simple Analogie einer Transportbox. Eine detaillierte Darstellung der gesamten Verschlüsselungskette sprengt jedoch den Rahmen dieser Anleitung.

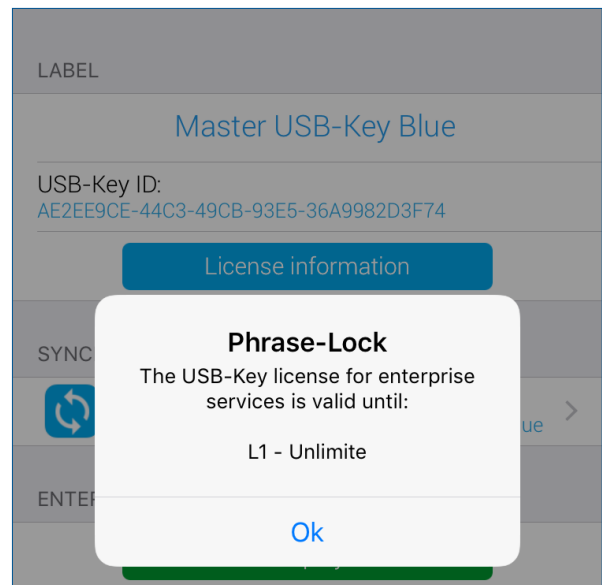
***Bitte beachten Sie:** Diese Anleitung setzt voraus, dass ein USB-Key auf einem Telefon installiert ist und hierfür auch ein persönlicher Schlüssel angelegt wurde, um bspw. die Backup- und Wiederherstellungsfunktionen nutzen zu können. Es wird des Weiteren vorausgesetzt, dass der Anwender auf seinem Telefon Login-Daten anlegen und bearbeiten kann, bzw. dies bereits getan hat.*

Im ersten Schritt tippen Sie bitte auf **Einstellungen - USB-Key verwalten - Auswahl des gewünschten USB-Keys**.

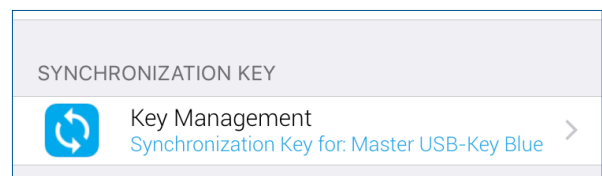


Jetzt tippen Sie auf den blauen Button **Licence information (Lizenzauskunft)**.

Wenn für den zuvor ausgewählten USB-Key eine entsprechende Lizenz für Enterprise-Services existiert, wird diese im Meldungsfenster mit der Gültigkeitsdauer angezeigt.

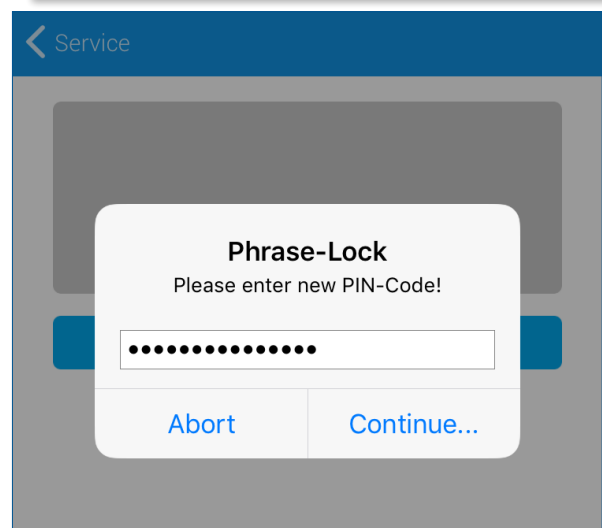


Quittieren Sie nun bitte das Meldungsfenster und tippen Sie auf den neuen Menüpunkt **Key Management (Schlüsselverwaltung)**.



Tippen Sie auf **Initiate Key (Schlüssel erzeugen...)** und geben Sie einen PIN-Code ein.

