31.01.2022

„Kochrezept“: Bereitstellung von Rollen-Informationen über IdM.nrw

Es wurden zwei Szenarien aufgestellt. Das erste Szenario bildet eine kleine Uni mit einer zentralen Backup Verwaltung ab (Abbildung 1). Das zweite Szenario bildet eine große Uni mit mehreren zentralen Admins ab, die auch auf Instituts- oder Fachbereichsebene aktiv sind (Abbildung 2).

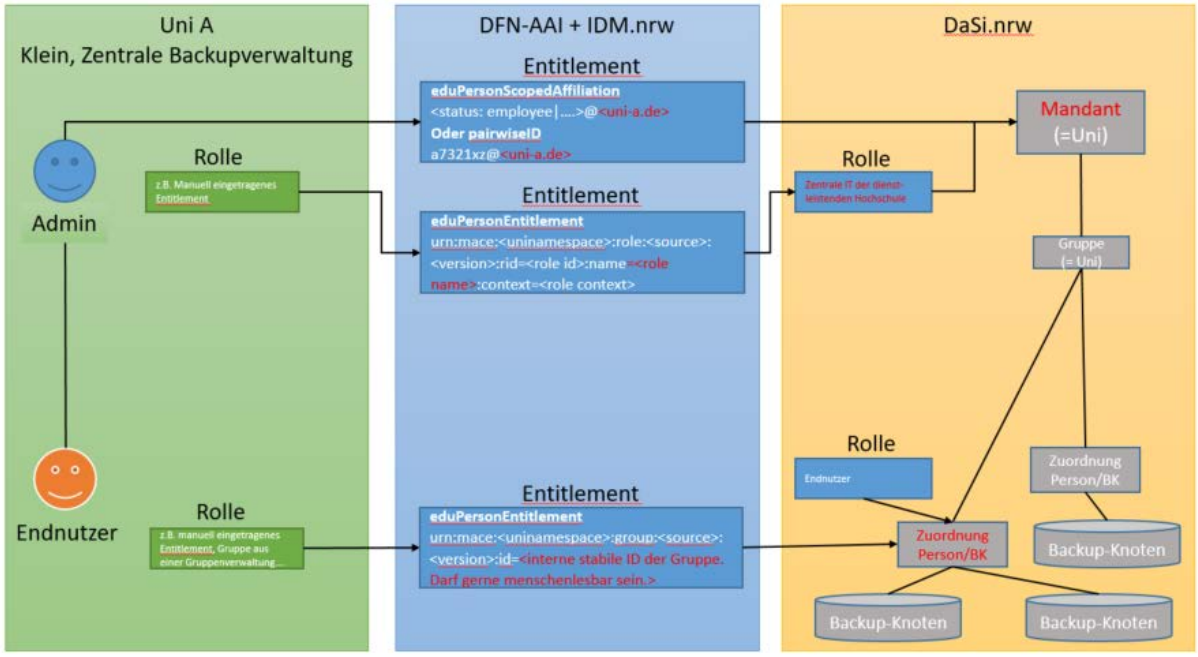

Abbildung 1. Kleine Uni mit zentraler Backuperwaltung

Admin und Endnutzer egal wer die Person ist und woher sie kommt, lässt sich immer über die beide Entitlemets (eduPersonScopedAffiliation oder pairwiseID) erkennen. So lässt sich die Zugehörigkeit zum Mandanten bestimmen. Über das eduPersonEntitlement (*urn:mace:<uninamespace>:role:<source>: <version>:rid=<role id>:name=<role name>:context=<role context>*) wird die Rolle des zentralen Admins übertragen.

Endnutzer ist eine organisatorische Rolle, der Mensch ist nur Endnutzer und hat nur den Zugriff auf einen Backup Knoten. Es ist also keine direkte Rolle, wo das Recht dranhängt. Die Zuordnung Person/Backup Knoten ist das was man für den Endnutzenden abbilden muss.

