Repository-Standorte

Zugehörige Informationen			
Standorte, Nutzer..., Prüfregeln, Abfragen..., Masken, Prüfpläne..., Kommunikation, Nachrichten..., Vorgangssteuerung, Allgemeine Konfiguration	Allgemeine Bedienungshinweise	—	—
Übersicht, **Standorte**, Institutionen, Nutzer, Nutzerprofile, Arbeitsgruppen (VG), Nummernkreise (VG), Arbeitsverteilungen (VG)			

Fachlich/inhaltliche Beschreibung

Die Perspektive **Standorte, Nutzer...** umfasst alle ASYS-Repositoryobjekte, die mit Repositorystandorten, Nutzern und der Rechteverwaltung zu tun haben. Teilweise werden hier Objekte konfiguriert, die primär in anderen Perspektiven zum Einsatz kommen. Da es sich um Einstellungen zu Nutzern handelt, sind sie trotzdem in dieser Perspektive angesiedelt.

Die in dieser Perspektive konfigurierbaren Repository-Objekte sind:

- **Repository-Standorte**: Viele Konfigurationseinstellungen in ASYS können und müssen individuell für jeden Repository-Standort vorgenommen werden. In vielen Fällen entspricht ein Repository-Standort einem Bundesland (je Bundesland gibt es zumindest einen Repository-Standort). Diese Standorte können Unterstandorte beherbergen, d.h. die Repository-Standorte bilden einen Baum [1)]. Der Standort, an dem der Admin sich beim Administrator anmeldet, bildet jeweils die Wurzel des Objektbaums auf der linken Seite des Programms. Die Konfiguration ist somit beschränkt auf den Anmeldestandort und seine Unterstandorte. Übergeordnete Standorte sind hingegen weder einsehbar noch änderbar.
  Ein Standort besitzt eine oder mehrere *Institutionen*, denen *Nutzer* zugeordnet sind. Pro Standort können ein oder mehrere *Nutzerprofile* definiert werden, denen Rechte an Masken und Abfragen zugeordnet sind. *Nutzer* sind mit einem oder mehreren *Nutzerprofilen* verbunden, wodurch sich die Rechte des jeweiligen *Nutzers* ergeben. *Arbeitsgruppen*, *Nummernkreise* und *Verteilungen* werden für die Vorgangssteuerung benötigt, um Arbeitsschritte aus Vorgängen einem Bearbeiter zuzuteilen. Diesen drei Objekten werden *Nutzer* zugeordnet.
- **Institutionen**: Institutionen können genutzt werden, um einen *Repository-Standort* logisch zu gliedern. Zumindest muss ein *Standort* eine Institution beherbergen, da diese die *Nutzer* enthalten - ohne Institution –> keine *Nutzer*!.
  Je Institution und *Maske* kann ein Lesefilter definiert werden, d.h. die *Nutzer* einer Institution sehen auf der betreffenden *Maske* nur einen Ausschnitt der in der Datenbank vorhandenen Daten und für jede Institution kann ein anderer Ausschnitt definiert werden. Ebenso lassen sich je Institution individuelle Einstellungen an den Masken vornehmen (z.B. abweichende Beschriftung, Pflichtfeldstatus, Defaultwert, Defaultsuchwert etc.).
  Nach welchen Gesichtspunkten eine Gliederung erfolgen soll, ist stark von der