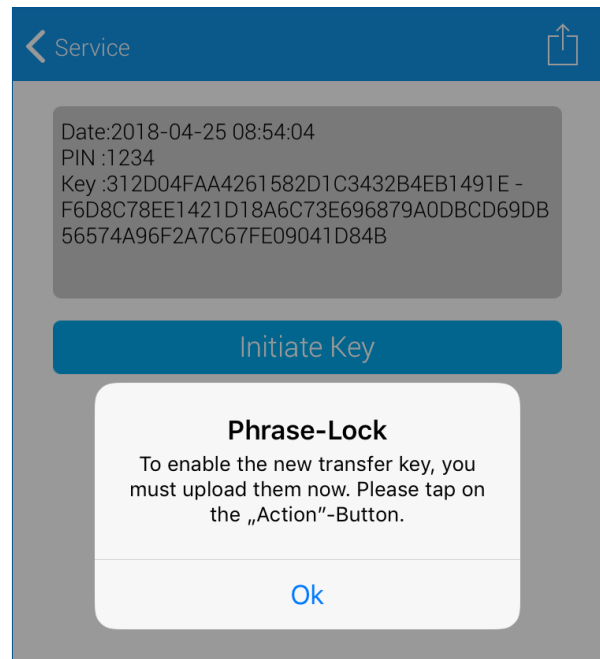
Tippen Sie auf **Continue (Weiter...)** und beachten Sie das Meldungsfenster! Lesen Sie den Hinweis und führen Sie bitte den nächsten Schritt aus.



Tippen Sie nun auf den **Aktions-Button** rechts-oben, beachten das Meldungsfenster und quittieren es, nachdem Sie den Hinweis gelesen haben.

Der S-Key ist jetzt bereit und Sie können beginnen die Enterprise-Services zu nutzen.

***Bitte beachten Sie:** Die Phrase-Lock Enterprise-Services sind Serviceleistungen der Betreiberin iPoxo IT GmbH, die über deren Infrastruktur (Server) angeboten werden. Die auf dem Telefon des Anwenders erzeugten S-Keys werden in dieser Infrastruktur **doppelt** verschlüsselt gespeichert. Die erste Verschlüsselung erfolgt mit einem Schlüssel, der aus dem PIN-Code errechnet wird. Diese Verschlüsselung erfolgt ausschließlich auf dem Telefon des Anwenders. Nach der Übertragung des bereits verschlüsselten S-Key an den Server wird dieser nochmals innerhalb der Datenbank verschlüsselt.*



*Es ist somit für die Betreiberin iPoxo IT GmbH oder deren Mitarbeiter ohne Kenntnis des PIN-Codes nicht möglich, S-Keys oder damit synchronisierte Login-Daten ihrer Kunden im Klartext zu sehen oder sichtbar zu machen. Jegliche dem Anwender zugeordnete Daten sind nur über dessen USB-Key und dem Enterprise-Service-Login zugänglich bzw. es besteht eine strikte **Mandantentrennung** der Daten durch den USB-Key. Dieses restriktive Vorgehen in Bezug auf Verschlüsselung schützt sowohl die Daten der Anwender als auch uns selbst davor die Daten unserer Kunden im Klartext einsehen zu können. Ohne Kenntnis des PIN-Codes ist eine Dechiffrierung der Kundendaten technisch nicht möglich. Dementsprechend empfehlen wir für den PIN-Code eine entsprechende Komplexität.*

