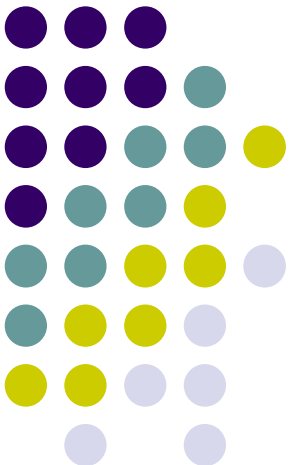
Υλοποίηση Δικτυακών Υποδομών και Υπηρεσιών: Εξυπηρετητής LDAP

Πανεπιστήμιο Πελοποννήσου
Τμήμα Επιστήμης & Τεχνολογίας Τηλεπικοινωνιών

Ευάγγελος Α. Κοσμάτος

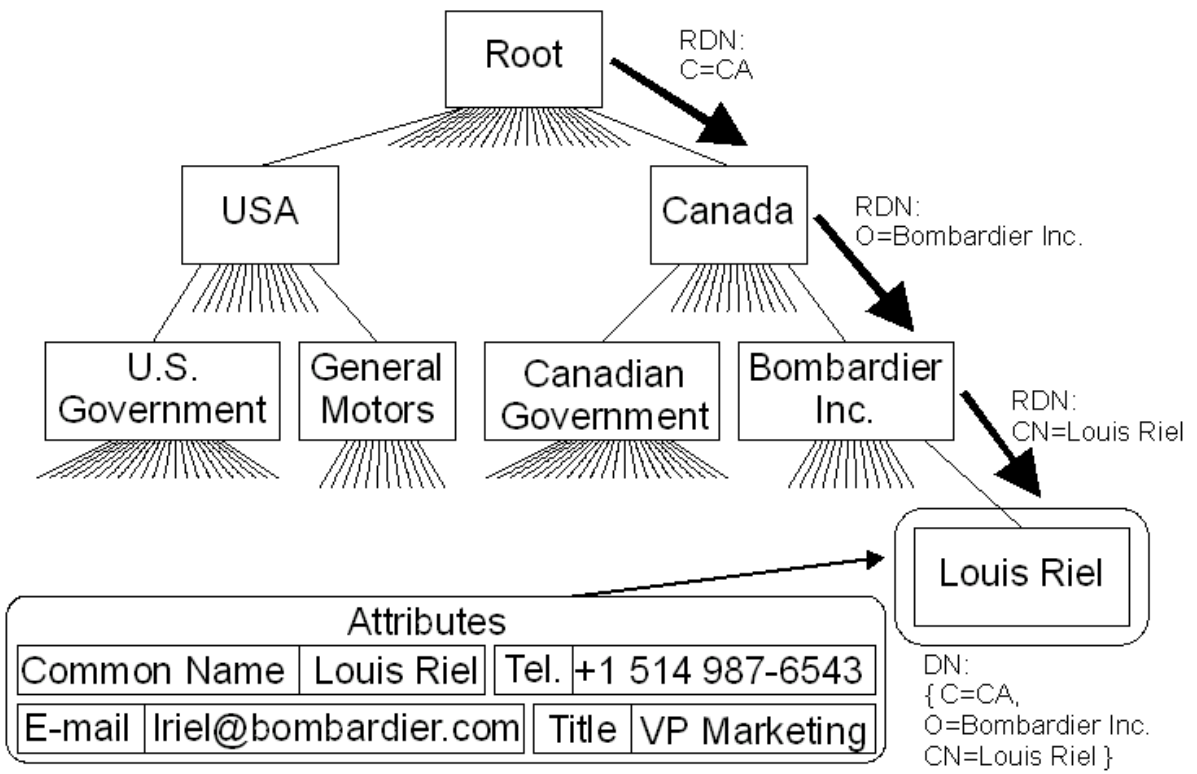


Ανάγκη για χρήση Καταλόγου

- Υπάρχει απαίτηση για on-line καταλόγους γιατί η χρησιμοποιούμενες μέθοδοι είναι ξεπερασμένες (κατάλογοι σε εκτυπώσεις)
- Αρχικά κάθε εφαρμογή χρησιμοποιούσε το δικό της κατάλογο με αποτέλεσμα να υπάρχουν προβλήματα συγχρονισμού
- Ο οργανισμός ITU δημιούργησε το πρότυπο X.500 για την δημιουργία καταλόγου.
- Το X.500 είναι βαρύ, δυσκίνητο και δεν υπάρχουν πολλά APIs

Πρότυπο X.500

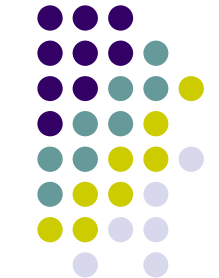
- Το πρότυπο X.500 της ITU



Πρότυπο X.500

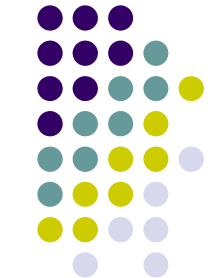
- Οργανώνει τα περιεχόμενα του κατάλογου σε ένα ιεραρχικό χώρο ονομάτων (namespace)
- Παρέχει δυνατότητα για πολύπλοκες αναζητήσεις
- Συχνά χρησιμοποιείται ως διεπαφή (interface) σε μη συμβατές υπηρεσίες καταλόγου
- Πολύ βαρύ για μικρά περιβάλλοντα

LDAP (1)