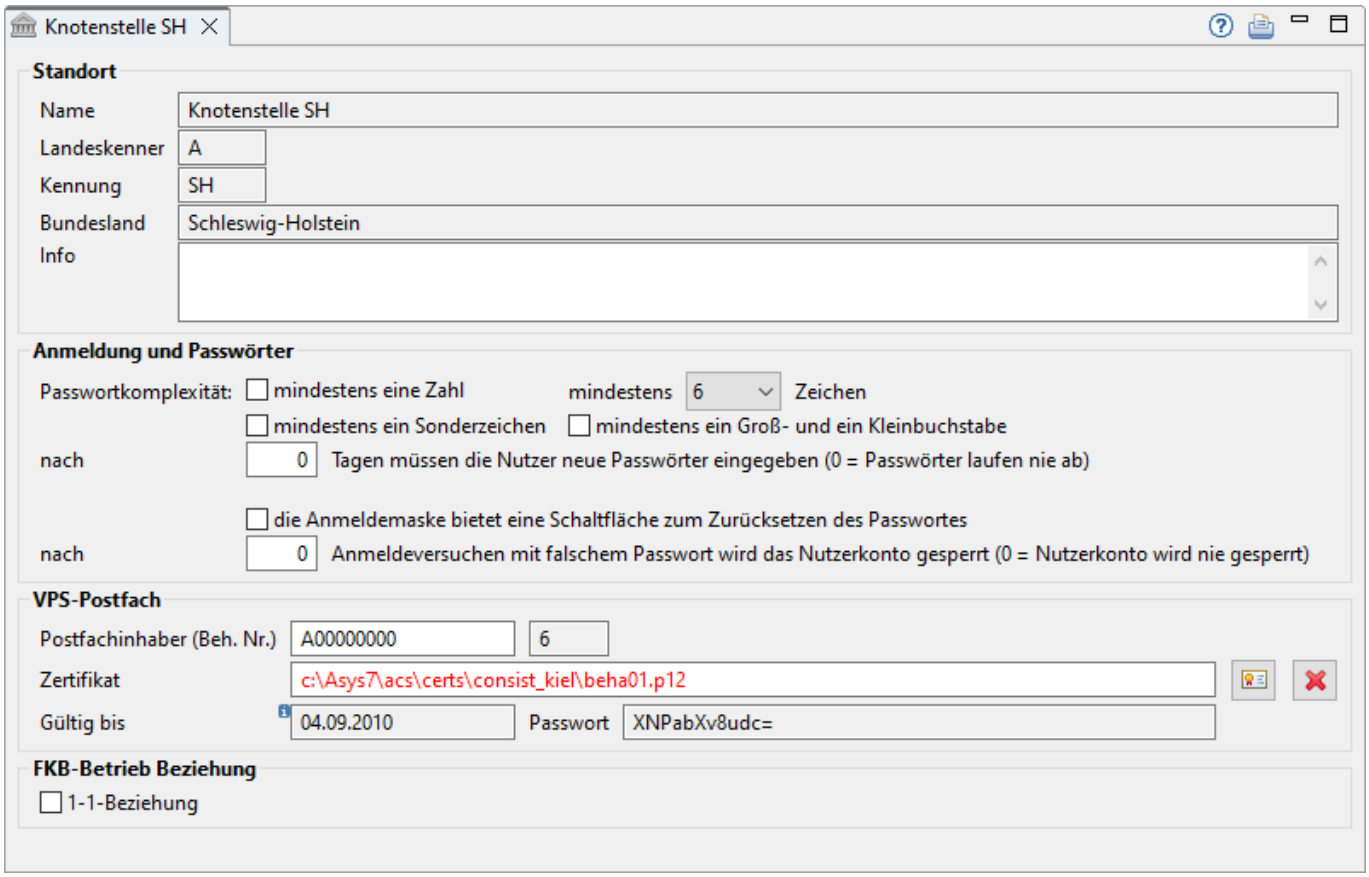
Zuständigkeitstruktur des *Standortes* abhängig. Ist in einem Bundesland nur eine Behörde für die Abfallüberwachung zuständig, so sind ggf. Referate, Gruppen oder drgl. Kandidaten für die Definition individueller Institutionen. Bei Bundesländern mit vielen zuständigen Behörden stellt ggf. jede Behörde eine Institution dar. Wichtig ist dabei, dass mit der Gliederung in Institutionen bis auf die statische Vorfilterung mit Lesefiltern noch keine Rechtevergabe auf Masken verbunden ist, d.h. alle *Nutzer* einer Institution dürfen potentiell alles.

