ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΕ ΥΠΟΛΟΓΙΣΤΙΚΑ ΠΛΕΓΜΑΤΑ

ΙΓΝΑΤΙΟΣ ΝΑΝΙΔΗΣ

ΤΕΙ ΚΡΗΤΗΣ
ΠΑΡΑΡΤΗΜΑ ΧΑΝΙΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ

ΠΡΟΛΟΓΟΣ – ΕΥΧΑΡΙΣΤΙΕΣ

Το θέμα της παρούσας πτυχιακής εργασίας είναι η υποδομή ασφάλειας σε υπολογιστικά πλέματα.

Στην παρούσα εργασία γίνεται μια εισαγωγή στο τι είναι το υπολογιστικό πλέγμα, το λεγόμενο Grid computing. Η δεύτερη ενότητα, αναφέρεται στην υποδομή ασφάλειας του πλέγματος και συγκεκριμένα σε χρήσιμους μηχανισμούς κρυπτογράφησης και καθορισμούς εννοιών που βοηθάνε στην κατανόηση των περαιτέρω κεφαλαίων. Στην τρίτη ενότητα αναφέρονται οι εικονικοί οργανισμοί και πως λειτουργεί το κομμάτι της κρυπτογράφησης με αναφορά στους μηχανισμούς κρυπτογραφίας που χρησιμοποιούνται. Στη τέταρτη ενότητα αναλύονται τα πρωτόκολλα και τα πιστοποιητικά που πρέπει να γνωρίζει και να έχει στην κατοχή του ένας πιστοποιημένος χρήστης του πλέγματος. Στη πέμπτη ενότητα γίνεται μια αναφορά για την υποδομή του HellasGrid, τι δυνατότητες έχει και τι μπορεί να προσφέρει στους χρήστες του πλέγματος. Στην έκτη και τελευταία ενότητα υπάρχει η βιβλιογραφία όπου φαίνονται όλες οι πηγές που αντλήθηκαν για την διαικπεραίωση της παρούσας εργασίας.

Οφείλω να ευχαριστήσω τον κ. Κορόσογλου Πασχάλη υπεύθυνο στο τμήμα υποστήριξης του HellasGrid για την πολύτιμη βοήθειά του. Επίσης θέλω να ευχαριστήσω τον καθηγητή μου κ. Μπαρμπουνάκη Ιωάννη για τις οδηγίες που μου έδωσε και την άριστη συνεργασία μας.

Περίληψη

Το υπολογιστικό πλέγμα είναι μια συλλογή γεωγραφικά κατανεμημένων πόρων που χρησιμοποιούνται σαν σύνολο για εκτέλεση εφαρμογών μεγάλης κλίμακας. Λειτουργεί σαν μία υπηρεσία για την διανομή της υπολογιστικής δύναμης και της ικανότητας αποθήκευσης δεδομένων μέσω του διαδικτύου. Η υποδομή ασφάλειας πλέγματος είναι αυτή που βοηθάει τους χρήστες να έχουν πρόσβαση στους πόρους με ασφάλεια. Για να είναι ένας χρήστης πιστοποιημένος στο πλέγμα θα πρέπει να έχει εγγραφεί σε έναν εικονικό οργανισμό και να κάνει αίτηση απόκτησης πιστοποιητικού σε μια πιστοποιούσα αρχή. Η αρχή αυτή εκδίδει ψηφιακά πιστοποιητικά και μαζί με αυτά ο χρήστης λαμβάνει και ένα ζευγάρι κλειδιών (δημόσιο & ιδιωτικό) που χρησιμοποιούνται για κρυπτογράφηση και αποκρυπτογράφηση αντίστοιχα. Υπάρχουν δύο είδη κρυπτογράφησης, η συμμετρική και η ασύμμετρη. Το σημείο πρόσβασης για την είσοδο στο περιβάλλον του πλέγματος είναι η διεπαφή χρήστη από την οποία με κατάλληλες εντολές ο χρήστης εκδίδει ένα πληρεξούσιο πιστοποιητικό. Υπάρχουν εργασίες στο πλέγμα όμως που χρειάζονται αρκετό χρόνο διεκπεραίωσης γι'αυτό υπάρχει και η επιλογή δημιουργίας μακροπρόθεσμου πιστοποιητικού το οποίο έχει πολύ περισσότερο χρόνο διάρκειας από ότι το απλό πληρεξούσιο.

