# Εθνική υποδομή πιστοποίησης για ενοποιημένη πρόσβαση σε υπηρεσίες βιβλιοθηκών

ΕΘΝΙΚΟ ΔΙΚΤΥΟ ΕΡΕΥΝΑΣ & ΤΕΧΝΟΛΟΓΙΑΣ

Α. Βαρβιτσιώτης
Δ. Δασκόπουλος
Δ. Βαρδαλής

15ο Πανελλήνιο Συνέδριο Ακαδημαϊκών Βιβλιοθηκών 2/11/2006

# 1. Παρουσίαση ΕΔΕΤ

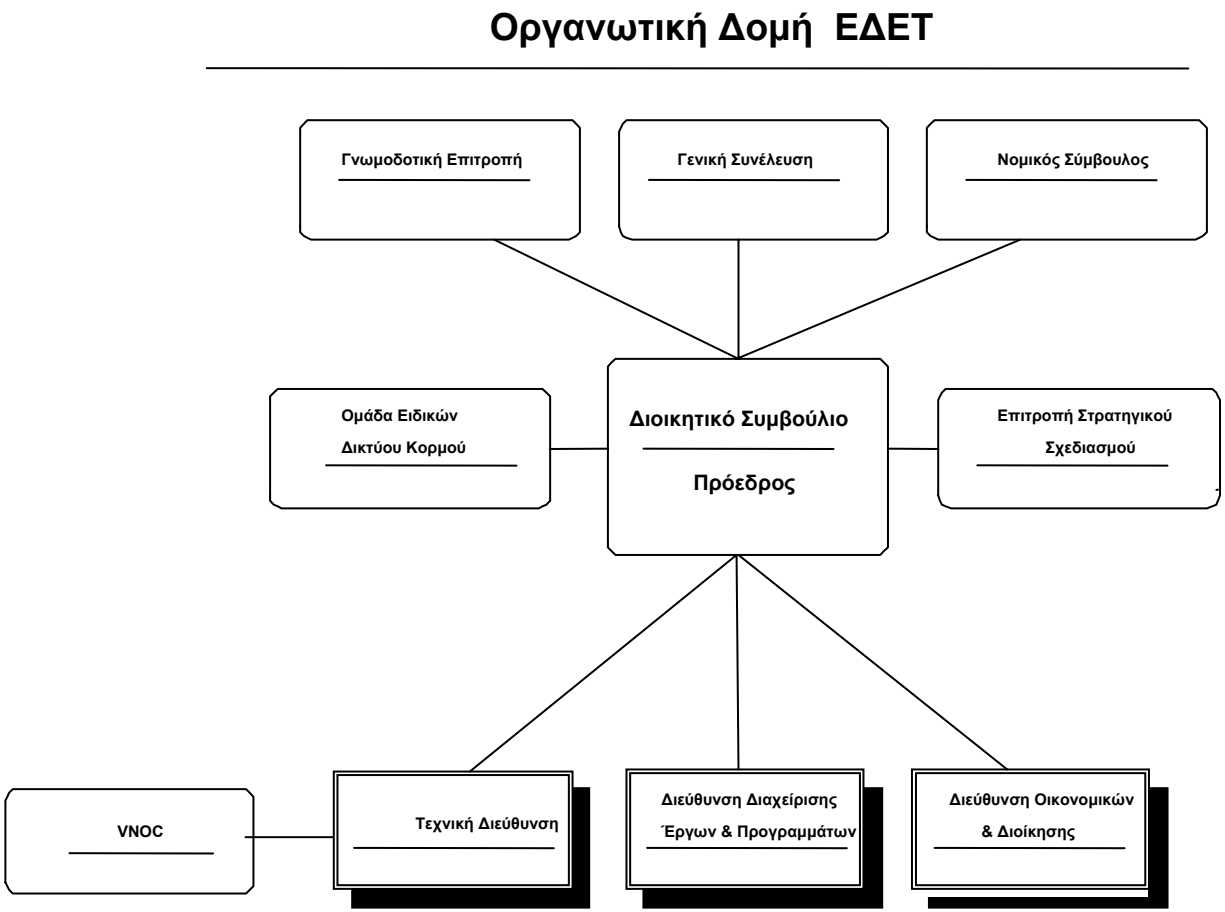
- Τι είναι τα NRENs:

