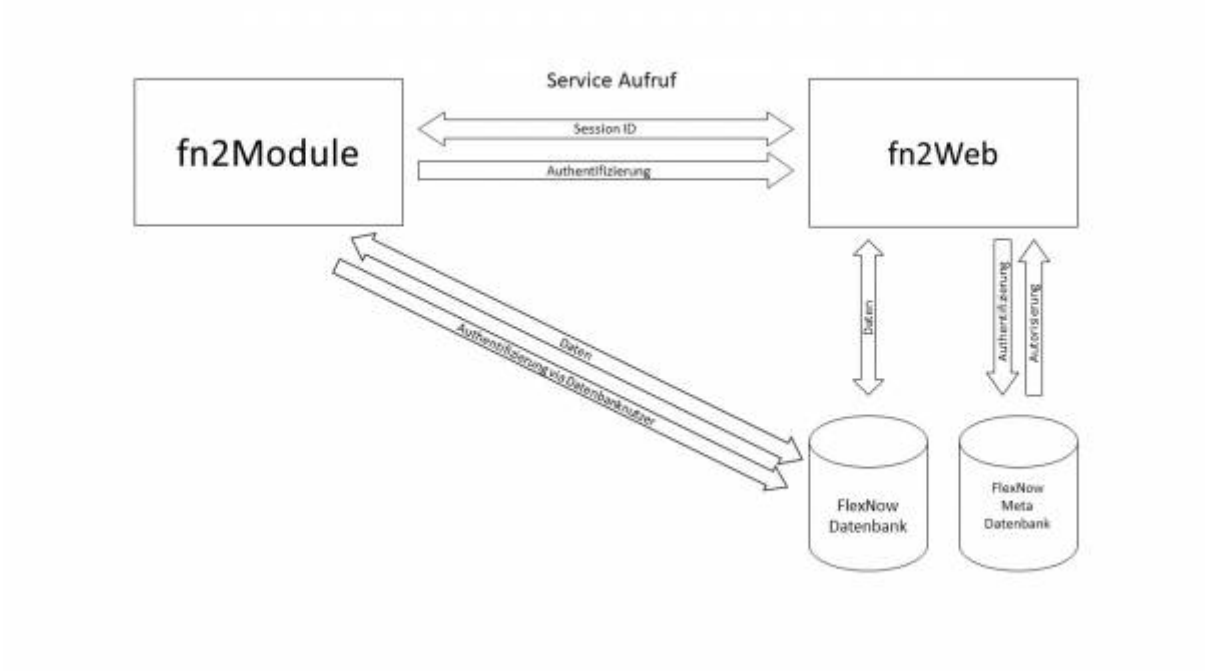
FN2 Web-Services - Authentifizierung

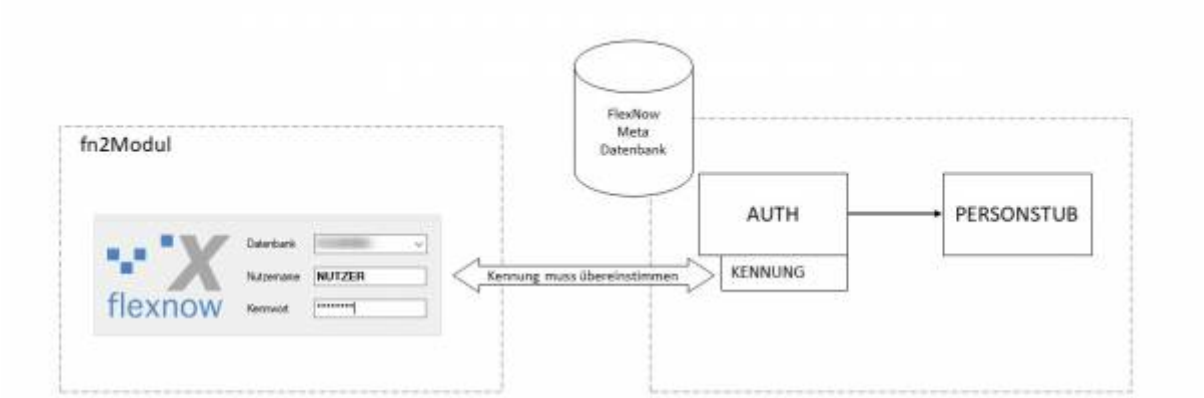
Authentifizierung

Die fn2-Module und fn2-Web verwenden unterschiedliche Methoden der Authentifizierung. Bei den fn2-Modulen wird hierfür das Konzept des Datenbank-Benutzers verwendet. D.h. es die Funktionalität wird vom verwendeten Datenbanksystem (Oracle, SAPDB, Informix...) bereitgestellt. Das Modul prüft lediglich ob mit dem angegeben Anmeldedaten ein Datenbankzugriff möglich ist.

Die Authentifizierung bei fn2 Web wird hingegen über eigene Benutzer, Rollen und Rechte verwaltet welche wiederum den Zugriff auf die verschiedenen Funktionalitäten von fn2Web steuern. Die nötigen persistenten Daten hierfür werden in der FlexNow Meta Datenbank verwaltet. Jeder Zugriff auf Komponenten von fn2 Web, unabhängig ob es sich um die Anmeldung via Browser (z.B. Studenten-Schnittstelle) oder dem Aufruf eines Service (z.B. Druck) handelt benötigen daher einen gültigen Benutzer welcher wiederum über eine Rolle verfügt welcher die gültigen Rechte zugeordnet wurden.