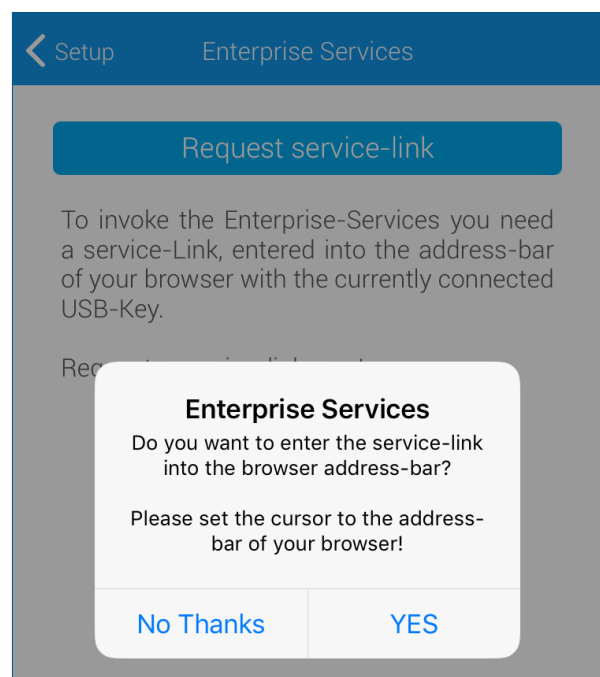
Einloggen zu den Enterprise-Services

Zu den Enterprise-Services gelangen Sie über den Menüpunkt **Enterprise Services Login** in den Einstellungen. Wählen Sie diesen Menüpunkt aus und fordern Sie einen Service-Link an.

Es erscheint danach ein Meldungsfenster. Lesen Sie bitte den Hinweis, öffnen ein Browser-Fenster und richten den Cursor in die Adresszeile.

Tippen Sie jetzt auf **YES (Ja)** im Meldungsfenster und der Enterprise-Service-Login-Link wird in die Adresszeile des Browser automatisch eingegeben.

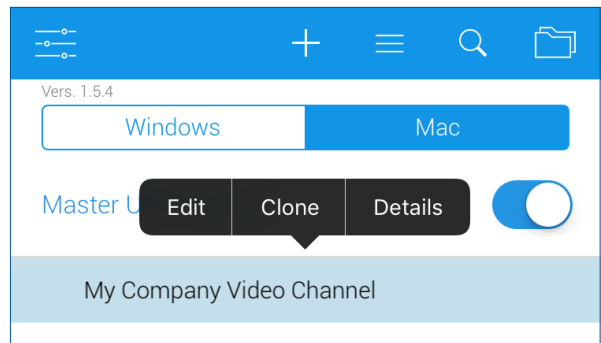
Nachdem die Seite geladen wurde, sehen Sie die Ihrer Lizenz entsprechenden Menüs der Enterprise-Services.



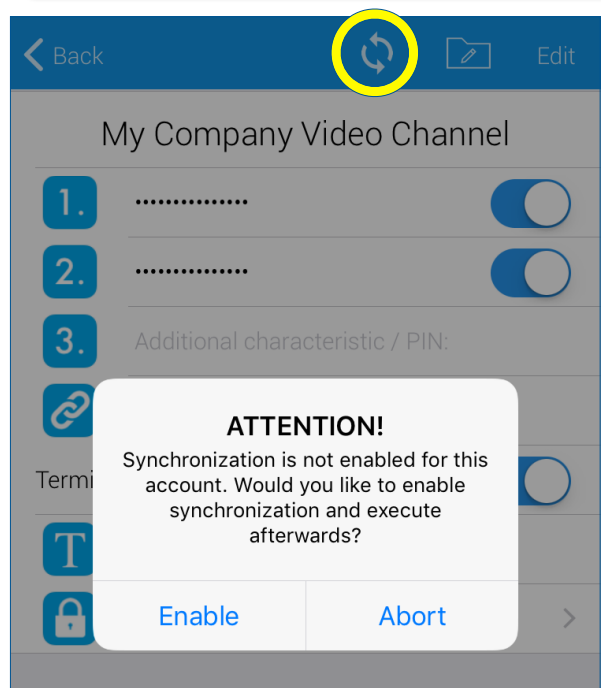
Vom Telefon aus Login-Daten synchronisieren

Bestehende Login-Daten, die sich bereits auf dem Telefon befinden, können von dort aus auch synchronisiert werden. Bei der Synchronisation eines Login-Datensatzes wird dieser doppelt verschlüsselt auf den Servern der Serviceanbieterin iPoxo IT GmbH abgespeichert.

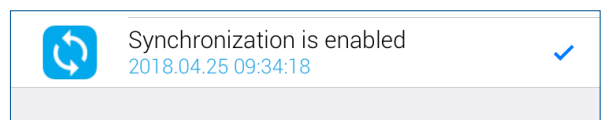
Wählen Sie nun hierzu das **Details-Menü (Einzelheiten-Menü)** eines Login-Datensatzes Ihrer Wahl.