Λέξεις κλειδιά: υπολογιστικό πλέγμα, διεπαφή χρήστη, εικονικός οργανισμός, ψηφιακή υπογραφή, μεσισμικό, κρυπτογραφία, αρχή πιστοποίησης, πληρεξούσιο.

Summary

Grid computing is a collection of geographically distributed resources that is used in a unified way for implementation of applications of large scale. It functions as a service for the distribution of computing power and the ability of data storage via the internet. Grid Security Infrastructure (GSI) helps the users have access to the resources with safety. In order for a user to be certified in Grid computing, he has to be registered in a Virtual Organization (VO) and send a certificate request to a Certificate Authority (CA) who issues digital certificates. Each user also receives a pair of keys (public and private) which are used for encryption and decryption respectively. There are two types of encryption, symmetric and asymmetric. The access point for the entry in the grid computing is the User Interface (UI) from which a user can issue a Proxy certificate with suitable proxy commands. Sometimes the jobs which are submitted by the users need more time to be completed than the lifetime of a proxy certificate. For that reason a user has to choose having a long-term proxy which has usually a longer lifetime than the proxy certificate.

Keywords: grid computing, user interface, virtual organization, digital signature, middleware, cryptography, certificate authority, proxy.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΑΚΡΩΝΥΜΙΩΝ

API: Application Programming Interface (προγραμματισμός εφαρμογών διεπαφής)
AUTH: Aristotle University of Thessaloniki (Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης (ΑΠΘ))
CA: Certificate Authority (πιστοποιούσα αρχή)
CASTOR: Cern Advanced STORage system (προηγμένο σύστημα αποθήκευσης του Cern)
CE: Computing Element (υπολογιστικό στοιχείο)
CERN: Conseil Europeen pour la Recherche Nucleaire (European Council for Nuclear Research) (κέντρο πυρηνικών μελετών και ερευνών)
CTI: Computer Technology Institute (Ινστιτούτο Τεχνολογίας Υπολογιστών (ITY))
CRL: Certificate Revocation List (κατάλογος ανάκλησης πιστοποιητικών)
CTL: Certificate Trust List (κατάλογος εμπιστευόμενων πιστοποιητικών)
DES: Data Encryption System (πρότυπο κρυπτογράφησης στοιχείων)
3-DES: Triple- Data Encryption System (τριπλό- πρότυπο κρυπτογράφησης στοιχείων)
DFS: Distributed File System (διανεμημένο σύστημα αρχείων)
DMS: Data Management System (υπηρεσία διαχείρησης δεδομένων)
EGEE: Enabling Grids for E-sciencE
FORTH: Foundation for Research and Technology Hellas **(**Ιδρυμα Τεχνολογίας και Έρευνας (ITE)**)**
FTP: File Transfer Protocol (πρωτόκολλο μεταφοράς αρχείων)
FTP: Functionality Trusted Parties (λειτουργικά εμπιστευόμενο πρόσωπο)
GPFS: General Parallel File System (γενικό παράλληλο σύστημα αρχείων)
GSI: Grid Security Infrastructure (υποδομή ασφάλειας πλέγματος)
HPSS: High Performance Storage System (σύστημα αποθήκευσης υψηλης επίδοσης)
IASA: Institute of Accelerating Systems and Applications (Ινστιτούτο Επιταχυντικών Συστημάτων και Εφαρμογών (ΙΕΣΕ))
IETF: Internet Engineering Task Force (Ομάδα εργασίας μηχανικών διαδικτύου)
IS: Information Service (υπηρεσία πληροφοριών)
LHC: Large Hadron Collider (επιταχυντής που κατασκευάζεται στο Cern)
LCG: LHC Computing Grid (αποτελεί έργο του CERN και είναι συλλογή από γεωγραφικά κατανεμημένους πόρους)
MAC: Message Authentication Codes (κώδικες επικύρωσης μηνυμάτων)
NERSC: National Energy Research Scientific Computing Center (εθνικό επιστημονικό υπολογιστικό κέντρο αναζήτησης ενεργειακών πόρων)
NES: Network Enable Services (δίκτυο επιτρεπτών υπηρεσιών)

