Account Deprovisioning and Deletion

GUnet Identity Management

Πολιτική Διαγραφής Ανενεργών Λογαριασμών

Οριστική Διαγραφή Ανενεργών Λογαριασμών ή Ιδιοτήτων μετά το πέρας μίας συγκεκριμένης περιόδου μετά την Απενεργοποίησή(*) τους.

Γίνεται σε 3 Στάδια:

1. Active -> Interim
2. Interim -> Inactive : Deprovisioning
3. Deprovisioning -> Οριστική Διαγραφή

(*) Απενεργοποίηση Λογαριασμού: enrollmentStatus/employeeStatus not in (‘active’ or ‘interim’)

Γιατί είναι απαραίτητη;

- Ασφάλεια
    1. Αποφυγή επιθέσεων σε Λογαριασμούς που είναι ανενεργοί για πολύ καιρό
    2. Αποτροπή χρηστών να χρησιμοποιούν υπηρεσίες, χωρίς να έχουν πλέον ενεργό ρόλο στο ίδρυμα
- Καλύτερη απόδοση της Identity Management Υπηρεσίας
    1. Η διαδικασία συγχρονισμού θα λειτουργεί γρηγορότερα με την αφαίρεση ανενεργών Λογαριασμών
    2. Αποφυγή συγκρούσεων λόγω ασυνεπειών που υπάρχουν σε εγγραφές παλαιών ανενεργών Ιδιοτήτων

Λογαριασμός

Το αντικείμενο της υπηρεσίας Identity Management που περιλαμβάνει:

1. τα στοιχεία ταυτοποίησης, αυθεντικοποίησης και ελέγχου πρόσβασης ενός χρήστη σε υπηρεσίες
2. το προφίλ του χρήστη όπως αυτό προκύπτει από ένα ή περισσότερους ρόλους του στο Πανεπιστήμιο

Ιδιότητα

Η εγγραφή στο αντίστοιχο Πληροφοριακό Σύστημα του Ιδρύματος (SIS, HRMS, ELKE) και περιγράφει τη σχέση του χρήστη με το ίδρυμα.

Κάθε **Ιδιότητα** χρήστη μπορεί να είναι σε μία από τις παρακάτω καταστάσεις:

1. Active: μία ενεργή Ιδιότητα στο ίδρυμα
2. Interim: η **πρώτη μεταβατική κατάσταση** μιας ιδιότητας όταν αλλάζει από Ενεργή σε Ανενεργή
3. Inactive('graduated', 'discontinued'): μια ιδιότητα η οποία είναι ανενεργή στο ίδρυμα

Προσοχή: Οι **ανενεργές ιδιότητες δεν πρέπει να εξαφανίζονται από το view.** Θα πρέπει να διατηρούνται και για εύλογο χρονικό διάστημα που είναι της τάξης των 2+ ετών και να μαρκάρονται αναλόγως, είτε ως inactive είτε ως discontinued, graduated, retired κτλ.

Πρώτο Στάδιο: Active -> Interim

- Το πεδίο enrollmentStatus/employeeStatus της εγγραφής στο view γίνεται από ‘active’ σε ‘interim’
- Ο Λογαριασμός εξακολουθεί να είναι ενεργός στην IdM Υπηρεσία.
- Δίνεται χρόνος στον χρήστη να προβεί σε τελικές ενέργειες backup πριν την απενεργοποίηση του Λογαριασμού.
- Ο καθορισμός και η υλοποίηση της πολιτικής για την 'interim' κατάσταση των ιδιοτήτων είναι στην αποκλειστική αρμοδιότητα του κάθε Πανεπιστημίου.

Πρώτο Στάδιο: Active -> Interim (2)

Υπόδειγμα μετάβασης από Active σε Interim για απόφοιτους διδακτορικού:

```
If type = doctoral & status = graduated {
        If current date < graduation date + X days {
                enrollmentStatus = interim;
                enrollmentStatusDate = graduation date;
        } else {
                enrollmentStatus = graduated;
                enrollmentStatusDate = graduation date + X days
        }
}
```

Δεύτερο Στάδιο - Interim -> Deprovisioned

- Το enrollmentStatus/employeeStatus γίνεται από ‘interim’ σε ‘inactive’
- Το Object του χρήστη στον DS χάνει τα attributes Ταυτότητας του χρήστη και παίρνει την objectClass Account (*)
- Μπορεί μόνο να κάνει bind στον DS με το uid
- Διατηρείται η πρόσβαση σε ορισμένες υπηρεσίες

(*) Σε περίπτωση που όλες οι ιδιότητες δεν είναι ‘inactive’, τότε απλά αφαιρούνται

Δεύτερο Στάδιο - Interim -> Deprovisioned (2)

- Πρόκειται για μία Μεταβατική Κατάσταση

- Το Πανεπιστήμιο δεν θα πρέπει να βασίζεται στη δυνατότητα πρόσβασης αυτών των χρηστών σε κάποιες υπηρεσίες που δεν απαιτούν ειδικά στοιχεία.