Tippen Sie auf den **Synchronisations-Button** und beachten Sie bitte das Meldungsfenster. Lesen Sie dessen Inhalt und aktivieren Sie die Synchronisation oder brechen diese ab.



Achtung: Die Synchronisation kann durch das Antippen der Menüpunkt **Synchronisation ist aktiviert** deaktiviert werden. Bei der Deaktivierung werden die Login-Daten vom Server inhaltlich gelöscht, bleiben aber auf dem Telefon erhalten!



Bitte beachten Sie: Die Server befinden sich in einem Hochsicherheitsbereich eines Rechenzentrums in Wien. Alle Daten, die letztlich unseren Kunden gehören, werden in diesem Rechenzentrum aufbewahrt. Mitarbeiter des Rechenzentrums haben zwar physischen Zugang zu den Servern, besitzen jedoch keinerlei Zugriffsrecht. Selbst wenn ein Speichermedium unerlaubt entfernt werden würde, ist es auf Grund der angewandten doppelten Verschlüsselung der Kunden-Daten nicht möglich, Login-Daten auszulesen.

Login-Daten im Webinterface bearbeiten

Das Webinterface der Enterprise-Services wurden mit den neuesten Versionen von Google Chrome, Firefox und Safari entwickelt und getestet. Microsofts Internet Explorer und Edge Browser wurden in der Entwicklung nicht berücksichtigt. Im Einzelfall können diese Browser, je nach Version und Einstellungen, dennoch funktionieren, Support oder etwaige Fehlerbehebung bieten wir dafür aber nicht an.

Auch bieten wir nur für die oben genannten Browser "Push-To-Login" - Plug-Ins an. Die Browser von Microsoft haben wir aus technischen Gründen in der Entwicklung außer Acht gelassen.

Die Menüs der Enterprise-Services

Das Webinterface bietet zwei Hauptmenüs: **Login-Daten** und **USB-Keys**. Beide Hauptmenüs zeigen im ersten Reiter nur jenen USB-Key an, über den der Service-Link angefordert und eingegeben wurde. Hier sehen Sie auch, ob und wann die Lizenz der Enterprise-Services erneuert werden muss. In den meisten Fällen verlängert sich die Lizenz jedoch automatisch.

Im zweiten Reiter des Hauptmenüs USB-Keys sind jene USB-Keys aufgelistet, auf die sich die Lizenz erstreckt.

Label	License Number	License valid until
Master USB-Key Blue	763582333492462792939266	0000-00-00 00:00:00

Im weiteren Verlauf befasst sich diese Anleitung nur mit dem Hauptmenüpunkt **Login-Daten** und es wird davon ausgegangen, dass es noch mindestens einen weiteren USB-Key gibt, dem Login-Daten zugewiesen werden können.

Im **zweiten Reiter** sehen Sie einen Login-Datensatz (My Company Video Channel), der bereits über das Telefon synchronisiert wurde.

Das **zweite** Feld dient dazu, die Login-Daten zu bearbeiten, bzw. den Editor aufzurufen.

Im **dritten** Feld können Sie eine Anmerkung einfügen, die dann am Telefon angezeigt wird. **Diese Anmerkung läßt sich nicht am Telefon bearbeiten, sondern nur in den Enterprise-Services.**

Das **vierte** Feld zeigt die eindeutige ID des jeweiligen Login-Datensatzes an.

Das **fünfte** Feld führt zu weiteren Optionen.

Label	Login-Data	Remark	UUID
My Company Video Channel	🔒		8B515525-8377-4440-B5CE-A5BD6B1FF0F9