Um zu verhindern, dass ein Anwender der fn2Module bei jedem Aufruf eines Service von fn2Web zusätzlich noch gültige Anmeldedaten angeben muss, werden hierfür derselbe Nutzername und dasselbe Kennwort verwendet, welches der Anwender bereits zur Anmeldung am fn2Modul (z.B. PA-Modul) verwendet hat (Datenbankbenutzer). Hierfür muss sichergestellt werden, dass es in der Metadatenbank einen Benutzer (Personstub) gibt welcher dieselben Anmeldedaten besitzt (AUTH) wie der Datenbankbenutzer.



Beispiel:

Der Anwender Max Mustermann meldet sich an den Modulen mit der Kennung „mmuster“ und dem Passwort „12345“ an. Damit das Modul auf Services von fn2Web zugreifen kann, muss in der Metadatenbank in der Tabelle „Auth“ ein Eintrag geben, welcher die Kennung „mmuster“ hat. Das Passwort kann von dem der Datenbank abweichen.

Service-Rollen und Rechte

Die Grundsätzliche Funktionalität des Rollen- und Rechte-Systems finden sie hier.

Für die Authorisierung wurde eine Rollenhierarchie eingeführt um Rechte, die mehrere Rollen nutzen, kapseln zukönnen.

Beispiel:

Rolle Nutzer (ID 7) Grundätzlicher Zugriff auf FN2 Web. Diese Rolle wird als Basisrolle verwendet, die alle anderen Rollen haben müssen. Rolle fn2Modul (Grundrolle) (ID60). Diese Rolle wird als Grundrolle für alle Service Aufrufe aus allen fn2Modulen einschl. Stud2Flex verwendet. Die Rolle erbt alle Rechte der Nutzer Grundrolle (ID 7).