- **Nutzer**: Jeder Nutzer ist ein Zugangskonto zur ASYS-Oberfläche und ihren Daten. Ein Nutzer gehört immer zu einer *Institution* und ist an die dort einstellbaren *Lesefilter* und *Maskeneinstellungen* gebunden. In der Regel wird ein Nutzer einer natürlichen Person entsprechen. In einigen Fällen werden aber auch Nutzer einer Rolle entsprechen, die von mehreren Personen parallel oder nacheinander ausgeübt werden (z.B. Praktikant mit stark eingeschränkten Rechten).
  Ein frisch angelegter Nutzer besitzt **anfangs keine Rechte**. Diese werden dem Nutzer über die Zuordnung von einem oder mehreren *Nutzerprofilen* zugewiesen. Die Summe aller Rechte aus allen *Nutzerprofilen*, die einem Nutzer zugewiesen sind, bestimmt die Gesamtheit seiner Rechte auf der ASYS-Oberfläche.
  Jedem Nutzer müssen *Signaturrechte* individuell zugewiesen werden (diese erlangt der Nutzer nicht über ein Nutzerprofil!). Die Auswahl erfolgt aus einer Auswahlliste von Masken, auf denen die Signaturfunktion möglich ist.
- **Nutzerprofile**: Nutzerprofile stellen prototypische *Nutzer* oder Rollen dar. Änderungen an den Einstellungen eines Profils wirken sich dabei auf alle *Nutzer* aus, denen das Profil zugeordnet ist[2)].
  In Nutzerprofilen werden *Rechte auf Masken* vergeben, d.h. es wird bestimmt ob die *Nutzer* des Profils die *Maske* öffnen und nach Datensätzen suchen dürfen (Leserecht), Datensätze neu anlegen (Anlegerecht), ändern (Änderungsrecht) oder löschen dürfen (Löschrecht). Ebenso wird im Profil eine Liste der Abfragen[3)] und Textformulare verwaltet, die durch die Nutzer des Profils aufgerufen werden dürfen.
- **Arbeitsgruppen**: Arbeitsgruppen werden für die Bearbeiterermittlung in der Vorgangssteuerung verwendet. Über die Gruppen wird gesteuert, welche *Nutzer* gemeinsam mit bestimmten *Arbeitsschritten* beaufschlagt werden. Die Zuteilung der neu anfallenden *Arbeitsschritte* wird per Zufall auf die Mitglieder eine Arbeitsgruppe verteilt. Dabei besteht die Möglichkeit, einzelne Gruppenmitglieder von der Arbeitszuteilung auszuschließen (Chef-Kennzeichen).
- **Nummernkreise**: Nummernkreise werden für die Bearbeiterermittlung in der Vorgangssteuerung verwendet. Nummernkreise dienen der Zuordnung von *Arbeitsschritten* anhand eines Merkmals des zugehörigen Datensatzes zu einem Mitglied einer Gruppe von ASYS-Nutzern. Die Zuordnung erfolgt dabei über genau ein Feld des Datensatzes (z.B. der Name des Entsorgers im Begleitschein: **A-F** –> Bearbeiter X, **G-M** –> Bearbeiter Y, **N-S** –> …).
- **Arbeitsverteilungen**: Arbeitsverteilungen werden für die Bearbeiterermittlung in der Vorgangssteuerung verwendet. Arbeitsverteilungen dienen der Zuordnung von *Arbeitsschritten* anhand von Quoten. Für die *Nutzer* in einer Arbeitsverteilung wird protokolliert, wie viele *Arbeitsschritte* sie in der Vergangenheit erhalten haben. Dem stehen Sollwerte für die Anteile gegenüber. Ein neuer *Arbeitsschritt* wird demjenigen *Nutzer* in einer Arbeitsverteilung zugewiesen, dessen Ist-Anteil unter dem Soll-Anteil liegt.

Über die Arbeitsgruppen wird gesteuert, welche *Nutzer* als Kollegen gegenseitige Einsicht in den Arbeitsvorrat haben und bedarfsweise *Arbeitsschritte* von Kollegen übernehmen (Stellvertreterregelung) oder an diese übergeben dürfen (Delegierung).

2013/12/11 14:34 · eflor

Bedienung



Der Tab-Reiter eines Repository-Standortes im Bearbeitungsbereich des Administrators gliedert sich in drei Abschnitte:

Standort

Die ersten drei Zeilen des Abschnitts 'Standort' enthalten den Namen, den Landeskenner, die Kennung und das Bundesland des Repository-Standortes. Der Name und die Kennung werden bei der Erstellung eines neuen Standortes vom Admin vergeben. Diese Angaben können nachträglich nicht mehr verändert werden. Ein Standort erbt automatisch das Bundesland (Name und Bundeslandskennbuchstabe) vom übergeordneten Standort. Diese Angaben können daher ebenfalls nicht verändert werden.

Info

Das Info-Feld ist ein Textfeld für Freitext und kann für eine interne Dokumentation genutzt werden.

Passwörter

Diese Einstellungen gelten für den jeweiligen Repository-Standort, also für alle seine Institutionen und deren Nutzer, nicht jedoch für Unterstandorte.