- Lightweight Directory Access Protocol
- Χρησιμοποιείται για την πρόσβαση και την ενημέρωση πληροφορίας σε καταλόγους οι οποίοι έχουν υλοποιηθεί στο X.500 μοντέλο
- Το πρότυπο ορίζει τα περιεχόμενα των μηνυμάτων ανάμεσα στους client και τους servers
- Παρέχει λειτουργίες για την εδραίωση και τον τερματισμό sessions σε ένα server

LDAP (2)

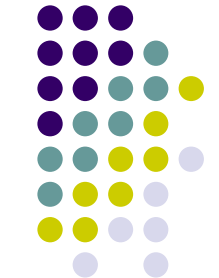


- Ο δημιουργός του LDAP Tim Howes στο University of Michigan δημιούργησε το LDAP ως ένα lightweight directory access protocol για την πρόσβαση σε X.500 καταλόγους.
- LDAP αναπτύχθηκε στην κοινότητα του Διαδικτύου παρέχοντας προτυποποίηση σε:
  - Μοντέλο Πληροφοριών - Information Model (πως η πληροφορία απεικονίζεται)
  - APIs (πως οι εφαρμογές βλέπουν την πληροφορία)
  - Replication (πως οι servers διαμοιράζονται πληροφορία)
  - Έλεγχο πρόσβασης Access Control (ποίος έχει πρόσβαση στην πληροφορία)

LDAP (3)

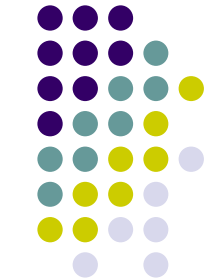
- Το LDAP είναι κατάλληλο για:
  - Πληροφορία στην οποία αναφέρονται πολλές οντότητες και εφαρμογές
  - Πληροφορία η οποία απαιτείται να προσπελαστεί από περισσότερες από μια τοποθεσίες
  - Πληροφορία η οποία διαβάζεται περισσότερες φορές από ότι γράφεται (δεν αλλάζει συχνά)
- Το LDAP δεν είναι κατάλληλο για:
  - Πληροφορία η οποία αλλάζει συχνά
  - Πληροφορία η οποία δεν είναι δομημένη

LDAP (4)



- Το LDAP μπορεί να χρησιμοποιηθεί για:
  - Ενοποιημένο sign on (ένα login/password για όλες τις εφαρμογές)
  - Single sign on (sign στο δίκτυο μια φορά και χρήση σε όλες
  - τις εφαρμογές -- απαιτεί PKI)
  - PKI certificate repository
  - Βιβλίο διευθύνσεων - Address Book (“White Pages Service”)
  - Organizational Chart (“Yellow Pages Service”)
  - Έλεγχος πρόσβασης και πιστοποίηση για εφαρμογές

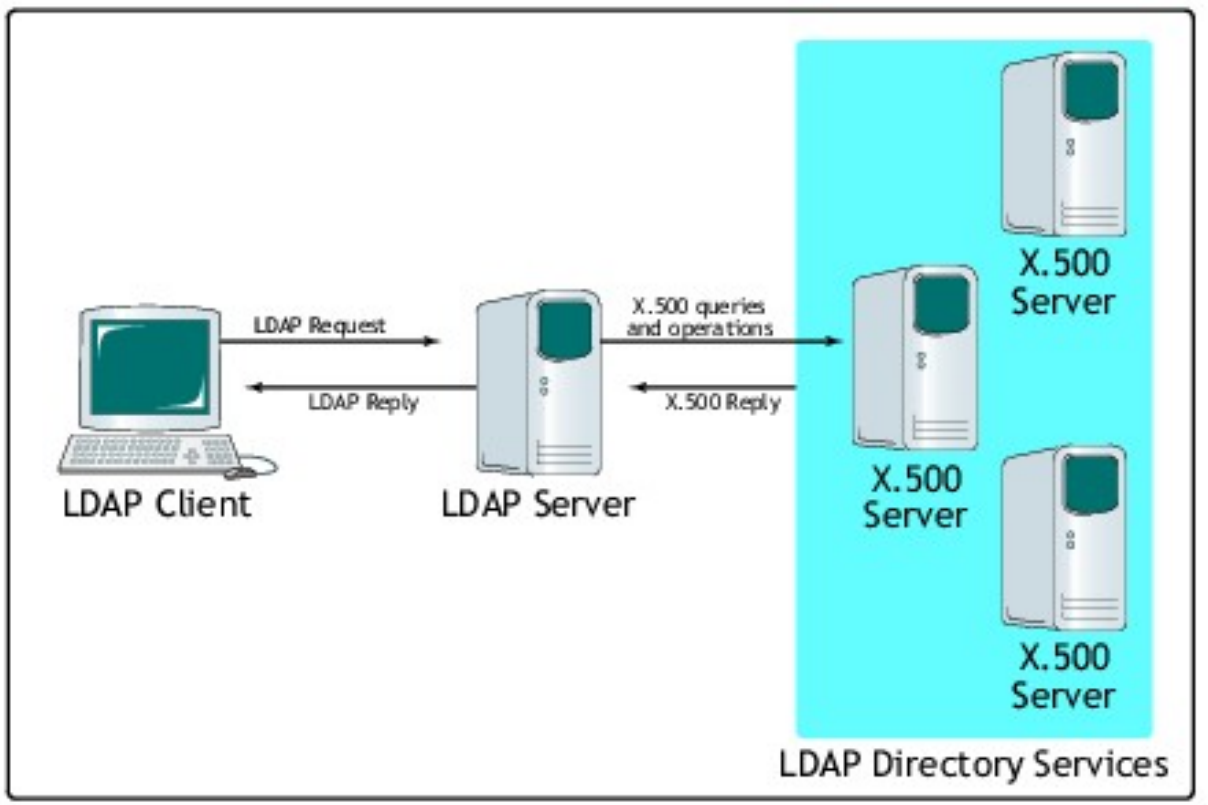
LDAP (5)