Beschreibung zum Anlegen von Rollen

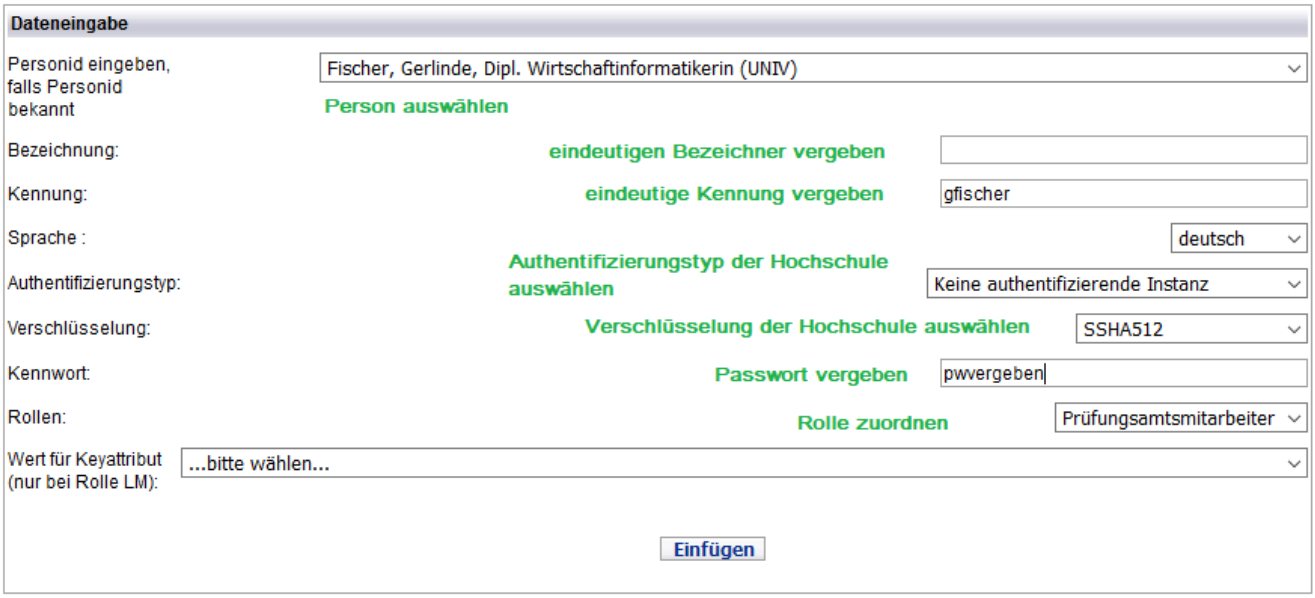
In FlexNow können bestimmte Rollen parametrisiert werden. Man kann ihnen Fakultäten und / oder Studiengänge zuordnen und so Berechtigungen vergeben. Aktuell beschränkt sich diese Funktionalität auf die Rollen PA und PAVOR.

Wird der Person eine Fakultät zu geordnet, ist diese zur Bearbeitung für alle Studiengänge der zugeordneten Fakultät freigeschaltet. Werden der Person, zusätzlich zur Fakultät, Studiengänge zugeordnet, beschränken sich die Berechtigungen der Person auf diese Studiengänge der Fakultät.

Werden der Person auch Berechtigungen für Studiengänge außerhalb der zugeordneten Fakultät hinzugefügt, ist die Person zusätzlich zur Bearbeitung dieser Studiengänge berechtigt.

Werden der Person nur Studiengänge zugeordnet, dann die diese ausschließlich für diese Studiengänge berechtigt.

Anlegen eines neuen Nutzers



Unter dem Menü-Punkt **'Personen verwalten'** - **'Neue Person anlegen'** kann man einen neuen Nutzer anlegen. Handelt es sich um eine Organisationseinheit bzw. Person, die bereits in FlexNow existiert, kann diese im ersten Dropdown-Feld ausgewählt werden. In den nachfolgenden Feldern werden Benutzername, Kennung, etc. vergeben. Bei den Werten für die Authentifizierung und die Verschlüsselung ist darauf zu achten, dass auch wirklich die Werte ausgewählt werden, welche die Hochschule benutzt.

