Account Lifecycle Deprovisioning and Deletion

GUnet Identity Management

ΕΙΣΑΓΩΓΗ

Ο **Κύκλος Ζωής ενός Λογαριασμού** στην υπηρεσία Identity Management ξεκινά με την αρχική ενεργοποίησή του μέσω της υπηρεσίας URegister του εκάστοτε ιδρύματος. Τα στοιχεία του Λογαριασμού αυτού συγχρονίζονται στην Υπηρεσία Καταλόγου(Directory Service - DS) του Ιδρύματος και διατηρούνται εκεί καθ' όλη τη διάρκεια της ζωής του. Τα στοιχεία αυτά, στο σύνολό τους, επιτρέπουν την πρόσβαση σε διάφορες υπηρεσίες του Ιδρύματος, ανάλογα με την/τις ιδιότητα/τες του φυσικού προσώπου στο οποίο ανήκει ο Λογαριασμός αυτός. Κατά το πρώτο στάδιο της διαγραφής του Λογαριασμού, τα στοιχεία που αφορούν την πρόσβαση στις υπηρεσίες διαγράφονται από την Υπηρεσία DS και παραμένουν τα ελάχιστα δυνατά για την ταυτοποίηση του χρήστη. Κατά την τελική διαγραφή, διαγράφεται ο Λογαριασμός μαζί με όλα τα στοιχεία του τον αφορούν.

Πιο αναλυτικά, ως **Λογαριασμός** νοείται το αντικείμενο της υπηρεσίας Identity Management που περιλαμβάνει α)τα στοιχεία ταυτοποίησης, αυθεντικοποίησης και ελέγχου πρόσβασης ενός χρήστη σε υπηρεσίες και β)το προφίλ του χρήστη όπως αυτό προκύπτει από ένα ή περισσότερους ρόλους του στο Πανεπιστήμιο.

Ως **Ιδιότητα** ενός χρήστη νοείται 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:

Active: Πρόκειται για μία ενεργή Ιδιότητα στο ίδρυμα. Για να είναι μία ιδιότητα ενεργή, το πεδίο enrollmentStatus/employeeStatus θα πρέπει να έχει αποκλειστικά την τιμή 'active' και το πεδίο *enrollmentStatusDate/employeeStatusDate* θα πρέπει να περιέχει την ημερομηνία ενεργοποίησης της ιδιότητας αυτής(σε format YYYYMMDD) στο αντίστοιχο πληροφοριακό σύστημα**.**

Inactive: Πρόκειται για μια ιδιότητα η οποία είναι ανενεργή στο ίδρυμα, δηλαδή η συγκεκριμένη σχέση του χρήστη με το ίδρυμα έχει τερματιστεί. Καθορίζεται από την τιμή των πεδίων *enrollmentStatus/employeeStatus* και *enrollmentStatusDate/employeeStatusDate*. Στο πεδίο *enrollmentStatus/employeeStatus* μπορεί να είναι γενικά 'inactive', αλλά μπορεί να ορισθεί και η αιτία διακοπής της σχέσης, που μπορεί να είναι πχ. 'graduated','discontinued', για τους φοιτητές, ή πχ.'retired' για τους εργαζόμενους. Περισσότερες πληροφορίες σχετικά με τις δυνατές τιμές των πεδίων *enrollmentStatus/employeeStatus* βρίσκονται στα definitions των SIS και HRMS views.

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.

Interim: Πρόκειται για τη **πρώτη μεταβατική κατάσταση** μιας ιδιότητας όταν αλλάζει από Ενεργή σε Ανενεργή. Η χρήση της κατάστασης αυτής μπορεί να αξιοποιηθεί από το ίδρυμα για την διατήρηση του Λογαριασμού ενός χρήστη πέρα του χρόνου λήξης της συμβατικής σχέσης του χρήστη με το ίδρυμα. Παραδείγματα χρήσης μπορούν να είναι τα εξής:

- Φοιτητές που πρέπει να διατηρήσουν τα στοιχεία του φοιτητικού ρόλου του λογαριασμού τους για ένα διάστημα μετά την ημερομηνία ανακήρυξής τους.
- Μέλη ΔΕΠ που πρέπει να διατηρήσουν την πρόσβαση σε υπηρεσίες όπως το eClass ή στον ΕΛΚΕ, μετά την συνταξιοδότησή τους.
- Ερευνητές με κενά μεταξύ διαδοχικών συμβάσεων στον ΕΛΚΕ. Η υιοθέτηση πολιτικής "interim" για ένα χρονικό διάστημα μετά την τυπική λήξη της σύμβασης εξασφαλίζει την ομαλή συνέχεια του δικτυακού λογαριασμού του χρήστη

Σημειώνεται ότι ο καθορισμός και η υλοποίηση της πολιτικής για την 'interim' κατάσταση των ιδιοτήτων είναι στην αποκλειστική αρμοδιότητα του κάθε Πανεπιστημίου και θα πρέπει να υπάρχει πρόβλεψη υλοποίησης της πολιτικής αυτής στο αντίστοιχο πληροφοριακό σύστημα του ιδρύματος. Για παράδειγμα, κατά την ανακήρυξη ενός διδάκτορα το status της ιδιότητας αυτής θα μπορούσε να διαμορφώνεται σύμφωνα με τον παρακάτω ψευδο-κώδικα:

```
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
  }
}
```

Όπως δηλώνεται από το όνομα της κατάστασης (interim), αυτή θα πρέπει να χρησιμοποιείται αποκλειστικά για προσωρινό διάστημα με αποκλειστικό σκοπό την εξυπηρέτηση μεταβατικών καταστάσεων, καθώς κατά παρέκκλιση των κανόνων ο συμβατικά ανενεργός ρόλος συνεχίζει να τροφοδοτεί με στοιχεία το δικτυακό προφίλ του χρήστη. Αν η εφαρμογή της κατάστασης interim υπερβαίνει το διάστημα λίγων μηνών και παίρνει μόνιμο χαρακτήρα, επειδή για παράδειγμα ο χρήστης δεν έχει πλέον καμια συμβατική σχέση με το ίδρυμα (SIS,HRMS,ΕΛΚΕ), για να διατηρήσει τον Λογαριασμό του, θα πρέπει τότε να εξεταστεί η λύση της μεταφοράς του λογαριασμού του χρήστη κάτω από το σχήμα των local accounts στην Υπηρεσία Καταλόγου(Directory Service - DS) με την ιδιότητα eduPersonAffiliation = affiliate.

ΔΙΑΓΡΑΦΗ ΛΟΓΑΡΙΑΣΜΟΥ

Η διαγραφή ενός λογαριασμού ακολουθεί 2 στάδια, που είναι τα **Account Deprovisioning** και **Account Deletion**.

Account Deprovisioning
Όταν **όλες οι ιδιότητες** ενός χρήστη γίνουν inactive, τότε η υπηρεσία Identity Management ενεργοποιεί τη διαδικασία **Account Deprovisioning**. Η διαδικασία αυτή οδηγεί στη **δεύτερη μεταβατική κατάσταση** ενός Λογαριασμού πριν την οριστική διαγραφή του. Κατά το account deprovisioning ο Λογαριασμός μεταβαίνει σε κατάσταση ελάχιστης λειτουργικότητας. Επιτρέπεται μόνο η αυθεντικοποίηση του χρήστη και αφαιρούνται από τον Λογαριασμό του όλα τα ονοματεπωνυμικά στοιχεία καθώς και τα στοιχεία ρόλων που προέρχονταν από τα πρωτογενή πληροφοριακά συστήματα (SIS,HRMS,ΕΛΚΕ). Τα αποτελέσματα της διαδικασίας deprovisioning αποτυπώνονται στο προφίλ του Λογαριασμού στην υπηρεσία SSO σε πραγματικό χρόνο, και στην υπηρεσία DS, στον επόμενο συγχρονισμό του LDAP object, όπου ή structural objectclass υποβαθμίζεται από inetOrgPerson σε account.