- Πληροφορία
  - Δομή της πληροφορίας η οποία αποθηκεύεται σε ένα LDAP κατάλογο
- Ονοματολογία
  - Πως η πληροφορία οργανώνεται και αναγνωρίζεται
- Λειτουργία
  - Περιγράφει τις λειτουργίες οι οποίες μπορούν να εκτελεστούν στην πληροφορία η οποία είναι αποθηκευμένη στον LDAP κατάλογο.
- Ασφάλεια
  - Περιγράφει πως η πληροφορία προστατεύεται από μη εξουσιοδοτημένη πρόσβαση.

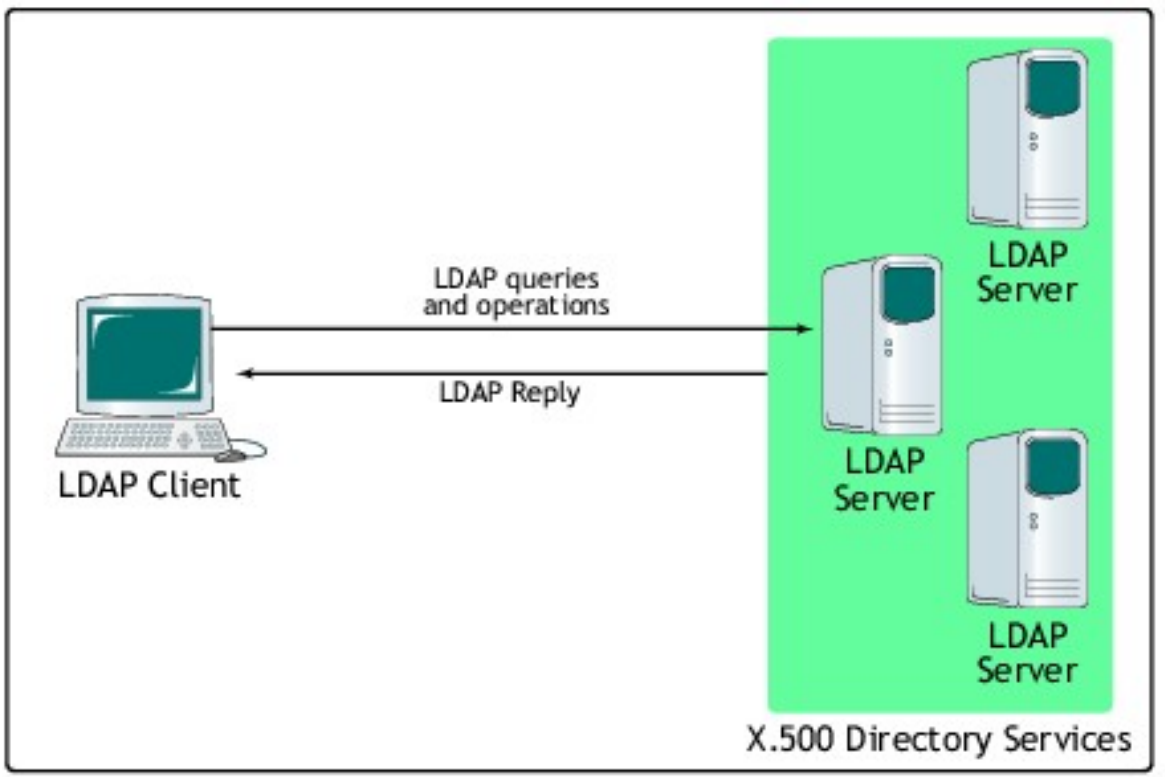
LDAP Server (1)

- LDAP Server λειτουργεί ως interface



LDAP Server (2)

- LDAP Server λειτουργεί ως stand-alone directory service



LDAP Server (3)