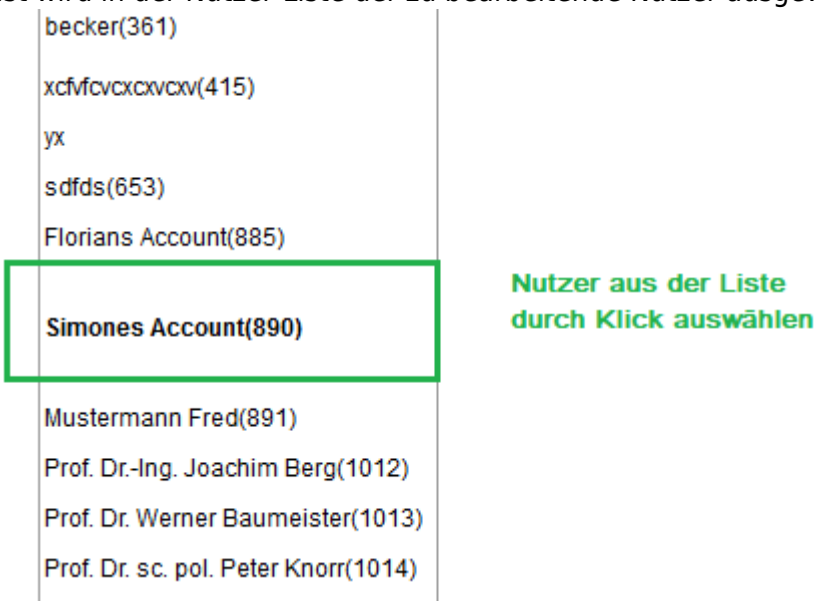
Wird dem Nutzer die Rolle **'Lehreinheit'**,**'Modulverantwortlicher'** oder **'Studiengangsbeauftragter'** zugeordnet, muss aus dem darauffolgenden DropDown-Feld eine Organisiationseinheit ausgewählt werden für die der neue Nutzer zuständig ist. Für die Rollen **'Prüfungsamtmitarbeiter'** (RolleID = 3) und **'PAVOR'** muss an der Stelle nichts ausgwählt werden.

Zuordnung der Fakultäten und Studiengänge in FN2RBACWEB

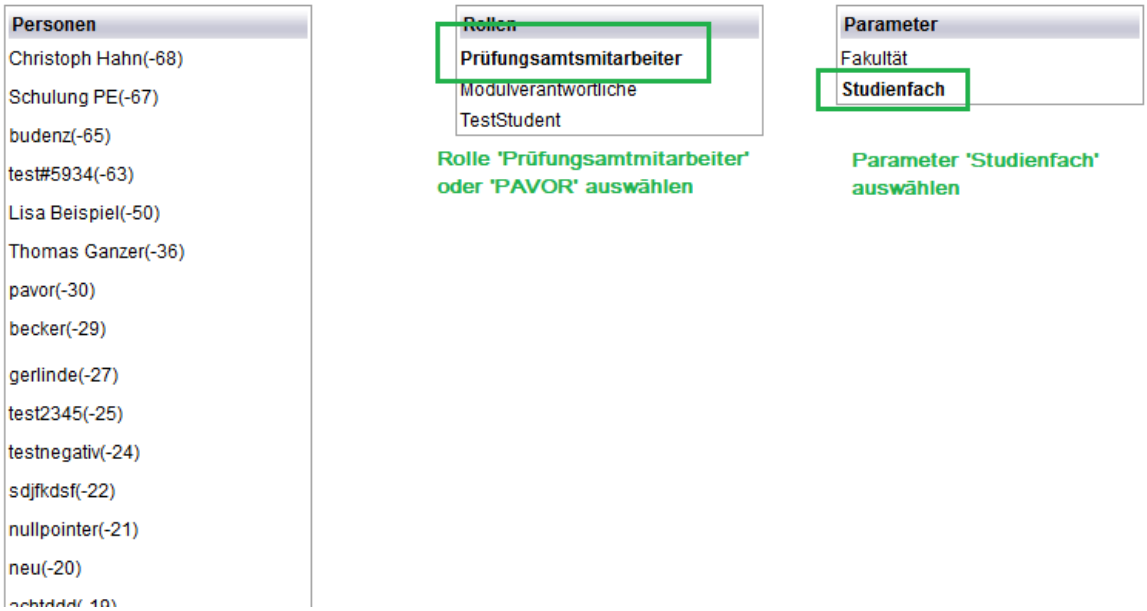
Wurde ein Nutzer mit der Rolle 'Prüfungsamtmitarbeiter' oder 'PAVOR' angelegt, ist es für die Arbeit in fn2Web zwingend erforderlich, dass dem Nutzer Berechtigungen für Fakultäten und / oder Studiengänge zugeordnet werden.