Επισημαίνεται ότι η κατάσταση αυτή είναι ενδιάμεσο στάδιο πριν την διαγραφή του Λογαριασμού, και το ίδρυμα δεν θα πρέπει να βασίζεται στη δυνατότητα πρόσβασης αυτών των χρηστών σε κάποιες υπηρεσίες που δεν απαιτούν ειδικά στοιχεία. Περισσότερες πληροφορίες υπάρχουν στο Διαγραφή μη ενεργών λογαριασμών από τον ιδρυματικό ldap.

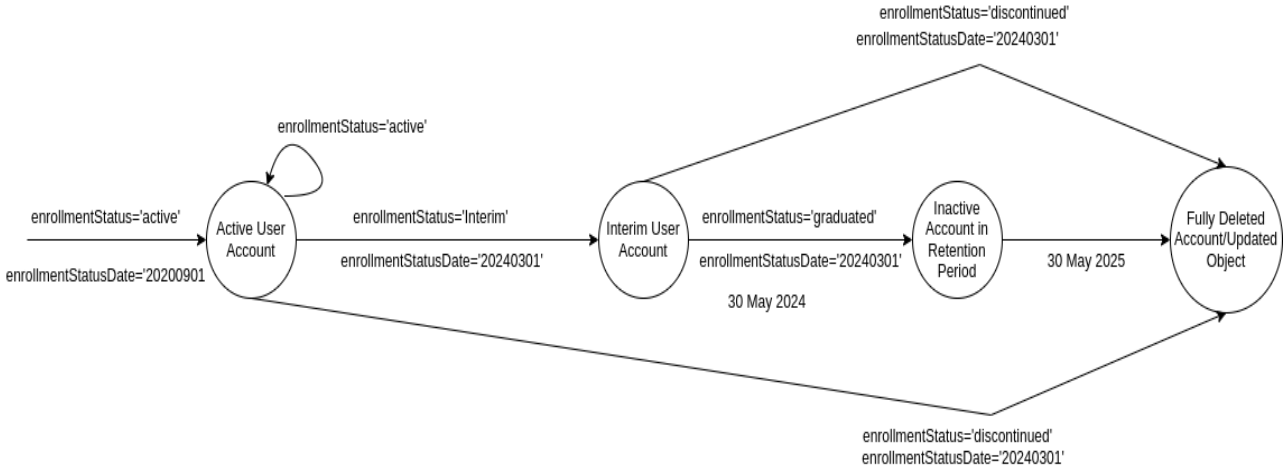
Account Deletion
Ο μηχανισμός οριστικής διαγραφής (account deletion) έπεται της διαδικασίας απενεργοποίησης (account deprovisioning). Ακολουθώντας την πολιτική του ιδρύματος, **οι απενεργοποιημένοι λογαριασμοί θα διαγράφονται οριστικά** από την υπηρεσία Identity Management μετά την **πάροδο μιας περιόδου χάριτος**. Η περίοδος αυτή θα υπολογίζεται με βάση το πεδίο enrollmentStatusDate/employeeStatusDate, όταν η τιμή του πεδίου enrollmentStatus/employeeStatus θα γίνεται διάφορη του active ή του interim. Οπότε το πεδίο enrollmentStatusDate/employeeStatusDate θα πρέπει να είναι πάντα ενημερωμένο.

Για παράδειγμα, ένας φοιτητής ανακηρύσσεται την 1η Μαρτίου 2024. Μετά από 3μηνη 'interim' περίοδο, γίνεται 'graduated' στο IDM SIS DB View στις 30 Μαΐου. Η υπηρεσία Identity Management τότε θα αφαιρέσει από τον Λογαριασμό του χρήστη κάθε αναφορά στο φοιτητικό του ρόλο. Αν του δοθεί περίοδος χάριτος 12 μηνών, τότε στις 30 Μαίου 2025 θα διαγραφεί οριστικά από την υπηρεσία Identity Management, εφόσον δεν έχει προκύψει άλλη μεταβολή ρόλων του χρήστη.