  "Υψηλής ταχύτητας δίκτυα επικοινωνιών ευρείας κλίμακας που παρέχουν υψηλής ποιότητας επικοινωνίες και υπολογιστικές υπηρεσίες σε εθνικό επίπεδο στις Ερευνητικές και Εκπαιδευτικές κοινότητες"

# Τι είναι το ΕΔΕΤ

- Η εταιρεία - οι άνθρωποι
- Το δίκτυο
- Οι φορείς
- Οι υπηρεσίες

# Οργανόγραμμα του ΕΔΕΤ



# Το δίκτυο του ΕΔΕΤ


- Μισθωμένα κυκλώματα κορμού στα 2,5 Gbps
- Διασύνδεση με το ευρωπαϊκό δίκτυο Géant στα 10 Gbps
- Σύντομα θα διαθέτει «ιδιόκτητες» οπτικές ίνες (15ετής μίσθωση)

# Οι φορείς του ΕΔΕΤ

- ΑΕΙ, ΤΕΙ & Ερευνητικά Ιδρύματα
- Περισσότερα από 100 σημεία διασύνδεσης σε όλην την Ελλάδα
- Επιπρόσθετα: AIX, ΦDSL

# Οι υπηρεσίες του ΕΔΕΤ

- Βασικές υπηρεσίες: connectivity στο δίκτυο κορμού, mail, DNS, DWS, κλπ.
- Πρόσθετες υπηρεσίες και εθνικές υποδομές: Directory Services, VoIP, PKI, EduRoam, Grid
- Υπηρεσίες επόμενης γενιάς: VPNs, QoS, AAI, κ.ά.
- Εστιάζοντας στις υπηρεσίες AAI

# 2. Το πρόβλημα του ΑΑ - λύσεις

- Το πρόβλημα είναι η ελεγχόμενη πρόσβαση
  - [πιστοποίηση ταυτότητας χρήστη και βάσει αυτής] εκχώρηση άδειας πρόσβασης = Authentication/Authorization («ΑΑ»)
- Συμβατικές μέθοδοι ΑΑ
- Προβλήματα συμβατικών μεθόδων
- Τι ζητάμε από τις νέες μεθόδους ΑΑ
- Τι παρέχει μια «υποδομή ΑΑ» (AAI)
- Πώς δουλεύει μια υποδομή AAI

# Πρόβλημα: έλεγχος πρόσβασης

- Το πρόβλημα: η ελεγχόμενη πρόσβαση:
  - σε ψηφιακό υλικό, δημοσιεύσεις, κλπ. (σχετίζεται άμεσα με τις βιβλιοθήκες)
  - με ποιον τρόπο;
- Συμβατικές μέθοδοι:
  - με έλεγχο της διεύθυνσης IP του χρήστη
  - με username/password
  - με ψηφιακά πιστοποιητικά

# α. Βάσει διεύθυνσης IP (1/2)

- Ο πάροχος εξετάζει τη διεύθυνση του χρήστη και, αν η διεύθυνση βρίσκεται μέσα σε κάποιες περιοχές που έχουν δικαίωμα πρόσβασης (π.χ., διευθύνσεις ενός Πανεπιστημίου που έχει συνδρομή για το ζητούμενο αντικείμενο), ο SP δίνει στο χρήστη πρόσβαση στο ζητούμενο πόρο
- Πλεονεκτήματα:
  - απλότητα (ο χρήστης έχει εξαρχής πρόσβαση χωρίς να χρειαστεί να κάνει κάτι γι' αυτό)
  - ανωνυμία (ο πάροχος δε γνωρίζει το χρήστη)