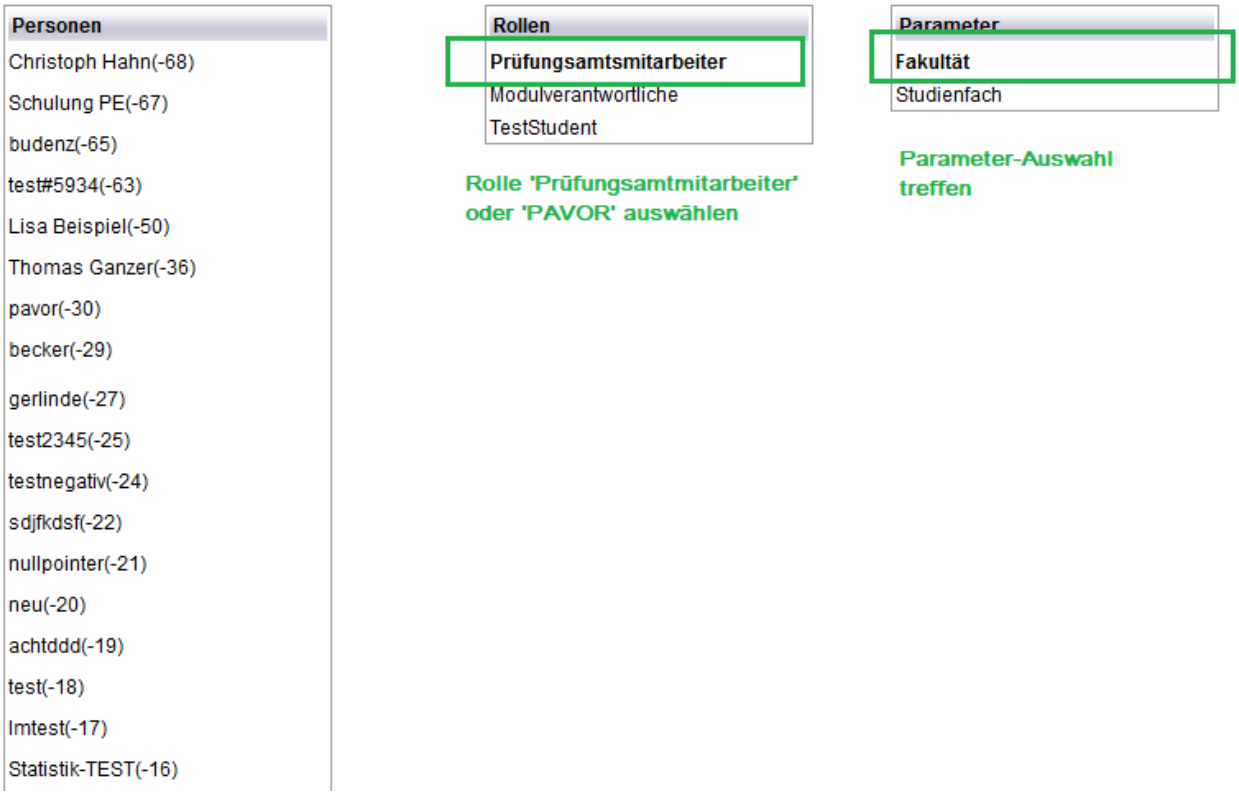
Die Parametrisierung kann unter *'Person verwalten'* - *'Parametrisierung'* vorgenommen werden.

Zunächst wird in der Nutzer-Liste der zu bearbeitende Nutzer ausgewählt.