Από την διαδικασία Account Deletion εξαιρούνται:

1. όσοι SIS χρήστες πάρουν τιμή enrollmentStatus='discontinued', οι οποίοι θα διαγράφονται αμέσως.
2. όσοι HRMS χρήστες έχουν employeeStatus='retired', η οριστική διαγραφή των οποίων συνεχίζει να εκτελείται μετά από επιλογή των διαχειριστών του ιδρύματος.

Στην Εικόνα 1 φαίνεται το διάγραμμα του Κύκλου Ζωής του Λογαριασμού του φοιτητή του παραδείγματος.



Εικόνα 1: Ενδεικτικός Κύκλος Ζωής Λογαριασμού φοιτητή.

Ειδικός Χειρισμός στην Υπηρεσία DS
Η Υπηρεσία Καταλόγου (Directory Service - DS) εξυπηρετεί πολλαπλούς ρόλους στην υπηρεσία IdM. Συγκεκριμένα η υπηρεσία DS αποτελεί:

1. **target σύστημα της υπηρεσίας IdM** για τις κατηγορίες **χρηστών με ενεργό ρόλο** ή ρόλους σε ένα ή περισσότερα πρωτογενή πληροφοριακά συστήματα του ιδρύματος (SIS,HRMS,ΕΛΚΕ).
2. **source σύστημα της υπηρεσίας IdM** για την κατηγορία **επισκεπτών του ιδρύματο**ς στους οποίους αποδίδεται προσωρινός Λογαριασμός πχ για την πρόσβαση στο ασύρματο δίκτυο, μέσω της υπηρεσίας uGuest.
3. **source σύστημα της υπηρεσίας IdM** για την κατηγορία των “**local DS λογαριασμών**”, οι οποίοι κατασκευάζονται απευθείας υπηρεσία DS από τους διαχειριστές του ιδρύματος για την απόδοση λογαριασμών σε φυσικά πρόσωπα που δεν έχουν κάποια συμβατική σχέση με το ίδρυμα και δεν υπάγονται σε καμία από τις κατηγορίες φοιτητές, μέλη ΔΕΠ, προσωπικό ή συνεργάτες με σύμβαση.

Για τις δύο τελευταίες κατηγορίες χρηστών, η υπηρεσία DS λειτουργεί ως ειδικό πρωτογενές πληροφοριακό σύστημα του ιδρύματος που τροφοδοτεί την υπηρεσία IdM με αυτοτελείς Λογαριασμούς χρηστών. Ως εκ τούτου η διαχείριση του κύκλου ζωής τους δεν αποτελεί αντικείμενο της IdM υπηρεσίας. Ειδικότερα για τη διαγραφή αυτών των Λογαριασμών ισχύουν τα παρακάτω:

- Η διαγραφή των uGuest χρηστών εκτελείται αυτόματα, από το σύστημα διαχείρισης της υπηρεσίας uGuest, βάση των πολιτικών που έχουν ορισθεί εκεί και του χρόνου ζωής των λογαριασμών που δημιουργούνται.
- Η διαγραφή των local DS λογαριασμών, είναι στην αποκλειστική ευθύνη, των διαχειριστών του ιδρύματος τόσο ως προς το χρόνο όσο και ως προς τον μηχανισμό που θα επιλεγεί.

Η κατηγορία Λογαριασμών ωστόσο που αρχικοποιούνται και ενημερώνονται από την υπηρεσία IdM είναι μια πιο σύνθετη περίπτωση. Αυτού του τύπου οι Λογαριασμοί μπορούν να επαυξηθούν εντός της υπηρεσίας DS, από τους διαχειριστές του ιδρύματος, με επιπλέον στοιχεία (ojectClasses, attributes) για την εξυπηρέτηση απαιτήσεων συγκεκριμένων υπηρεσιών. Χαρακτηριστικές περιπτώσεις είναι προσθήκη ειδικών στοιχείων για τη λειτουργία σταθμών εργασίας σε εργαστήρια, για τη λειτουργία της υπηρεσίας eMail, ή τη λειτουργία IP phones. Για το λόγο αυτό οι Λογαριασμοί αυτής της κατηγορίας στην υπηρεσία DS αποτελούν ταυτόχρονα target accounts, για όσα στοιχεία προέρχονται από τα πρωτογενή πληροφοριακά συστήματα, και source accounts για τα επιπρόσθετα στοιχεία καθως κατ' επιλογή τα στοιχεία αυτά γίνονται διαθέσιμα μέσω των IdM ροών και προς τρίτες υπηρεσίες.