NFS: Network File System (σύστημα αρχείων δικτύων)
OCSP: Online Certificate Status Protocols (απευθείας σύνδεση σε πρωτόκολλα κατάστασης πιστοποιητικών)
PKI: Public Key Infrastructure (υποδομή δημόσιου κλειδιού)
RA: Registration Authority (αρχή εγγραφής)
RFT: Reliable File Transfer (αξιόπιστη μεταφορά αρχείων)
ROC: Regionals Operation Center (περιφερειακό κέντρο διαδικασιών)
SEE: South Eastern Europe (*εικονικός οργανισμός* νοτιοανατολικής Ευρώπης)
SE: Storage Element (στοιχείο αποθήκευσης)
SDK: Software Development Kit (πακέτο ανάπτυξης λογισμικού)
SSL: Secure Sockets Layer (ασφάλεια στρώματος υποδοχής)
TCP: Transmission Control Protocol (πρωτόκολλου ελέγχου μετάδοσης)
TCP: Trusted Third Parties (εμπιστευόμενα τρίτα πρόσωπα)
UI: User Interface (διεπαφή χρήστη)
UTP: Unconditionally Trusted Parties (άνευ όρων εμπιστευόμενο πρόσωπο)
VO: Virtual Organization (εικονικός οργανισμός)
VOMS: Virtual Organization Membership Service (υπηρεσία μελών των εικονικών οργανισμών)
VOMS: Virtual Organization Management Service (διαχείριση
WMS: Workload Management System (υπηρεσία διαχείρησης φόρτου εργασίας)

1. Εισαγωγή

1.1 Τι είναι το Grid computing

Το Grid computing (υπολογιστικό πλέγμα) είναι ένας νέος κλάδος στον τομέα της πληροφορικής και των υπολογιστών ο οποίος βρίσκεται υπό συνεχή εξέλιξη τα τελευταία 10-15 χρόνια. Είναι μια συλλογή γεωγραφικά κατανεμημένων πόρων που χρησιμοποιούνται σαν σύνολο για εκτέλεση εφαρμογών μεγάλης κλίμακας.

Μπορεί να θεωρηθεί σαν μια υπηρεσία στην οποία οι χρήστες μοιράζονται την υπολογιστική ισχύ και την ικανότητα αποθήκευσης δεδομένων μέσω του διαδικτύου και αποτελεί νέα εξέλιξη των κατανεμημένων συστημάτων. Ουσιαστικά είναι μία μορφή δικτύου η οποία ενεργεί σαν ένας μεγάλος και ισχυρός εικονικός υπολογιστής αποτελούμενος από μία ομάδα διαδικτυακών υπολογιστών, γεωγραφικά κατανεμημένων και συνδεδεμένων μεταξύ τους. Επίσης ενεργούν σαν σύνολο για την επίτευξη των στόχων οι οποίοι είναι η κοινή εκμετάλλευση των πόρων και η συντονισμένη επίλυση των προβλημάτων στους πολύ-θεσμικούς εικονικούς οργανισμούς (virtual organizations).Το grid δίνει την δυνατότητα σε αυτές τις ομάδες χρηστών (virtual organizations) να μοιράζονται τους πόρους και να επιδιώκουν κοινούς στόχους.

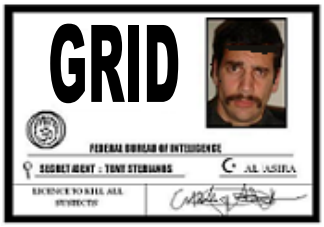
Οι τεχνολογίες, το λογισμικό, το υλικό, τα δίκτυα, οι εφαρμογές αποτελούν αυτό που λέμε πλέγμα το οποίο επιτρέπει στους χρήστες να έχουν πρόσβαση και κυρίως χρήση στους γεωγραφικά κατανεμημένους πόρους. Όταν ξεκίνησε η ευρεία χρήση του παγκόσμιου ιστού (world wide web) εκεί είχαμε πρόσβαση μόνο σε δεδομένα. Με το Grid ερχόμαστε ένα βήμα παραπέρα κάνοντας χρήση πόρων οι οποίοι είναι διασκορπισμένοι.