Passwortkomplexität

Es kann eingestellt werden, welchen Komplexitätsgrad die durch die *Nutzer* selber vergebenen Passwörter haben müssen. Wird hier nichts eingestellt, gilt als Mindeststandard:

- Ein Passwort muss aus wenigstens sechs beliebigen Zeichen bestehen.

Über die weiteren Felder kann das Niveau der Passwortkomplexität angehoben werden:

- **mindestens eine Zahl**: Mit dem Ankreuzfeld kann bestimmt werden, dass im Passwort zumindest eine Ziffer (Zeichen aus dem Bereich [0 - 9]) enthalten ist.
- **mindestens … Zeichen**: Die Mindestlänge kann auf einen höheren Wert als sechs Zeichen festgelegt werden. Die Auswahl der Mindestlänge erfolgt aus einer Werteliste von 6 bis 18.
- **mindestens ein Sonderzeichen**: Mit dem Ankreuzfeld kann bestimmt werden, dass im Passwort zumindest ein Zeichen enthalten ist, dass weder ein Wortzeichen (Zeichen aus dem Bereich [a - z, A - Z, äÄöÖüÜß]) noch eine Ziffer ist.
- **mindestens ein Groß- und ein Kleinbuchstabe**: Unter den Buchstaben des Passwortes muss sich zumindest ein Kleinbuchstabe [a - z, öäüß] und ein Großbuchstabe [A - Z, ÄÖÜ] befinden (bedeutet gleichzeitig: das Passwort muss mindestens zwei Buchstaben enthalten).

Achtung: Bei der Neueingabe eines Passwortes durch einen *Nutzer* wird nur überprüft, ob das neue Passwort sich vom bisherigen unterscheidet. Es wird keine Historie von Passworten zu jedem *Nutzer* verwaltet. Ein *Nutzer* kann daher nach einer ersten Passwortneueingabe durch eine anschließende manuelle Passwortneuvergabe zu seinem alten Passwort zurückkehren! Die Regeln der Passwortkomplexität sind aber in jedem Falle einzuhalten!

Hinweis: Die Anforderungen an die Passworte werden nur bei der Neueingabe eines Passwortes durch einen *Nutzer* überprüft. Bereits vergebene Passworte, die keiner Gültigkeitsbeschränkung unterliegen, sind daher von einer Verschärfung der Regeln nicht betroffen. Erst wenn ein *Nutzer* selbst ein neues Passwort vergibt oder durch den Admin ein neues Einmalpasswort vergeben bekommt (bei einem neuen Nutzer oder bei einer späteren Passwortvergabe durch den Admin) werden die oben genannten Regeln angewandt.

Die Regeln für die Vergabe von Passwörten gelten nicht, wenn dem *Nutzer* das Recht, sein Passwort zu ändern, entzogen wurde. In diesem Fall gilt nur das vom Administrator für den *Nutzer* vergebene Passwort. Dieses wird aber nicht gegen die hier einstellbaren Regeln geprüft.

Gültigkeitsdauer von Passwörtern

Zusätzlich kann festgelegt werden, dass ein durch einen *Nutzer* vergebenes Passwort nach einer vorgegebenen Anzahl von Tagen abläuft und daraufhin durch den *Nutzer* neu vergeben werden muss. Wird hier der Vorgabewert 0 Tage eingetragen, so bleiben die Passworte zeitlich unbeschränkt gültig.

Hinweis: Das durch den *Nutzer* vergebene Passwort wird (verschlüsselt!) mitsamt dem Datum der Vergabe in die ASYS-Nutzdatenbank eingetragen. Ist als Gültigkeitsdauer ein Wert größer als 0 eingetragen, so wird nach der erfolgreichen Passwortüberprüfung die Anzahl der Tage zwischen dem aktuellen Datum und dem Datum der Passwortvergabe errechnet. Überschreitet diese Differenz den Wert der Gültigkeitsdauer, so wird der *Nutzer* gezwungen, ein neues Passwort gemäß den Komplexitätsregeln (s.o.) einzugeben.

Wird die Gültigkeitsdauer nachträglich eingerichtet oder verringert, so sind davon alle *Nutzer* betroffen, deren Passwortvergabe länger zurückliegt, als die neue Gültigkeitsdauer zulässt. Diese *Nutzer* müssen bei der nächsten Anmeldung an der ASYS-Oberfläche ein neues Passwort vergeben.

Die Gültigkeitsdauer von Passwörtern wirkt sich nicht auf *Nutzer* aus, denen das Recht, ihr Passwort zu ändern, entzogen wurde!