# α. Βάσει διεύθυνσης IP (2/2)

- Μειονεκτήματα:
  - Εξαρτάται από την τοποθεσία του χρήστη και επεκτείνεται μόνο με VPNs (όπου παύει να είναι απλή μέθοδος και απαιτεί username/password)
  - Επειδή είναι ανώνυμη μέθοδος, είναι δύσκολο να αποδώσει διαφορετικά δικαιώματα σε διαφορετικά είδη χρηστών (π.χ., καθηγητές έναντι φοιτητών)
  - Λόγω ανωνυμίας, είναι μέθοδος ανεξέλεγκτη και επιδεκτική κατάχρησης (π.χ. με έναν proxy server)
  - Ενέχει δυσκολίες όταν αποκτώνται επιπλέον διευθύνσεις IP (βλ. ΦDSL) ή αλλάζουν οι παλιές

# β. Username/password (1/2)

- Ο πάροχος κάθε υπηρεσίας (π.χ., κάθε εκδοτικός οργανισμός) τηρεί μια χωριστή βάση ονομάτων και passwords. Ο χρήστης, για να προσπελάσει το περιεχόμενο, δίνει username και password
- Πλεονεκτήματα:
  - επιτρέπει τη διαφοροποίηση δικαιωμάτων μεταξύ χρηστών
  - επιτρέπει την κινητικότητα των χρηστών

# β. Username/password (2/2)

- Μειονεκτήματα:
  - ο χρήστης χρειάζεται ξεχωριστή εγγραφή σε κάθε πάροχο
  - σύντομα αυτό γίνεται αδύνατο να το διαχειριστεί και ο ίδιος ο χρήστης και ο οποιοσδήποτε τρίτος για λογαριασμό του (π.χ. αλλαγή password)
  - οι χρήστες τείνουν να χρησιμοποιούν τα ίδια usernames & passwords παντού, πράγμα που εισάγει προβλήματα ασφάλειας
  - δεν εξασφαλίζεται η ανωνυμία του χρήστη, με αποτέλεσμα κάθε πάροχος μπορεί να μαθαίνει δεδομένα (και συνήθειες) του κάθε χρήστη

# γ. Ψηφιακά πιστοποιητικά(1/2)

- Ο χρήστης αποκτά ένα ψηφιακό πιστοποιητικό, η πρόσβαση στο οποίο προστατεύεται (π.χ. με password).
- Ο χρήστης «εμφανίζει» το πιστοποιητικό του στον πάροχο για να αποκτήσει πρόσβαση στο περιεχόμενο.
- Πλεονεκτήματα:
  - όλα τα πλεονεκτήματα των μεθόδων username/ password και επιπλέον
  - δεν απαιτούνται πολλαπλές εγγραφές χρηστών (ούτε μια εγγραφή/χρήστη, ούτε μια/πάροχο)

# γ. Ψηφιακά πιστοποιητικά(2/2)

- Μειονεκτήματα:
  - παραμένει η μη ανωνυμία του χρήστη
  - η διαχείριση πιστοποιητικών είναι περίπλοκη και για τον ίδιο το χρήστη (tokens, κλπ.)
  - απαιτείται η συμφωνία υποδομής πιστοποίησης (PKI) που να είναι από κοινού αποδεκτή μεταξύ χρήστη, παρόχου περιεχομένου και ιδρύματος
  - απαιτείται μια σχετική ομοιομορφία στη δομή και τα δεδομένα των πιστοποιητικών, κάτι που είναι επίσης δύσκολο

# Τι ζητάμε από μια λύση; (1/2)

- Ευκολία στη διαχείριση:
  - ένας μοναδικός λογαριασμός χρήστη
  - εξασφάλιση δικαιωμάτων του χρήστη από το ίδρυμα χωρίς να απαιτείται παρέμβαση του ιδίου του χρήστη
- Ανωνυμία
  - ο χρήστης να αποκτά πρόσβαση βάσει των ιδιοτήτων του και όχι βάσει της ταυτότητάς του
  - ανωνυμία μεν, αλλά χωρίς δυνατότητα εύκολης κατάχρησης
- Διαφοροποίηση
  - τα δικαιώματα του χρήστη να μπορούν να διαφοροποιούνται ανάλογα με την ιδιότητά του (φοιτητής, καθηγητής, κλπ.)