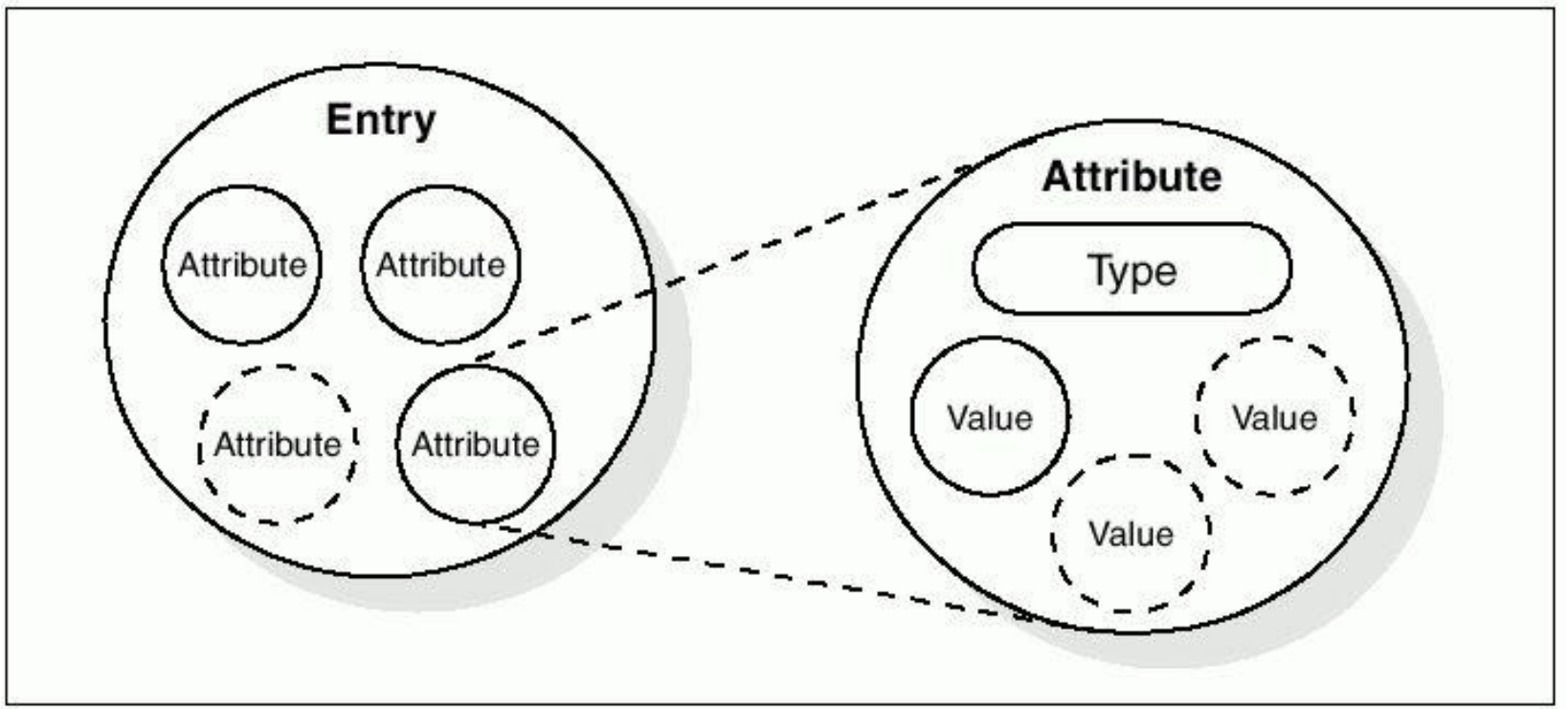
- Χρησιμοποιεί TCP/IP αντί για την OSI protocol stack
- Απλοποιεί συγκεκριμένες λειτουργίες και παραλείπει άλλες (σε σχέση με το X.500)
- Χρησιμοποιεί strings αντί για την ASN.1 notation για την απεικόνιση των δεδομένων.

```
struct employee {
char    name[32];
int     salary;
int     entryDate;
int     sex;
};
```

```
employee :: SEQUENCE {
Name          OCTET STRING, --32 characters
Salary        INTEGER,
EntryDate     INTEGER,
Sex           BOOLEAN
}
```

Κείμενο σε ASN.1

Αποθήκευση πληροφορίας στο LDAP



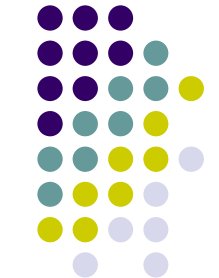
Αποθήκευση πληροφορίας στο LDAP (2)

- Κάθε attribute έχει ένα τύπο / σύνταξη και μια τιμή
- Μπορεί να οριστεί πως οι τιμές συμπεριφέρνονται κατά τις αναζητήσεις και τις άλλες λειτουργίες του καταλόγου
- Σύνταξη: bin, ces, cis, tel, dn etc.
- Όρια: ssn – μόνο ένα, jpeg φωτογραφία – 10K

Αποθήκευση πληροφορίας στο LDAP (3)

- Κάθε ‘entry’ περιγράφει ένα αντικείμενο (Class)
  - Άτομο, Server, Εκτυπωτής κλπ
- Παράδειγμα Entry:
  - InetOrgPerson(cn, sn, ObjectClass)
- Παράδειγμα Attributes:
  - cn (cis), sn (cis), telephoneNumber (tel), ou (cis), owner (dn), jpegPhoto (bin)

Σύνταξη των attributes



Syntax	Description
bin	Binary information
ces	Case exact string, also known as a *directory string*, case is significant during comparisons.
cis	Case ignore string. Case is not significant during comparisons.
tel	Telephone number. The numbers are treated as text, but all blanks and dashes are ignored.
dn	Distinguished name.
Generalized Time	Year, month, day, and time represented as a printable string.
Postal Address	Postal address with lines separated by "$" characters.