Anmeldeversuche

Neu/geändert ab Version 7.14

Über das Ankreuzfeld **die Anmeldemaske bietet eine Schaltfläche zum Zurücksetzen des Passwortes** kann festgelegt werden, ob dem ASYS-Nutzer im Anmeldedialog die Möglichkeit gegeben wird, sich ein neues Einmalpasswort per E-Mail zusenden zu lassen. Voraussetzung ist, dass in der Nutzerkonfiguration eine gültige E-Mail-Adresse eingetragen ist und der ASYS-Funktionsserver Zugang zu einem E-Mail-Server besitzt, über den die E-Mail verschickt werden kann. Hierzu müssen mindestens die Konfigurationsparameter 'MailFacade.smtpHost' und 'MailFacade.absenderEMail' mit passenden Angaben versehen werden.

Der Ablauf ist wie folgt:

1. Der Nutzer klickt den Button 'Passwort vergessen'.
2. Der Nutzer gibt die E-Mail-Adresse ein, an die das Einmalpasswort verschickt werden soll.
    1. Diese E-Mail-Adresse MUSS ÜBEREINSTIMMEN mit der E-Mail-Adresse in der Nutzerkonfiguration!
3. Der ASYS-Funktionsserver verschickt eine E-Mail mit dem Einmalpasswort.
4. Der Nutzer meldet sich mit dem Einmalpasswort an der ASYS-Oberfläche an. Die Oberfläche verlangt die doppelte Eingabe eines neuen, dauerhaften Passwortes gemäß den oben eingestellten Komplexitätsregeln.

Über das Feld **Anmeldeversuche mit falschem Passwort...** kann festgelegt werden, dass das Nutzerkonto nach der angegebenen Anzahl an Fehlversuchen dauerhaft gesperrt[4)] wird.

Zur Freigabe eines derart gesperrten Nutzerkontos ist wie folgt vorzugehen:

1. In der Nutzerkonfiguration ist durch den ASYS-Fachadministrator ein neues Einmalpasswort zu vergeben und dem betroffenen Nutzer mitzuteilen.
    1. Für die Übermittlung des Einmalpasswortes gibt es in ASYS keinen Standardmechanismus. Ob die Mitteilung des neuen Einmalpasswortes per E-Mail,

fernmündlich, per SMS oder über einen anderen Kommunikationsweg erfolgt, ist nicht vorgegeben.

2. Der Nutzer meldet sich mit dem Einmalpasswort an der ASYS-Oberfläche an. Die Oberfläche verlangt die doppelte Eingabe eines neuen, dauerhaften Passwortes gemäß den oben eingestellten Komplexitätsregeln.

Wird als Anzahl der Wert 0 eingetragen, sind beliebig viele Fehlversuche erlaubt! Davon unabhängig wird nach jedem Fehlversuch eine Wartezeit bis zur nächsten Passworteingabemöglichkeit eingelegt. Diese **Wartezeit verdoppelt sich** mit jedem fortgesetzten Fehlversuch, bis eine erfolgreiche Anmeldung stattgefunden hat.

VPS-Postfach

Ein Repository-Standort, der mit der ZKS kommunizieren können soll, benötigt einen privaten Schlüssel in einem Verschlüsselungs-Zertifikat. Der öffentliche Schlüssel dieses Zertifikats muss bei der VPS der ZKS-Abfall für das eigene Postfach registriert sein. Mit dem öffentlichen Schlüssel werden alle Nachrichten verschlüsselt. Nur mit dem privaten Schlüssel des Zertifikats lassen sich diese Nachrichten wieder entschlüsseln. Mit diesem Zertifikat werden daher die Dateien aus Ihrem eigenen Postfach abgeholt und entschlüsselt.

Hinweis: Nicht jeder Standort benötigt ein eigenes Postfach bei der ZKS-Abfall und damit eine Zertifikatszuordnung an dieser Stelle. Diese Konfiguration ist aber zumindest für einen Repository-Standort je Bundesland notwendig, damit sowohl ein- und ausgehenden BMU-Nachrichten des eANV als auch der ASYS-interne Nachrichtenaustausch abgewickelt werden können.