# Τι ζητάμε από μια λύση; (2/2)

- Κινητικότητα
  - ο χρήστης να έχει τα ίδια δικαιώματα όπου και αν βρίσκεται, χωρίς να χρειάζεται να μεταφέρει υπολογιστές, κλειδιά, κλπ., ή να χρειάζεται VPN
- Ευρεία αποδοχή
  - λύση κατανοητή και υλοποιήσιμη από τα ιδρύματα
  - αποδεκτή και υποστηριζόμενη από τους παρόχους περιεχομένου
  - (άρα) με χρήση προτύπων και εργαλείων ευρείας αποδοχής
- Επιπλέον πλεονεκτήματα

# Υπάρχει σήμερα λύση; Ποια;

- Ναι (και μάλιστα περισσότερες από μία)
- Οι λύσεις αυτές είναι γνωστές ως συστήματα «Υποδομής Πιστοποίησης και Δικαιωμάτων Πρόσβασης» (Authentication – Authorization Infrastructure ή AAI)

# Τι παρέχει μια υποδομή ΑΑΙ;

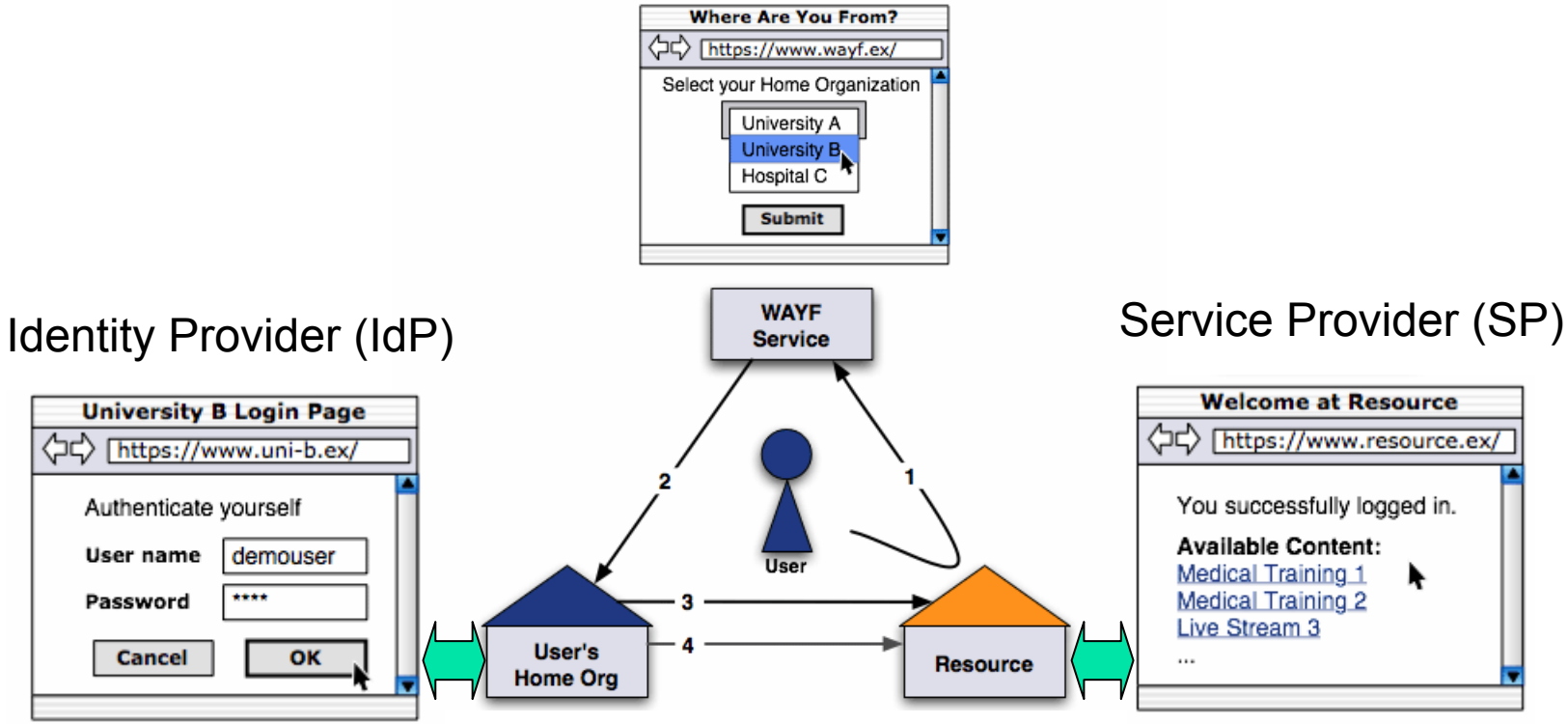
- Όλα τα «ζητούμενα από μια λύση ΑΑΙ»:
  - ένας μοναδικός λογαριασμός χρήστη: οι χρήστες γράφονται μόνο μία φορά, στο οικείο ίδρυμα
  - κινητικότητα: οι χρήστες μπορούν να έχουν πρόσβαση από παντού
  - ανωνυμία: οι πάροχοι δεν μαθαίνουν στοιχεία των χρηστών
  - διαφοροποίηση δικαιωμάτων: διαφορετικές κατηγορίες χρηστών μπορούν να έχουν διαφορετικά δικαιώματα
  - ευκολία: η απόδειξη ταυτότητας γίνεται μέσω web (user/password)
- Και επιπλέον:
  - συμμετρία: με την ίδια ακριβώς υποδομή, ένα ίδρυμα μπορεί να παράσχει υπηρεσίες και περιεχόμενο με την ίδια ευκολία που μπορεί να λάβει υπηρεσίες και περιεχόμενο από τρίτους