Die Rolle sagt nur in welchem Mandant ist der Endnutzer und für welchen einzelnen oder mehreren Knoten hat er Zugriff. Das eduPersonEntitlement (*urn:mace:<uninamespace>:group:<source>: <version>:id=<interne stabile ID der Gruppe. Darf gerne menschenlesbar sein.>*) entspricht einer Gruppe und die Gruppe entspricht einer Zuordnung genau zwischen einem Backup Knoten und einer Person. Auf beiden Seiten muss etwas gemacht werden. Auf beiden Seiten muss der Endnutzende durch irgendetwas markiert werden und in diesem Fall ist es eine Gruppe, dass als Entitlement transportiert wird und auf der anderen Seite muss festgelegt werden welche Berechtigung auf welchem Backup Knoten die Gruppe hat.

Datensicherung.nrw muss die Vorgabe machen wie die Rolle heißen soll und muss auch sagen, dass eine Gruppe 173 für den Backup Knoten abcdf angelegt wurde und wenn eine Person aus der Gruppe 173 zugreifen soll muss der Endnutzende entsprechend der Gruppe 173 zugeordnet werden.

D.h. der Admin muss diese Gruppe 173 bei Datensicherung.nrw anlegen und gleichzeitig auch bei sich an der Uni.

Da bleibt die Frage offen, macht Datensicherung.nrw da bestimmte Vorgaben oder sagt sie wir nehmen alles was da kommt und dann kann der Admin da alles reinschreiben.

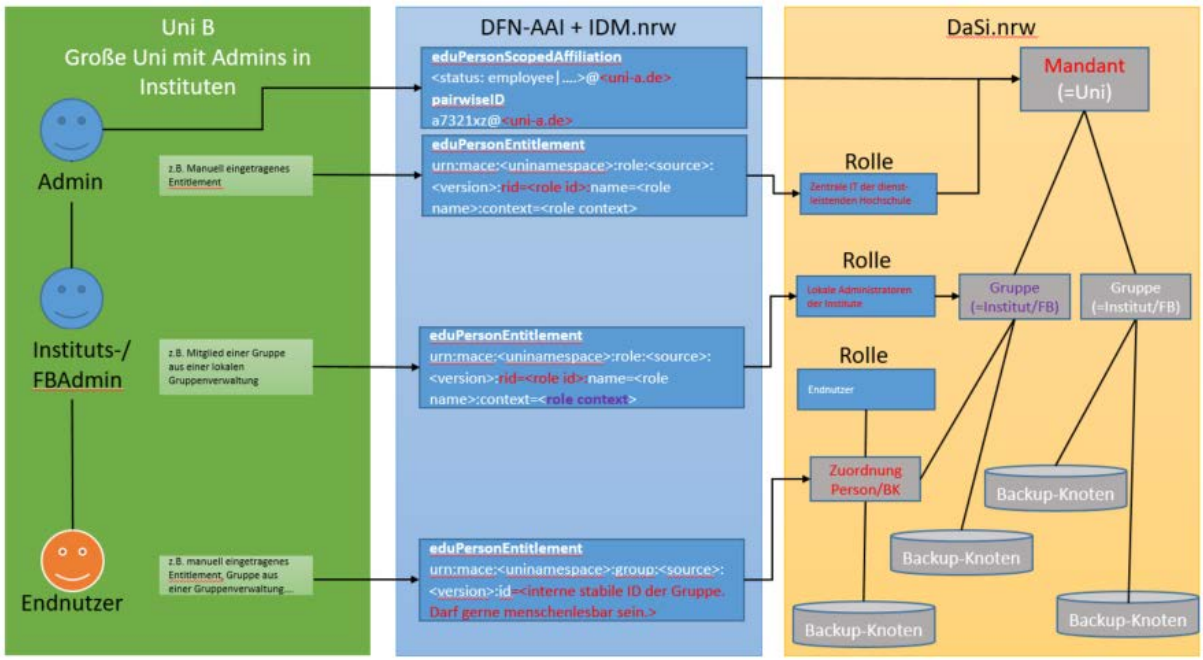

Abbildung 2. Große Uni mit Admins in Instituten/Fachbereichen

Das zweite Szenario ist fast identisch bis auf den Instituts- oder Fachbereichsadmin. Der Institutsadmin oder Fachbereichsadmin ist durch den „context“ in eine bestimmte Gruppe zugeordnet. Von dort aus kann er/sie die Zuordnung seiner Endnutzenden auf einen Backup knoten vornehmen.