Τρίτο Στάδιο - Οριστική Διαγραφή

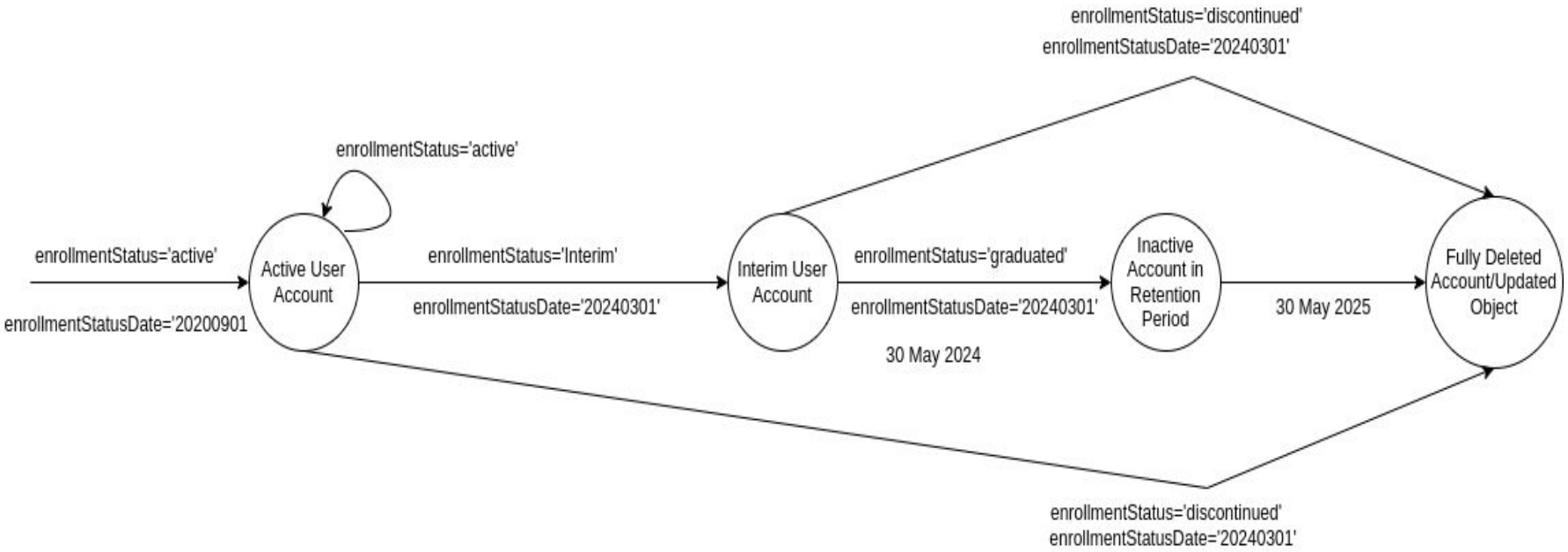
Μετά το πέρας της Περιόδου Χάριτος, διαγράφεται οριστικά το object από τον DS

Αν έχει ενεργές ιδιότητες, τότε αφαιρούνται μόνο το uid και οι αντίστοιχες τιμές του schGrAcPersonLinkageID

Από τη διαγραφή αυτή εξαιρούνται:

1. Οι employeeStatus = ‘retired’
2. Όσους χρήστες επιστρέψει αυτό το φίλτρο από τον DS:
   "(&(objectClass=schacLinkageIdentifiers)(|(!(objectClass=account))
   (cn=*)(sn=*)(givenName=*)(mail=*)
   (eduPersonEntitlement=urn:mace:gunet.gr:idm:keep_ds)))"

Κύκλος Ζωής Λογαριασμού Φοιτητή



Διαγραφή Επαυξημένων Λογαριασμών

- Η υπηρεσία IdM κατά το deprovisioning δεν μπορεί να γνωρίζει αν η διαγραφή από το IdM/DS οδηγήσει στη δημιουργία ορφανών δεδομένων σε κάποιο εσωτερικό πληροφοριακό σύστημα του ιδρύματος.
- Θα πρέπει **να αφαιρεθούν θα attributes που επαυξάνουν το object που πρέπει να διαγραφεί οριστικά**.
- **Αυτή η ενέργεια θα πρέπει να γίνεται από το ίδιο τα ίδρυμα.**

Διατήρηση Λογαριασμών στον DS

- Υπάρχει πιθανότητα το Ίδρυμα να μην επιθυμεί τη διαγραφή κάποιων Λογαριασμών, ανεξάρτητα από το enrollmentStatus/employeeStatus στο view.

- Σε αυτήν την περίπτωση θα πρέπει να προστίθεται το attribute **eduPersonEntitlement** στο object του χρήστη που δεν πρέπει να διαγραφεί από τον DS και να έχει την τιμή: **urn:mace:gunet.gr:idm:keep_ds**

Προεργασία

1. Διορθώσεις των πεδίων **registrationID, systemID, loginName, enrollmentStatus/employeeStatus** και **enrollmentStatusDate/employeeStatusDate**

2. Όλοι οι σχετιζόμενοι χρήστες να φαίνονται στο view

3. Έλεγχος Λογαριασμών στον DS που δεν πρέπει να διαγραφούν

4. Απόφαση για το retentionPeriod στα SIS/HRMS