# Δημοφιλείς υποδομές ΑΑΙ

- Το σύστημα Shibboleth (Internet2), το οποίο είναι και το πρώτο ιστορικά σύστημα ΑΑΙ
  - (υποστηρίζεται από το ΕΔΕΤ)
- Άλλα συστήματα (A-SELECT, κλπ.)

# Πώς δουλεύει το Shibboleth

Κεντρικός server WAYF



# Πώς δουλεύει το Shibboleth (με λόγια)

1. Ο χρήστης επισκέπτεται τη σελίδα του παρόχου
2. Η σελίδα του παρόχου ανακατευθύνει το χρήστη στην κεντρική σελίδα της υποδομής (WAYF) στην οποία ο χρήστης επιλέγει τον φορέα όπου ανήκει
3. Η σελίδα WAYF ανακατευθύνει το χρήστη προς την σελίδα του ιδρύματός του, στην οποία ο χρήστης εισάγει τα στοιχεία του (username, password)
4. Αφού ο χρήστης δώσει σωστά τα στοιχεία του, ανακατευθύνεται αυτόματα στην αρχική σελίδα του παρόχου από όπου ξεκίνησε
5. Με ασφαλή τρόπο(*) οι ιδιότητες του χρήστη που επιθυμεί το ίδρυμα γνωστοποιούνται στον πάροχο

# Γιατί είναι «υποδομή»;

- Διότι δεν είναι απλώς μία υπηρεσία:
  - προβλέπει την ύπαρξη ενός κεντρικού WAYF server ώστε να διευκολύνεται η κλιμάκωση (π.χ. οι προσχωρήσεις νέων φορέων) χωρίς να απαιτούνται αλλαγές
  - περιλαμβάνει τεχνολογία διαχείρισης δικαιωμάτων (SAML)
  - απαιτεί σχέση εμπιστοσύνης μεταξύ των παρόχων περιεχομένου (Service Providers), του κεντρικού WAYF server, των επιμέρους servers στα ιδρύματα (Identity Providers) και των τελικών χρηστών
  - απαιτεί μια κοινά αποδεκτή υποδομή πιστοποίησης (PKI) μεταξύ όλων των παραπάνω
- Γι' αυτό: οργανώνεται βέλτιστα σε συσσωματώσεις ιδρυμάτων που μοιράζονται τα παραπάνω, και που ονομάζονται «ομοσπονδίες» (federations)