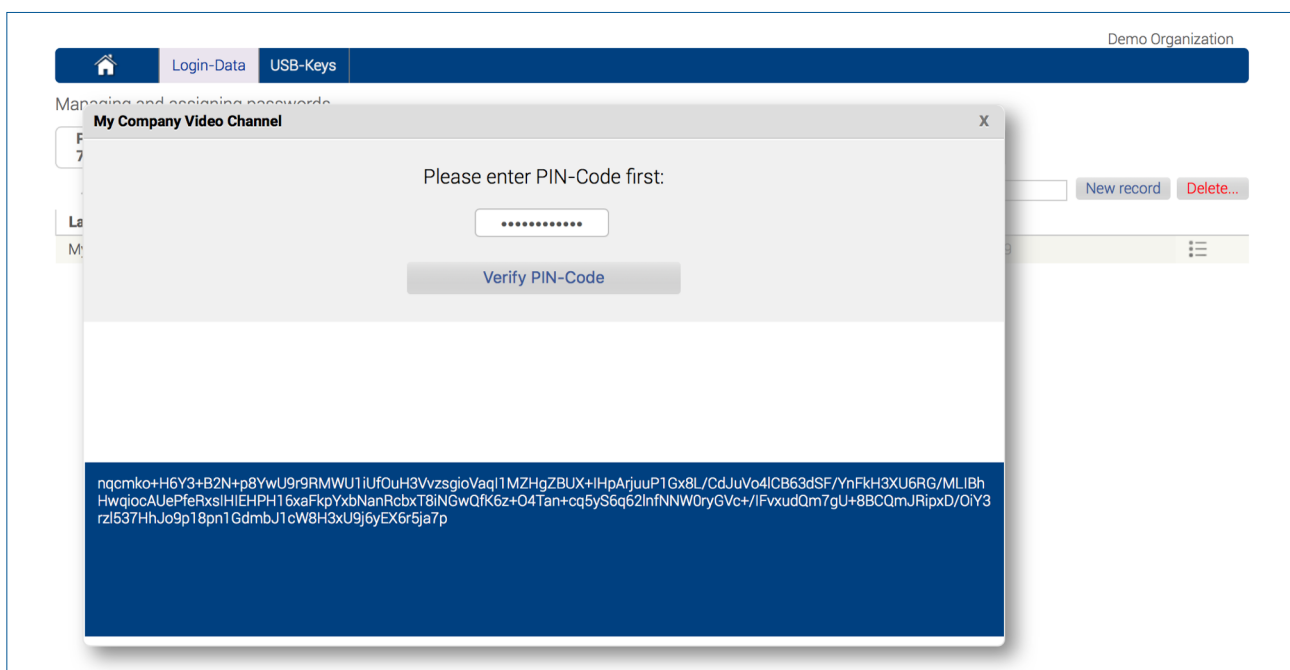
Die Bedienung der Enterprise-Services Masken