Διαγραφή επαυξημένων Λογαριασμών

Στο σενάριο που η υπηρεσία DS περιλαμβάνει Λογαριασμούς με επαυξημένα στοιχεία, 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. Για παράδειγμα η παρουσία της objectClass posixAccount στα LDAP objects της υπηρεσίας DS που διαχειρίζεται το IdM, σηματοδοτεί ότι ο Λογαριασμός αυτός διατηρεί σε μια συνδεδεμένη υπηρεσία (π.χ. Linux Labs, ή Mail Message Store) μια περιοχή δεδομένων (homeDirectory) που θα πρέπει να εκκαθαριστεί πριν το IdM διαγράψει τα στοιχεια uidNumber, gidNumber, homeDirectory, τα οποία απαιτούνται για την πρόσβαση στην περιοχή αυτή από τον χρήστη. Για το λόγο αυτό η παρουσία επαυξημένων Λογαριασμών στο DS, μπλοκάρει τη διαδικασία deprovisioning για τους Λοριασμούς αυτούς, ως εκ τούτου και την οριστική διαγραφή τους.

Στις περιπτώσεις αυτές, αν και το IdM μέσω της υπηρεσίας SSO δεν ανακοινώνει στοιχεία των ανενεργών ρόλων του χρήστη, οι υπηρεσίες που συνδέονται μέσω LDAP απευθείας στην υπηρεσία DS λαμβάνουν στοιχεία τα οποία αναφέρονται σε μη ενεργούς ρόλους τους. Για την επίλυση των θεμάτων αυτών αλλά και για την αποτελεσματικότερη διαχείριση της υπηρεσίας IdM, **τα ιδρύματα που επαυξάνουν τα DS LDAP objects, θα πρέπει να εκτελούν και τις διαδικασίες διαγραφής των στοιχείων αυτών**, μετά την παύση της συμβατικής σχέσης του χρήστη με το ίδρυμα και αυστηρά μέσα στην περίοδο χάριτος που έχει οριστεί.

Ενδεχόμενα τμήμα της διαδικασίας αυτής είναι και η εκκαθάριση δεδομένων από την εσωτερική υπηρεσία που κάνει χρήση των στοιχείων αυτών. Για παράδειγμα, στην περίπτωση των Linux Labs και της προσθήκης της objectClass=posixAccount, το ίδρυμα θα πρέπει να ενημερώσει τον χρήστη για την οριστική διαγραφή του προσωπικού του χώρου και όταν αυτή λάβει χώρα τότε να διαγράψει την objectClass posixAccount και τα posixAccount Attributes από τον DS. Ουσιαστικά, η διαδικασία διαγραφής θα πρέπει να ακολουθήσει ένα μοντέλο στοίβας, με τη διαγραφή των διαφόρων στοιχείων να λαμβάνει χώρα με την ανάποδη πορεία από αυτήν της δημιουργίας τους.

Υπάρχουν περιπτώσεις χρηστών όπου στον DS έχουν attributes που δίνουν πρόσβαση σε διάφορες υπηρεσίες του Ιδρύματος. Τέτοια παραδείγματα είναι η χρήση του attribute eduPersonEntitlement της objectClass='eduPerson' ή η χρήση των attributes της objectClass='posixAccount' τα οποία έχουν αναφορές στη mail υπηρεσία και ενδεχόμενα **δεν πρέπει να διαγραφούν άμεσα**.