Συνηθισμένα attributes

Attribute, Alias	Syntax	Description	Example
commonName, cn	cis	Common name of an entry	John Smith
surname, sn	cis	Surname (last name) of a person	Smith
telephoneNumber	tel	Telephone number	512-838-6008
organizationalUnitName, ou	cis	name of organizational unit	Tivoli
owner	dn	DN of person that owns the entry	cn=John Smith,o=IBM,c=us
organization, o	cis	Name of organization	IBM
jpegPhoto	bin	Photographic image in JPEG format	Photograph of John Smith

Αντικείμενα και απαραίτητα attributes

Object class	Description	Required attributes
InetOrgPerson	Defines entries for a person	commonName (cn) surname (sn) objectClass
organizationalUnit	Defines entries for organizational units	ou objectClass
organization	Defines entries for organizations	o objectClass

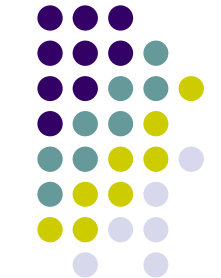
Ονοματολογία στο LDAP (1)

- Τα αντικείμενα σε ένα LDAP κατάλογο αναγνωρίζονται από τα ονόματα τους (distinguished name - DNs)
- Έχουν δύο τύπους:
  - String: (ορίζεται στο RFC2253): cn=Leslie Smith, ou=Austin, o=IBM
  - URL: ldap://<host>:<port>/<path>, όπου <path> έχει την μορφή <dn>[?<attributes>[?<scope>?<filter>]].
    - Όπου <dn> είναι ένα LDAP distinguished name το οποίο χρησιμοποιεί string.

Ονοματολογία στο LDAP (2)

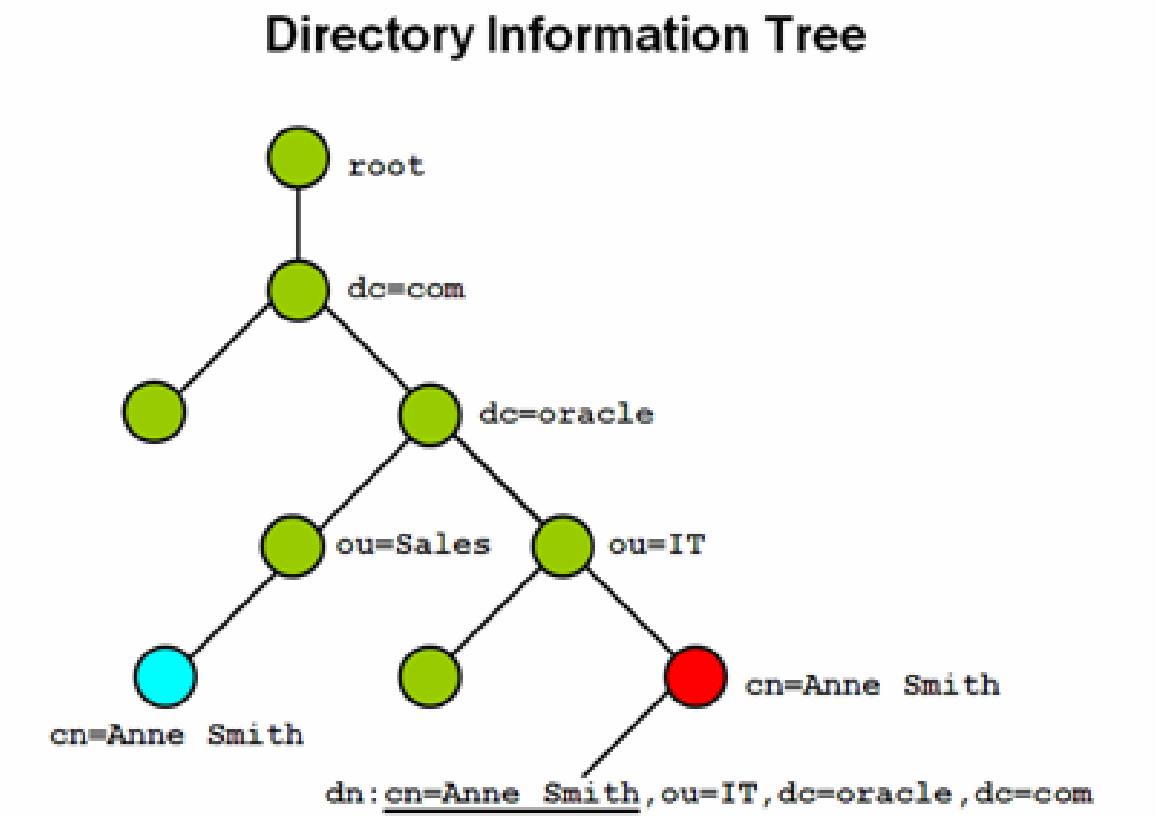
- Τα DNs αποτελούνται από αλληλουχία σχετικών DN
  - cn=John Smith,ou=Austin,o=IBM,c=US (Leaf 2 Root)
- Δέντρο πληροφοριών καταλόγου - Directory Information Tree (DIT)
- Ακολουθεί γεωγραφικά σχήματα ή σχήματα οργάνωσης

Ονοματολογία στο LDAP (3)



- Το LDAP σχήμα
  - Ορίζει ποια αντικείμενα επιτρέπονται
  - Που μπορούν να αποθηκευτούν
  - Τι attributes έχουν (objectClass)
  - Ποια attributes είναι προαιρετικά (objectClass)
  - Τύπος κάθε attribute (objectClass)
- Το LDAP σχήμα πρέπει να μπορεί να διαβαστεί από τον client

Directory Information Tree (DIT)



- Common attributes:
  - DC: Domain Component
  - OU: Organizational Unit
  - CN: Common Name
  - SN: Surname
    UID: Unique ID

Λειτουργίες LDAP

- Πιστοποίηση
  - BIND/UNBIND
  - ABANDON
- Αναζητήσεις
  - Αναζητήσεις
  - Σύγκριση entry
- Ενημέρωση
  - Προσθήκη entry
  - Διαγραφή entry (Μόνο nodes σε φύλλα, όχι aliases)
  - Ενημέρωση entry, Modify DN/RDN