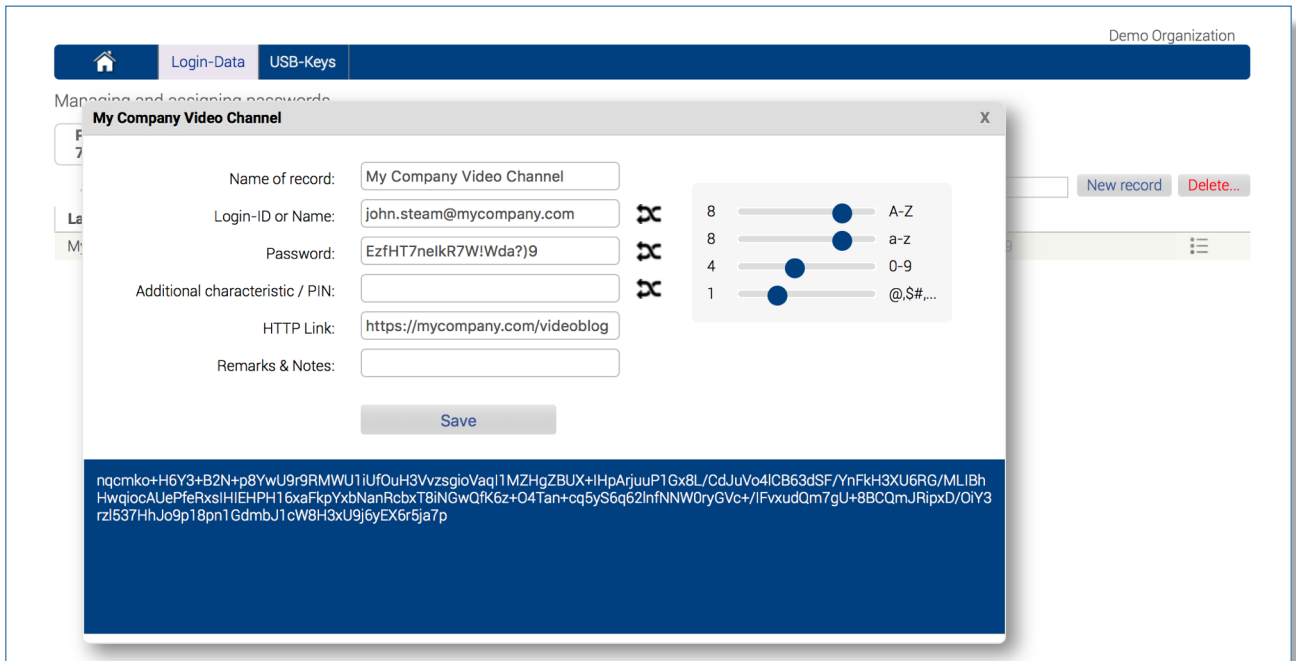
- 1) Hauptmenüpunkte können nur mit einem Mausklick ausgewählt werden.
- 2) Innerhalb eines Hauptmenüpunktes können die Reiter entweder durch Mausklick ausgewählt oder mit Shift+Pfeiltasten (Links und Rechts) gewechselt werden. Die Tastatursteuerung setzt jedoch den Fokus in einem der Felder voraus.
- 3) Innerhalb eines Reiters können die Felder entweder durch anklicken oder mit den Pfeiltasten gewechselt werden.
- 4) In die Optionen eines Login-Datensatzes gelangen Sie entweder durch das Anklicken des Feldes oder Sie richten mit den Pfeiltasten den Fokus darauf drücken die ENTER-Taste. Zurück gelangen Sie auf dem gleichen Weg.
- 5) Änderungen oder Eingaben in den Listendarstellungen (z.B. Bezeichnung oder Anmerkung der Login-Daten) müssen mit ENTER bestätigt werden. **Das Wechseln des Feldes mit den Pfeiltasten bzw. Tabulator sichert keine Änderungen!**

Bearbeiten eines Login-Datensatzes

In diesem Schritt setzt die Anleitung voraus, dass sich unter dem Hauptmenü **Login-Daten - Reiter Login-Daten** bereits ein Datensatz befindet, der über das Telefon synchronisiert wurde. Hier ist der Datensatz mit **My Company Video Channel** bezeichnet.

Richten Sie nun den Fokus auf das zweite Feld mit dem Schloss-Symbol und drücken Sie die ENTER-Taste. Danach öffnet sich der Editor. Im Editor werden Sie aufgefordert den PIN-Code einzugeben um den Datensatz für die Bearbeitung zu entschlüsseln. Sie sehen den verschlüsselten Datensatz in dem breiten blauen Balken im unteren Bereich des Editors. Wurde der richtige PIN-Code eingegeben, sieht man nun die Login-Daten als Klartext und kann diesen bearbeiten.





Bitte beachten Sie: Der PIN-Code bleibt jetzt für die aktuelle Session erhalten und muss nicht nochmals eingegeben werden, möchte man weitere Datensätze bearbeiten.

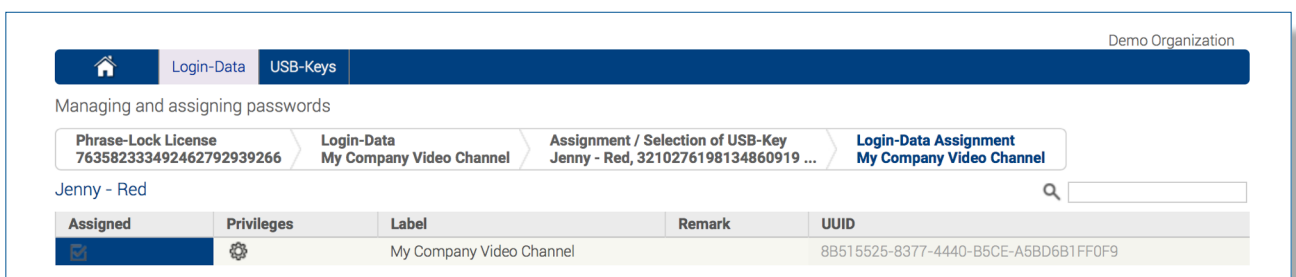
Jegliche Ver- und Entschlüsselung erfolgt in JavaScript direkt in dem aktuellen Fenster Ihres Browsers. PIN-Code und S-Key, in seiner entschlüsselten Form, verlassen die Oberfläche zu keinem Zeitpunkt! Dafür garantieren wir!