Το υπολογιστικό πλέγμα δεν είναι απλά μια υποδομή λογισμικού (software) και υλικού (hardware). Στηρίζεται περισσότερο σε ένα πιο προηγμένο λογισμικό που ονομάζεται μεσισμικό (middleware) το οποίο διασυνδέει πόρους κι εφαρμογές παρέχοντας στους χρήστες αξιόπιστη, συνεπή, διεισδυτική και φτηνή πρόσβαση στις υψηλές ικανότητες του πλέγματος. Δεν είναι απλά όμως μια υπηρεσία που συλλέγει υπολογιστικούς πόρους, αλλά σκοπός της είναι η δημιουργία ενός απέραντου ενιαίου υπολογιστικού πόρου αποτελούμενο από ένα δίκτυο υπολογιστών παγκόσμιας κλίμακας.

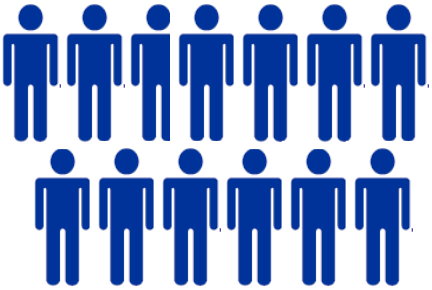
Μια γενικότερη εικόνα για το υπολογιστικό πλέγμα φαίνεται παρακάτω:

Ένας Η/Υ με εγκατεστημένο το λειτουργικό Linux.

Μία ταυτότητα.



Μία ομάδα ατόμων (εικονικός οργανισμός) που διαθέτει πόρους στους οποίους ένας πιστοποιημένος χρήστης του πλέγματος μπορεί να έχει πρόσβαση.

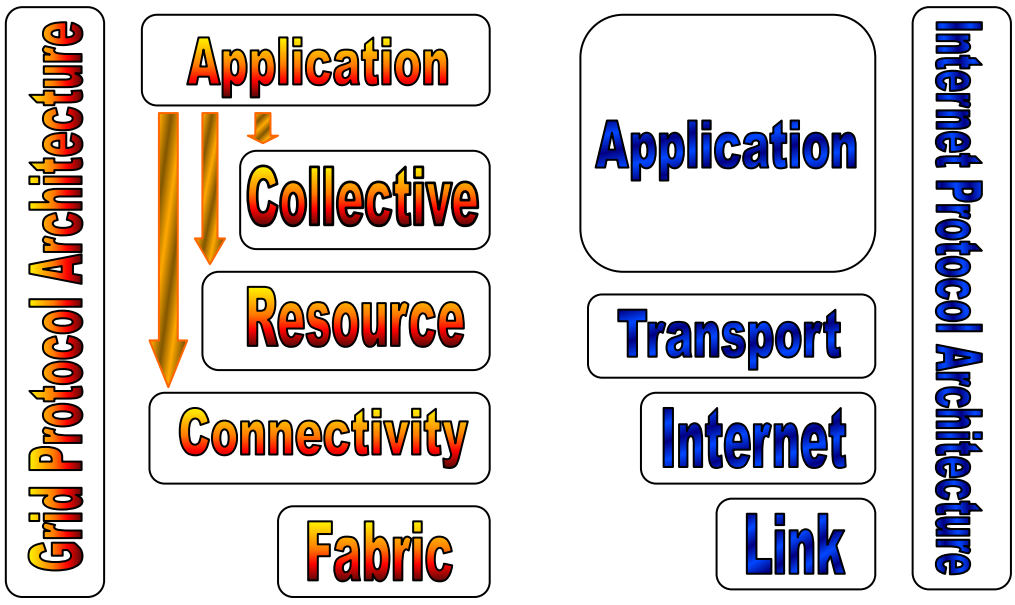


Εικόνα 1:Βασικά στοιχεία του Grid

Σ’αυτή την ενότητα περιγράφεται η αρχιτεκτονική του πλέγματος χρησιμοποιώντας κάποια στρώματα για καλύτερη κατανόηση. Τα στρώματα τα οποία αναφέρονται και αποτελούν την αρχιτεκτονική:

- το στρώμα δομής (fabric layer)
- το στρώμα συνδετικότητας (connectivity layer)
- το στρώμα πόρων (resource layer)
- το συλλογικό στρώμα (collective layer)

Τα πρωτόκολλα των πόρων και της συνδετικότητας διευκολύνουν τη διανομή των μεμονωμένων πόρων. Τα πρωτόκολλα σε αυτά τα στρώματα σχεδιάζονται έτσι ώστε να μπορούν να εφαρμοστούν πάνω από μια διαφορετική σειρά των τύπων των πόρων, που καθορίζονται στο στρώμα δομής τα οποία μπορούν στη συνέχεια να χρησιμοποιηθούν για να κατασκευάσουν ένα ευρύ φάσμα παγκόσμιων υπηρεσιών, εφαρμογών και συγκεκριμένων συμπεριφορών από το συλλογικό στρώμα.