Client - Server

- Ο Client εδραιώνει ένα session με τον server (BIND)
  - Hostname/IP και αριθμός port
  - Ασφάλεια
    - Πιστοποίηση βασισμένη σε User-id/password
  - Ανώνυμη σύνδεση με προκαθορισμένα δικαιώματα (Anonymous connection - default access rights
  - Κρυπτογράφηση επίσης υποστηρίζεται
- Ο Client εκτελεί λειτουργίες
  - Read/Update/Search
  - SELECT X,Y,Z FROM PART_OF_DIRECTORY
- Ο Client τερματίζει το session (UNBIND)
- Ο Client μπορεί να ABANDON το session

Bind / Unbind / Abandon

- BIND: Το αίτημα περιλαμβάνει την έκδοση του LDAP, το όνομα του client ο οποίος κάνει το αίτημα για BIND και η μέθοδος πιστοποίησης η οποία μπορεί να είναι:
  - Απλή (οι κωδικοί είναι καθαρό κείμενο, anonymous)
  - Kerberos v4 στο LDAP server (krbv42LDAP)
- Ο Server ανταποκρίνεται με ένα status indication
- UNBIND: Τερματίζεται το session
  - UnbindRequest ::= [APPLICATION 2] NULL
- ABANDON:
  - MessageID to abandon

Search / Compare

- Search: Το αίτημα περιλαμβάνει
  - baseObject: ένα LDAPDN
  - Scope: σε πόσα επίπεδα θα επεκταθεί η αναζήτηση
  - derefAliases: πως θα χειριστούν τα aliases
  - sizeLimit: μέγιστος αριθμός από entries τα οποία θα επιστραφούν
  - timeLimit: μέγιστος χρόνος για τον οποίο θα εκτελείται η αναζήτηση
  - attrsOnly: Επιστροφή μόνο τύπους attribute types ή και τις τιμές
  - Filter: Συνθήκες οι οποίες πρέπει να ικανοποιούνται κατά την αναζήτηση
  - Attributes: Λίστα με τα attributes τα οποία θα επιστραφούν
- Compare: παρόμοιο με το search αλλά επιστρέφει T/F

Add / Modify / Delete

- ADD request
  - Προσθήκη LDAPDN
  - Λίστα από Attributes και τιμές
- MODIFY request
  - Χρησιμοποιείται για να προσθέσει, διαγράψει και τροποποιήσει attributes
  - Το Request περιγράφει
    - Object: LDAPDN
    - Λίστα με τροποποιήσεις
      - Add, Delete, Replace
- DELETE request
  - Object: LDAPDN

Πρωτόκολλο LDAP (1)

- Μήνυμα LDAPMessage

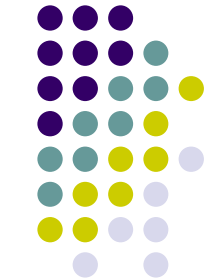
```
LDAPMessage ::=
    SEQUENCE {
         messageID       MessageID,
         protocolOp      CHOICE {
                              bindRequest          BindRequest,
                              bindResponse         BindResponse,
                              unbindRequest        UnbindRequest,
                              searchRequest        SearchRequest,
                              searchResponse       SearchResponse,
                              modifyRequest        ModifyRequest,
                              modifyResponse       ModifyResponse,
                              addRequest           AddRequest,
                              addResponse          AddResponse,
                              delRequest           DelRequest,
                              delResponse          DelResponse,
                              modifyRDNRequest     ModifyRDNRequest,
                              modifyRDNResponse    ModifyRDNResponse,
                              compareDNRequest     CompareRequest,
                              compareDNResponse    CompareResponse,
                              abandonRequest       AbandonRequest
                         }
    }

MessageID ::= INTEGER (0 .. maxInt)
```

Πρωτόκολλο LDAP (2)

- Μήνυμα LDAPResult

```
LDAPResult ::=
    SEQUENCE {
        resultCode      ENUMERATED {
                          success                      (0),
                          operationsError              (1),
                          protocolError                (2),
                          timeLimitExceeded            (3),
                          sizeLimitExceeded            (4),
                          compareFalse                 (5),
                          compareTrue                  (6),
                          authMethodNotSupported       (7),
                          strongAuthRequired           (8),
                          noSuchAttribute              (16),
                          undefinedAttributeType       (17),
                          inappropriateMatching        (18),
                          constraintViolation          (19),
                          attributeOrValueExists       (20),
                          invalidAttributeSyntax       (21),
                          noSuchObject                 (32),
                          aliasProblem                 (33),
                          invalidDNSyntax              (34),
                          isLeaf                       (35),
                          aliasDereferencingProblem    (36),
                          inappropriateAuthentication  (48),
                          invalidCredentials           (49),
                          insufficientAccessRights     (50),
                          busy                         (51),
                          unavailable                  (52),
                          unwillingToPerform           (53),
                          loopDetect                   (54),
                          namingViolation              (64),
                          objectClassViolation         (65),
                          notAllowedOnNonLeaf          (66),
                          notAllowedOnRDN              (67),
                          entryAlreadyExists           (68),
                          objectClassModsProhibited    (69),
                          other                        (80)
                        },
        matchedDN       LDAPDN,
        errorMessage    LDAPString
    }
```