Je betriebener ASYS-Datenbank in einem Bundesland (aktuell ist eine Datenbank je Land die Regel) ist ein Repository-Standort mit ZKS-Postfachanbindung notwendig, damit ein Nachrichtenaustausch möglich ist. Alle weiteren Repository-Standorte, die mit der gleichen Datenbank verbunden sind, partizipieren an dieser Kommunikationskonfiguration und benötigen keine eigenen Postfächer.

Das VPS-Postfach-Zertifikat dient auch der Authentifizierung gegenüber dem ZKS-Auftrags-Service (ermöglicht die synchrone nachträglich Zertifikatsprüfung für Signaturen durch berechtigte Nutzer).

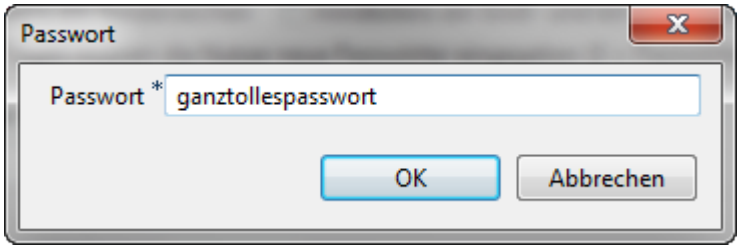
Ist das Zertifikat am konfigurierten Speicherort nicht vorhanden, erscheint der Inhalt des Feldes Zertifikat in roter Schrift (vgl. Abbildung oben).

Zertifikat zuordnen

Geben Sie zunächst Ihre Behördliche Nummer ein. Dies ist immer Ihr Landeskennbuchstabe gefolgt von acht Nullen (z.B. 'I00000000' für Bayern). Die Prüfziffer wird vom System automatisch berechnet und im Feld dahinter schreibgeschütz eingetragen.

Über den Button **Zertifikatauswahl** () leiten Sie die Zuordnung eines Zertifikats ein. Es öffnet

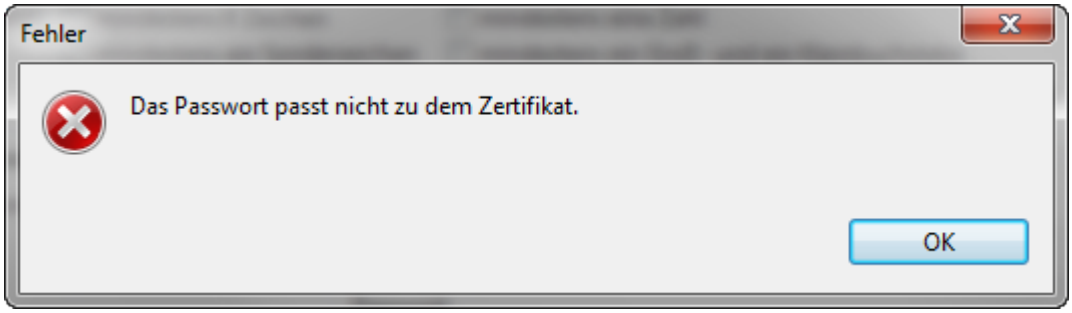
sich ein Passwort-Dialog, da die Zertifikatsdatei mit dem privaten Schlüssel durch ein Passwort geschützt ist. In diesem Dialog müssen Sie das **Passwort des Zertifikats** im Klartext eintragen [5)].



Es folgt ein Dateiauswahldialog des Betriebssystems, welcher bereits auf die übliche Dateiendung für Zertifikatsdateien mit privaten Schlüsseln (*.p12) eingestellt ist. Wählen Sie Ihre Zertifikatsdatei aus und bestätigen Sie die Auswahl im Dateiauswahldialog.

Falls das Passwort zum Zertifikat passt, werden Dateisystempfad und Name der Zertifikatsdatei, das Gültig bis-Datum der Zertifikatsgültigkeit und das verschlüsselte Passwort des Zertifikats schreibgeschützt angezeigt. Dieser Konfigurationsschritt ist damit abgeschlossen.

Wenn das Zertifikat und das Passwort nicht zueinander passen, erfolgt eine Fehlermeldung:



Zertifkat entfernen

Die Zuordnung eines Zertifikats zum Standort kann über den Button **Löschen** () aufgehoben werden. Anschließend ist dem Standort kein Zertifkat mehr zugeordnet. Der Standort kann nicht mehr auf ein Postfach bei der ZKS-Abfall zugreifen!