Εικόνα 2:Τα στρώματα αρχιτεκτονικής πρωτοκόλλου πλέγματος και η σχέση τους με την αρχιτεκτονική πρωτοκόλλου διαδικτύου.

1.1.1Fabric layer (στρώμα δομής)

Το στρώμα δομής παρέχει στο δίκτυο του πλέγματος τους πόρους στους οποίους ένας πιστοποιημένος χρήστης έχει πρόσβαση. Ένας πόρος μπορεί να είναι μια λογική οντότητα όπως ένα διανεμημένο σύστημα αρχείων, μια συστοιχία υπολογιστών κ.τ.λ. Οι πόροι θα πρέπει να εφαρμόσουν κάποιους μηχανισμούς έρευνας που επιτρέπουν την ανακάλυψη της δομής, της κατάστασης και των ικανοτήτων τους αλλά και κάποιους μηχανισμούς διαχείρισης των πόρων που παρέχουν έναν έλεγχο για την ποιότητα της εξυπηρέτησης. Παρακάτω γίνεται διάκριση των πόρων ανάλογα με το τι προσφέρουν στο υπολογιστικό πλέγμα.

Υπολογιστικοί πόροι: υπάρχουν μηχανισμοί οι οποίοι απαιτούνται για εκκίνηση προγραμμάτων, παρακολούθηση και έλεγχο των διαδικασιών που προκύπτουν. Επίσης μηχανισμοί που επιτρέπουν τον έλεγχο των πόρων, λειτουργίες έρευνας για τον καθορισμό χαρακτηριστικών του υλικού και του λογισμικού καθώς επίσης και πληροφορίες για την κατάστασή τους. Υπάρχουν τρεις τρόποι χρησιμοποίησης και εκμετάλλευσης των υπολογιστικών πόρων με τις κατάλληλες εκτελέσεις εφαρμογών όπως φαίνεται παρακάτω:

- Εκτέλεση μιας εφαρμογής σε ένα σύστημα του Grid αντί σ ένα μηχάνημα ενός τοπικού χρήστη.
- Εκτέλεση μιας εφαρμογής έτσι ώστε να χωρίζεται το έργο της σε τμήματα τα οποία μπορούν να εκτελεστούν παράλληλα σε διάφορα συστήματα/επεξεργαστές του πλέγματος .
- Η ανάγκη μιας εφαρμογής να εκτελεστεί πολλές φορές και σε πολλά διαφορετικά συστήματα.

Πόροι αποθήκευσης: εδώ βρίσκονται μηχανισμοί για να δέχονται και να αποθηκεύουν αρχεία καθώς και μηχανισμοί γραφής, ανάγνωσης αρχείων και διοίκησης που επιτρέπουν έλεγχο πόρων που διατίθενται για τις μεταφορές αρχείων.

Επίσης υπάρχουν και εδώ λειτουργίες έρευνας όπως και στους υπολογιστικούς πόρους. Ένα σύστημα στο πλέγμα παρέχει μία χωρητικότητα αποθηκευτικού χώρου για διαμοιρασμό και χρήση. Όταν το δίκτυο του πλέγματος παρουσιάζεται σαν μια υπηρεσία αποθηκευτικού χώρου αναφέρεται σαν data Grid (πλέγμα δεδομένων). Ο αποθηκευτικός χώρος μπορεί να είναι μνήμη σε έναν επεξεργαστή ενός Η/Υ ή πιο μόνιμος όπως σκληροί δίσκοι, ταινίες κ.τ.λ. Τέτοιου είδους μόνιμοι αποθηκευτικοί χώροι μπορούν να χρησιμοποιηθούν για αύξηση απόδοσης, χωρητικότητας και αξιοπιστίας δεδομένων.