# 3. Πού είμαστε και πού πάμε

- Ποιοι γνωστοί πάροχοι περιεχομένου υποστηρίζουν ΑΑΙ;
- Ποιες ομοσπονδίες υπάρχουν διεθνώς;
- Πού βρίσκονται τα πράγματα στην Ελλάδα;
- Ποιος είναι ο ρόλος του ΕΔΕΤ;
- Ποια προσφορά αναμένεται από τα ιδρύματα (και τις βιβλιοθήκες τους);

# Υποστήριξη του Shibboleth

- Πάροχοι περιεχομένου
  - Science direct
  - Elsevier
  - EBSCO
  - X-libris
  - JSTOR
- Πλατφόρμες e-learning
  - Blackboard
  - WebCT
  - WebAssign
  - Moodle
  - Ilias
  - Eclass

(με άλλα λόγια, υπάρχει ήδη μια ευρύτατη γκάμα περιεχομένου που μπορεί να προσπελαστεί από τον οποιονδήποτε κοινό χρήστη μιας ομοσπονδίας Shibboleth)

# Ποιες ομοσπονδίες υπάρχουν;

- InCommon (Internet2 – ΗΠΑ)
- Switch-AAI (SWITCH – Ελβετία)
- HAKA (CSC – Φινλανδία)
- UK Access Management (Μ. Βρεττανία)
- MAMS (Αυστραλία)

  ...και πολλές ακόμα σε εξέλιξη σε διάφορες χώρες
- (παρατήρηση: οι ομοσπονδίες διαρθρώνονται σε εθνικό επίπεδο)

# Πού βρίσκεται η Ελλάδα;

- Το ΕΔΕΤ έχει αναπτύξει και διαθέτει σήμερα μια ομοσπονδία Shibboleth
  - Μέλη: ΑΠΘ, ΕΜΠ, ΠΠ, Γραφεία ΕΔΕΤ
  - Μπορούν να προσχωρήσουν άμεσα όσα ιδρύματα έχουν ΚΥ ΕΔΕΤ (ΠΚ, ΠΙ, ΠΘ, ΠΑ, ΔΠΘ, ΠΠελ., Χαροκόπειο, κ.ά.)
- Ο ρόλος του ΕΔΕΤ είναι (και θα είναι) να υποστηρίζει κεντρικά αυτήν την υποδομή χωρίς υποχρεωτικά να θέτει όρους διαχείρισης αυτής της υποδομής (βλ. π.χ. HARICA)

# Ο ρόλος των ιδρυμάτων (1/3)

- Στενή συνεργασία με φορείς-χρήστες της υπηρεσίας εντός ιδρύματος (βιβλιοθήκες, αλλά και άλλες εφαρμογές, διοίκηση, κλπ.)
- Προώθηση της σημερινής ομοσπονδίας, σε τυπικό (π.χ. MoU) και τεχνικό επίπεδο (νέα μέλη, υλοποιήσεις, δοκιμές, κλπ.)
- Ανάπτυξη τοπικών υποδομών στα ιδρύματα (π.χ., Directory Services ή ισοδύναμη υποδομή User Database – πρβλ. και με απαιτήσεις e-University)

# Ο ρόλος των ιδρυμάτων (2/3)

- Αίτημα απόκτησης ΚΥ από το NOC του ιδρύματος προς το ΕΔΕΤ
- Χρήση ΚΥ ΕΔΕΤ για σκοπούς prototyping:
  - Directory Services (περιλαμβάνεται στο ΚΥ)
  - Shibboleth IdP (περιλαμβάνεται στο ΚΥ)
  - Shibboleth SP (θα προστεθεί στο ΚΥ 4Q06)
- Σταδιακή «αντιγραφή» υπηρεσιών από το ΚΥ και ενσωμάτωσή τους στην πληροφοριακή υποδομή του ιδρύματος