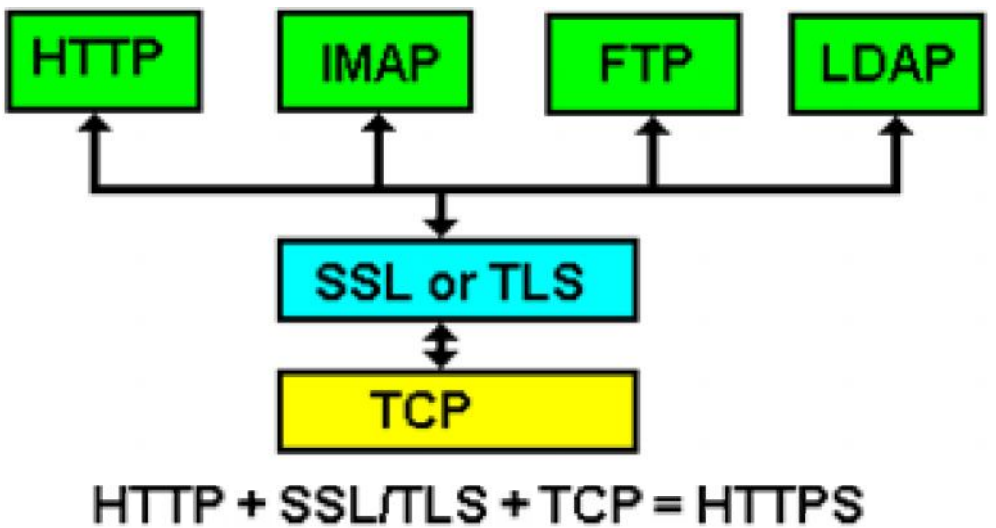
Ασφάλεια στο LDAP (1)



- Η ασφάλεια βασίζεται στο BIND μοντέλο
  - Καθαρό κείμενο στο ver 1
  - Kerberos στα ver 1,2,3(opt)
  - SASL στο ver 3
    - Simple Authentication and Security Layer
    - Χρησιμοποιεί μια από πολλές μεθόδους πιστοποίησης

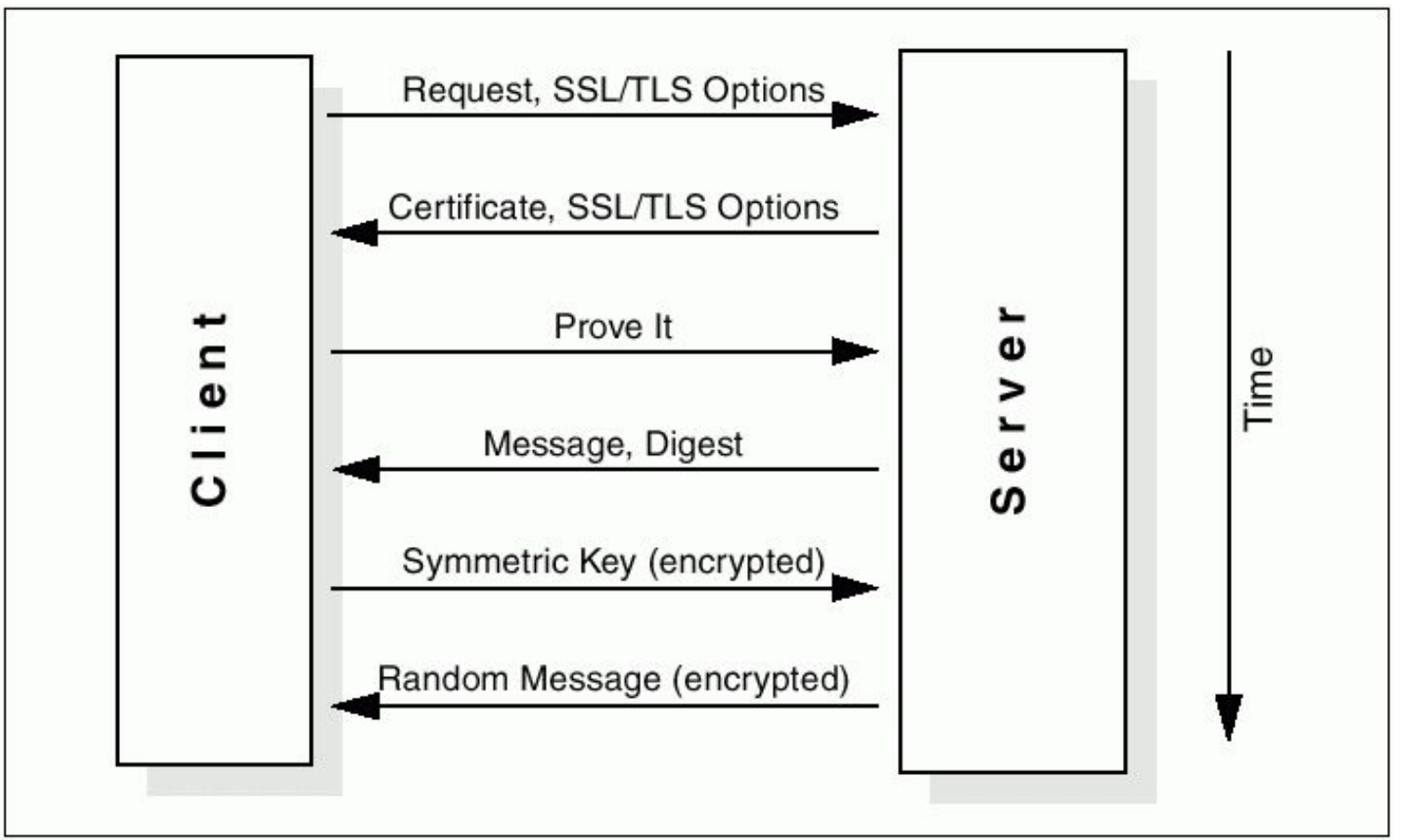
Ασφάλεια στο LDAP (2)