Σε αυτήν την περίπτωση το deprovisioning θα γίνεται **σε δύο στάδια**:

1) Θα πρέπει **να αφαιρεθούν θα attributes της objectClass='posixAccount'** από τα objects των χρηστών που πρέπει να διαγραφούν οριστικά. **Αυτή η ενέργεια θα πρέπει να γίνεται από το ίδιο τα ίδρυμα.**

2) Μετά τη διαγραφή των attributes αυτών, οι χρήστες αυτοί εντάσσονται πλέον στην πολιτική που αναφέρθηκε παραπάνω και διαγράφονται.

Εντοπισμός Deprovisioned Λογαριασμών

Για τον εύκολο εντοπισμό των Objects που, κατά το Deprovisioning, το job συγχρονισμού προσθέτει το εξής eduPersonEntitlement Object στον deprovisioned Λογαριασμό:

urn:mace:gunet.gr:deprovision:<timestamp>, όπου το timestamp είναι η χρονοσφραγίδα της χρονικής στιγμής που άλλαξε το object από τον συγχρονισμό.

Για τον εντοπισμό των Λογαριασμών που είναι υποψήφιοι προς διαγραφή μετά την περίοδο χάριτος, θα τους επιστρέψει το εξής φίλτρο στον DS:

(&(objectClass=account)(eduPersonEntitlement=urn:mace:gunet.gr:deprovision:))*

Για τον εντοπισμό των Λογαριασμών που θα έπρεπε να γίνουν deprovision, αλλά αυτό απέτυχ, αυτοί επιστρέφονται με το παρακάτω φίλτρο. Το timestamp ορίζει τη χρονική στιγμή που θα έπρεπε να είχαν γίνει deprovision.

(&(objectClass=inetOrgPerson)(eduPersonEntitlement=urn:mace:gunet.gr:deprovision:))*

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*.

Ένα παράδειγμα είναι οι συνταξιοδοτημένοι χρήστες του HRMS με employeeStatus=’retired’. Μπορεί το object τους να ακολουθεί την πρώτη φάση του Deprovisioning, αλλά δεν πρέπει να γίνει οριστική διαγραφή τους. Στην περίπτωση αυτή, το Ίδρυμα θα πρέπει να προσθέσει το attribute eduPersonEntitlement=*urn:mace:gunet.gr:idm:keep_ds,* ώστε να αποτραπεί η οριστική διαγραφή τους από την Υποδομή.

Συνεπώς, για την αποφυγή διαγραφής των προαναφερθέντων Λογαριασμών, ο Μηχανισμός που αναπτύχθηκε επιλέγει από τον DS με το φίλτρο *"(&(objectClass=schacLinkageIdentifiers)(|(!(objectClass=account))(cn=*)(sn=*)(givenName=*)(mail=*)(eduPersonEntitlement=urn:mace:gunet.gr:idm:keep_ds)))"* αυτούς που **ΔΕΝ** πρέπει να διαγραφούν, τους αποκλείει και διαγράφει όλους τους υπόλοιπους.

Να σημειωθεί ότι, παρά το γεγονός ότι ο Μηχανισμός μεριμνά για τη μη διαγραφή των προαναφερθέντων Λογαριασμών, **η εκτέλεση των ενεργειών για την οριστική διαγραφή τους από το Ιδρυμα είναι επιτακτικής ανάγκης**, καθώς η μη διαγραφή και διατήρηση του μεγάλου όγκου των Λογαριασμών αυτών, επηρεάζει τόσο την απόδοση του Μηχανισμού, όσο και τη συνολική απόδοση της Identity Management Υποδομής του Ιδρύματος.

Ωστόσο, είναι στην απόλυτη ευχέρεια του Ιδρύματος αν θα διατηρήσει τα objects του DS που έχουν κάποια επιπλέον ιδιαιτερότητα στα attributes. Βεβαίως μπορούν και αυτές οι περιπτώσεις να διαγράφονται κατά τον βασικό Μηχανισμό, χωρίς τον παραπάνω έλεγχο για τα επιπλέον attributes, αν θεωρεί το Ιδρυμα ότι η περίοδος χάριτος που θα δοθεί είναι αρκετή ώστε να είναι και αυτοί οι Λογαριασμοί ασφαλείς προς διαγραφή.