# Ο ρόλος των ιδρυμάτων (3/3)

- Παροχή υπηρεσίας Shibboleth IdP σε καθεστώς παραγωγής
- Ανάπτυξη τεχνογνωσίας για την παροχή υπηρεσιών του ίδιου του ιδρύματος μέσω Shibboleth SP σε τρίτους
- Σταδιακή μετάβαση εσωτερικών υπηρεσιών του ιδρύματος που τώρα βασίζονται σε άλλους τρόπους ΑΑ προς το Shibboleth

# Ο ρόλος των βιβλιοθηκών (1/2)

- Εγκαθίδρυση «συνδέσμου» (liaison) μεταξύ αρμοδίων φορέων (βιβλιοθηκών κ.ά.) και ΕΔΕΤ (κυρίως για διαδικαστικά θέματα)
- Στενή συνεργασία με το NOC ιδρύματος για συντονισμό, διατύπωση απαιτήσεων, κλπ.
- Υποστήριξη διαδικαστικών θεμάτων (κατάρτιση – υπογραφή MoU, αποδοχή από τις διοικητικές αρχές του κάθε ιδρύματος)

# Ο ρόλος των βιβλιοθηκών (2/2)

- Χρήση υπηρεσιών Shibboleth SP (ΚΥ ή ιδρύματος) για παροχή υπηρεσιών και περιεχομένου σε τρίτους
- Διαχείριση συνδρομών με τους παρόχους περιεχομένου και καθορισμός πολιτικής διάθεσης στοιχείων των χρηστών σε αυτούς
- Ανάπτυξη εφαρμογών ενδιαφέροντός τους βάσει της υπάρχουσας υποδομής
  - ενδεικτικά, διάθεση περιεχομένου του ιδρύματος (διατριβές, reports, κλπ.) σε φοιτητές κλπ.

# 4. Συμπεράσματα (1/2)

- Οι υποδομές ΑΑΙ:
  - έχουν πολλά πλεονεκτήματα συγκρινόμενες με τις σημερινές διαδικασίες και μεθόδους
  - διευκολύνουν σημαντικά και τις δύο κατευθύνσεις ΑΑ (πρόσβαση σε περιεχόμενο τρίτων παρόχων, ελεγχόμενη διάθεση ιδίου περιεχομένου)
  - είναι ήδη εδώ, διαθέσιμες σε όλα τα ιδρύματα
- Τα ιδρύματα μπορούν:
  - να μπουν αρχικά στο ΑΑΙ κάνοντας χρήση των έτοιμων υπηρεσιών στα ΚΥ του ΕΔΕΤ
  - βαθμιαία να αναπτύξουν δικές τους υπηρεσίες

# Συμπεράσματα (2/2)

- Οι βιβλιοθήκες μπορούν:
  - να προσφέρουν νέες υπηρεσίες βάσει ιδιοτήτων κάθε χρήστη (καθηγητές, φοιτητές κλπ.)
  - να καθορίζουν την πολιτική διάθεσης πληροφοριών που αφορούν τους χρήστες κάθε ιδρύματος προς τρίτους παρόχους
  - να αναπτύξουν νέες υπηρεσίες διάθεσης ιδίου περιεχομένου προς τρίτους φορείς
  - να είναι οι φορείς συντονισμού και προώθησης της προσπάθειας ανάπτυξης του AAI στην Ελλάδα

# Ευχαριστούμε!

- Περισσότερες πληροφορίες:
  - Site Shibboleth ΕΔΕΤ (http://shibboleth.grnet.gr/)
  - Site ΕΔΕΤ (http://www.grnet.gr/)
  - Site VNOC (http://vnoc.grnet.gr/)
  - avarvit (at) grnet.gr
- Εφαρμογή RTS βάσει Shibboleth:
  - http://rts.grnet.gr/h323/users-shib/
- Ερωτήσεις; Demos;
- Κοινές ενέργειες;