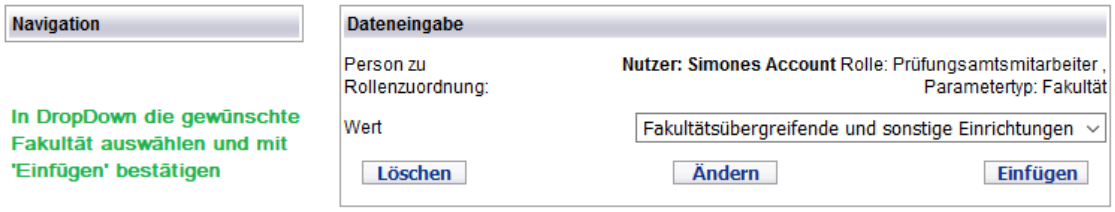


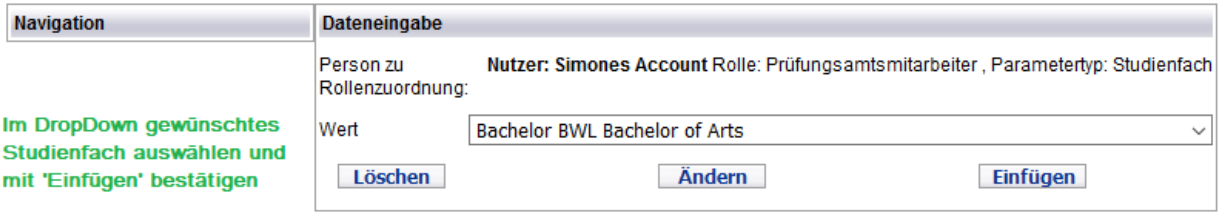
Anschließend erhält man eine Auflistung der Rollen, die dem Nuzter zugeordnet sind. Um einen Studiengang oder eine Fakultät zuordnen zu können, muss hier 'Prüfungsamtmitarbeiter' oder 'PAVOR' ausgewählt werden.





Je nachdem welchen Parameter man dem Nutzer änhängen möchte, wählt man 'Fakultät' oder 'Studiengang' aus und bekommt im nächsten Dialog eine Auswahlliste angeboten, aus der man die gewünschte Fakultät bzw. den gewünschten Studiengang auswählt.





ToDo zur Release vom 30.04.2020 (und höher)

Vorbemerkung: Welche Rollen an den jeweiligen Hochschulen zum Einsatz kommen, hängt stark von der Organisationsstruktur im Prüfungsamt ab. Es muss vor Einrichten der Rollen und der Zuordnung geklärt werden, ob alle PA-Mitarbeiter:innen die jeweilige Funktion ausführen dürfen oder nur dezidierte. Wer erhält welches Zugriffsrecht? Haben alle Prüfungsamtsmitarbeiter:innen die gleichen Rechte, so können diese auch direkt der Rolle „PA (ID = 3)“ zugeordnet werden. Falls es Unklarheiten gibt, bitte mit Gerlinde Fischer Kontakt aufnehmen.

- Der Webservice-Server muss für die Module erreichbar sein. In der Tabelle SETUP_ muss ein Eintrag für 'WEBSERVICE_SERVER' gemacht werden.
- Es ist zu prüfen, ob für alle User der fn2Module ein Eintrag in FN2META existiert. Die Kennung muss dem Datenbank-Usernamen entsprechen. Unter dem Menü-Punkt 'Personen verwalten' - Kennung ändern oder hinzufügen kann diese Kennung hinzugefügt werden. Bitte dabei den Authentifizierungstyp 'FN INTERN' verwenden.
- Für diese User muss jeweils die Rolle 3 „PA“ vergeben sein. Falls die Rollen umbenannt wurden, bitte in der FN2META Datenbank nachsehen, wie die Rolle mit der ID 3 an der jeweiligen Hochschule heisst.
- Sichtbarkeit von Fakultäten und Studiengängen: Pro User ist zu prüfen, ob die nötigen Einträge vorhanden sind. Fehlende Einträge müssen ergänzt werden. Sollen alle PA-User grundsätzlich alles sehen dürfen, so kann durch die Vergabe des Rechtes fnModule.isSuperuser die sonstige Zuordnung entfallen. Ob dieses Recht durch Zuordnung zu einer bestehenden Rolle oder durch Zuordnung einer extra Rolle zu bestimmten Personen verknüpft wird, ist von der Organisationsstruktur an der Hochschule definiert. Bitte Rücksprache bei Unklarheiten.
- User, die aus dem PA-Modul ins PO-Modul springen können sollen, benötigen die Rolle 63 „PO-Modul öffnen“.
- User, die Gruppen der Wiedervorlage verwalten können sollen, benötigen die Rolle 66 „Wiedervorlage Admin“. Diese Rolle wurde mit den SQL-Skripten publiziert und muss den dafür vorgesehen Personen zugeordnet werden.

Siehe auch: https://wiki.ihb-eg.de/doku.php/fn2service_pa/

From:
https://wiki.ihb-eg.de/ - **FlexWiki**

Permanent link:
https://wiki.ihb-eg.de/doku.php/fn2service_auth/start

Last update: **2021/02/25 09:12**