FKB-Betrieb Beziehung

Das Ankreuzfeld 1-1-Beziehung dient der Einstellung, ob die FKB-Ebene 'ausgeblendet' werden soll. Diese Einstellung gilt für einen kompletten Standort, also alle seine Institutionen und deren Nutzer, jedoch nicht auch für Unterstandorte. Sinnvoll ist dieses Flag für Standorte, die Ihre Firmen–Betriebs–Daten in einer 1-1-Beziehung pflegen. Ein Setzen des Flags hat diverse Auswirkungen auf die interne Programmlogik der ASYS-Oberfläche.

1. Betriebsstätten können nur noch über die Betriebsstättenmasken angelegt werden. Dabei wird automatisch auch eine FKB mit angelegt. Die FKB erhält hierbei die gleichen Adressangaben (Name, Adresse, Gemeinde) wie der Betrieb. Sofern als Default-Wert für den Firmenschlüssel der Wert '**AUTO**' im Repository eingetragen ist (s. Perspektive Masken, Prüfpläne...), wird der Firmenschlüssel automatisch bestimmt. Ansonsten wird als Firmenschlüssel die behördliche Nummer des Betriebes eingetragen. (**ACHTUNG**: Bitte achten Sie in diesem Fall auf eindeutige

behördliche Nummern über alle Betriebstypen hinweg!)
2. Beim Ändern eines Betriebsdatensatzes erfolgt ein Dialog, ob die Daten der FKB ebenfalls aktualisiert werden sollen (Default = Ja).
3. Beim Löschen eines Betriebsdatensatzes wird, sofern dies der einzige Betrieb an dieser FKB ist, die FKB ebenfalls gelöscht. Es erfolgt darüber hinaus noch eine Überprüfung auf historische Versionen. Sofern historische Versionen vorhanden sind, hat der Anwender über einen Dialog folgenden Möglichkeiten:
    1. Gesamte Historie löschen.
    2. Nur den aktuellen Datensatz löschen und die Datensatzgültigkeit des Vorgängers bzw. Nachfolgers anpassen. Hierbei folgen einige weitere Überprüfungen
        1. Gibt es nur einen Vorgänger in der Historie, bekommt der Vorgänger das 'Gültig bis' des gelöschten Datensatzes.
        2. Gibt es nur einen Nachfolger in der Historie, bekommt der Nachfolger das 'Gültig von' des gelöschten Datensatzes.
        3. Gibt es sowohl einen Vorgänger als auch einen Nachfolger in der Historie, wird der Anwender über einen weiteren Dialog gefragt, welcher diese Datensätze in seinem Gültigkeitszeitraum erweitert werden soll.
        4. Bei unterbrochenen Historien kann keine automatische Anpassung der Gültigkeiten vorgenommen werden. Hierüber wird der Anwender informiert.
    3. Gesamten Löschvorgang abbrechen.

Als Standard wird bei gesetztem Flag 1-1-Beziehung der Aufgabenbereich 'Firma, Körperschaft, Betreiber' nicht im Navigationsbaum angezeigt.

Weitere Informationen zu dieser Maske																
keine																
landesspezifische Zusatzinformationen:	SH	HH	NI	HB	NW	HE	RP	BW	BY	SL	BE	MV	ST	BB	TH	SN

---

1)

Die Wurzel des kompletten Baums ist der Standort 'Hauptknoten IKA', ihm sind u.a. die 16 Knotenstellen der Bundesländer als Unterstandorte zugeordnet.

2)

Dabei ist zu beachten, dass bei *Nutzern* mit mehreren Profilzuordnungen die Summe der Rechte aus allen Profilen gilt. Das gleiche Recht kann dabei parallel aus mehr als einem Profil erwachsen. Damit ein Recht für einen *Nutzer* nicht gilt, darf es in keinem der zugeordneten Profile vergeben sein!

3)

Betroffen hiervon sind Abfragen, die nicht als interne Abfragen gekennzeichnet sind, also freie Abfragen, QS-Abfragen und Auswertungsabfragen

4)

Hinweis: Die Sperrung erfolgt in der Nutzdatenbank und nicht im Repository! Ein derart gesperrtes Nutzerkonto erscheint daher in der Nutzerkonfiguration nicht als deaktiviert.

5)

Das Passwort wird Ihnen mit der Zertifikatsdatei von der ausgebenden Stelle mitgeteilt; aus Sicherheitsgründen können Ihnen Zertifikatsdatei und Passwort aber als getrennte Nachrichten (Brief, E-Mail,...) zugehen.