- Χρήση SASL το οποίο χρησιμοποιεί το SSL/TLS



Ασφάλεια στο LDAP (3)

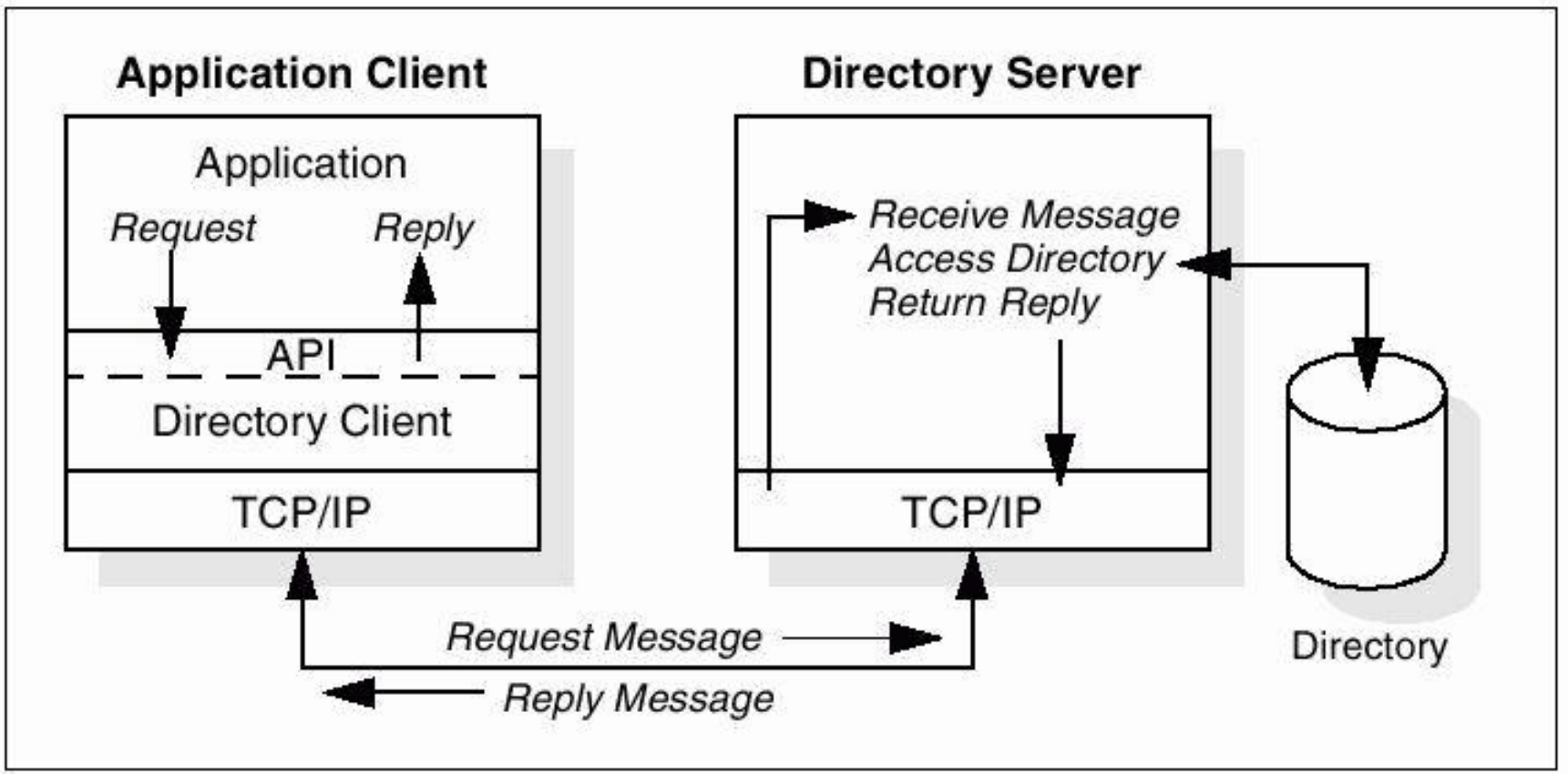
- SSL/TLS Handshake



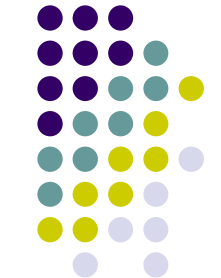
Το μοντέλο του πρωτοκόλλου

- Οι Clients εκτελούν λειτουργίες του πρωτοκόλλου σε servers
  - Οι Client στέλνουν request στον server
  - Ο Server επιτελεί λειτουργίες στον κατάλογο
  - Ο Server επιστρέφει το αποτέλεσμα ή μήνυμα λάθους
- Ασύγχρονη επικοινωνία με τον Server

Αλληλεπίδραση Client/Server



Υλοποιήσεις LDAP



- C Library API
  - LDAPv2 - RFC 1823 ‘The LDAP API’
  - LDAPv3 – In Internet Draft stage
- Java JNDI
- LDAP v3 χρησιμοποιεί UTF-8 encoding για το Unicode character set.
- HTTP to LDAP gateway
- LDAP to X.500 gateway