Verschiedentlich durchsuchen Browser-Plug-In, auch als Add-On bezeichnet, Webseiten nach bspw. Login-Namen, Passwörtern oder sonstiger interessanter Information. Add-Blocker zählen auch dazu. Zumeist sind diese kleinen Helfer harmlos und tun nur, wozu sie auch gedacht sind. Dennoch möchten wir hier darauf hinweisen, dass solche Plug-Ins, je nachdem woher sie kommen, auch ein gewisses Bedrohungspotenzial in sich bergen können. Deshalb ersuchen wir alle Anwender der Enterprise-Services sich darüber Gedanken zu machen und sich die Liste der Plug-Ins anzusehen und mehr darüber in Erfahrung zu bringen. Die Entscheidung, welchen Plug-Ins zu vertrauen ist und welchen nicht, können wir dem Anwender nicht abnehmen.

Als Faustformel für diese Entscheidung gilt: Hat man in den Browser seiner Wahl auf einem bestimmten Computer auch genug Vertrauen Bankgeschäfte zu erledigen oder die Kreditkarte einzugeben, sollte auch die Verwendung der Phrase-Lock Enterprise-Services keine Gefahr darstellen!

Login-Daten zuordnen

Eine der Hauptfunktion der Enterprise-Services ist die Zuordnung von Login-Daten. In diesem Beispiel werden Login-Daten eines fiktiven **My Company-Video-Account** einem USB-Key zugeordnet, der die Bezeichnung **Jenny Red** trägt. **Jenny Red** kann somit über die Synchronisationsfunktion **Zuweisungen importieren** die Login-Daten auf ihr Telefon übertragen. Existiert ein Login-Datensatz noch nicht, wird dieser Datensatz automatisch den Favoriten zugeordnet.



Rechte zugeordneter Login-Daten

Der Ersteller eines Login-Datensatzes kann die Rechte einer Zuordnung verändern. Die Einschränkung von Rechten für Dritte ist immer dann sinnvoll, wenn die ungewollte Veränderung eines Accounts verhindert werden soll. Ob ein Account dennoch am Zielsystem verändert wird, kann über diese Funktion nicht verhindert werden.

Name	Value
Allow editing by third parties	<input checked="" type="checkbox"/>
Allow rewriting by third parties	<input checked="" type="checkbox"/>
Created / Modified	2018-04-25 09:34:18

Änderungen synchronisieren

In den Einstellungen am Telefon befinden sich unter **Extended Services (Erweiterte Dienste)** - außer dem Menüpunkt sich für die Enterprise-Services einzuloggen - drei weitere Menüpunkte.

Import private data (Private Daten importieren):

Wenn Login-Daten in den Enterprise Services verändert oder hinzugefügt wurden, können diese hiermit wieder eingelesen, bzw. synchronisiert werden. Datensätze, die noch nicht auf dem Telefon existieren, werden ohne weiteren Hinweis importiert und den Favoriten zugeordnet. Änderungen bestehender Datensätze werden in einem Dialog angezeigt und man kann sich entscheiden, ob die Änderungen übernommen werden sollen oder nicht.

Export private data (Private Daten exportieren):

Änderungen von Login-Daten die am Telefon durchgeführt wurden, können mit diesem Menüpunkt synchronisiert werden. Gegebenenfalls werden die Unterschiede in einem Dialog angezeigt und man kann sich entscheiden, die Änderungen zu synchronisieren oder abzubrechen.

Assignments import (Zuweisungen importieren):

Mit diesem Menüpunkt lassen sich jene Datensätze synchronisieren, die einem Anwender durch einen anderen zugewiesen wurden.