Κάποια συστήματα αρχείων προσφέρουν επίσης ένα χώρο για αποθήκευση των ονομάτων των αρχείων. Κάτι τέτοιο διευκολύνει τους χρήστες οι οποίοι μπορούν να αναφέρονται και να αναζητάνε τα δεδομένα με την ονομασία τους χωρίς να ξέρουν την ακριβή τοποθεσία αυτών.

Πόροι δικτύων: σε αυτούς τους πόρους υπάρχουν μηχανισμοί για έλεγχο των πόρων που διατίθενται για την μεταφορά δικτύου όπως επίσης και λειτουργίες έρευνας για χαρακτηριστικά του δικτύου και του φορτίου.

Αποθηκευτικοί χώροι κώδικα προγραμμάτων: οι αποθηκευτικοί χώροι κώδικα προγραμμάτων είναι μέρος των πόρων του πλέγματος που αποθηκεύουν τους εκτελέσιμους κώδικες έτσι ώστε να τους παρέχουν αργότερα κατά απαίτηση. Οι αποθηκευτικοί αυτοί χώροι παράσχουν υπηρεσίες για την ανάκτηση θέσης αντιγράφου, το αίτημα κώδικα και τη μετάδοση κώδικα. Για έναν ορισμένο απαραίτητο κώδικα, θα υπάρξουν πολλαπλάσιες αποθήκες κώδικα διαθέσιμες

που αντιπροσωπεύονται σαν ένα σύνολο. Αυτή η εξειδικευμένη μορφή πόρων απαιτεί μηχανισμούς διοίκησης των αντικειμένων.

Κατάλογοι: εδώ απαιτούνται μηχανισμοί εφαρμογής διαδικασιών για αναπροσαρμογή και ερωτήσεις καταλόγου π.χ. μια σχεσιακή βάση δεδομένων.

1.1.2Connectivity layer (στρώμα συνδετικότητας)

Το στρώμα συνδετικότητας καθορίζει τα πρωτόκολλα επικοινωνίας και επικύρωσης που απαιτούνται για τις δικτυακές συναλλαγές στο περιβάλλον του πλέγματος.

Τα πρωτόκολλα επικοινωνίας επιτρέπουν την ανταλλαγή δεδομένων μεταξύ των πόρων ενώ τα πρωτόκολλα επικύρωσης στηρίζονται στις υπηρεσίες επικοινωνίας για να παρέχουν ασφαλείς μηχανισμούς κρυπτογράφησης για την ταυτότητα των χρηστών και των πόρων. Να σημειωθεί ότι τα πρότυπα ασφαλείας που αναπτύσσονται στα πρωτόκολλα του διαδικτύου, ισχύουν και για το υπολογιστικό πλέγμα.

Αυτό-εγγραφή (Single sign on): ο χρήστης πρέπει να είναι σε θέση να συνδέεται μια φορά στο πλέμα και να έχει πρόσβαση στους πολλαπλούς πόρους χωρίς την περαιτέρω επέμβασή του (υποβολή στοιχείων ξανά και ξανά).

Αντιπροσώπευση (Delegation): με αυτή την υπηρεσία ένας χρήστης έχει την δυνατότητα εξουσιοδότησης ενός προγράμματος το οποίο θα τρέχει για λογαριασμό του χρήστη έτσι ώστε το πρόγραμμα αυτό να έχει πρόσβαση στους πόρους στους οποίους ο χρήστης εξουσιοδοτείται. Προαιρετικά και υπό όρους

το πρόγραμμα αυτό μπορεί να εξουσιοδοτήσει ένα υποσύνολο των δικαιωμάτων του σε ένα άλλο πρόγραμμα για τον ίδιο σκοπό.

Ολοκλήρωση με διάφορες λύσεις τοπικής ασφάλειας: κάθε πόρος θα πρέπει να υιοθετήσει οποιαδήποτε λύση από τοπικές ασφάλειες (όπως π.χ. Kerberos και Unix ασφάλειες). Έτσι οι λύσεις ασφαλείας του grid θα πρέπει να είναι σε θέση να επικοινωνήσουν με αυτές τις διάφορες τοπικές λύσεις χωρίς την απαίτηση της ολικής αντικατάστασης των τοπικών λύσεων ασφαλείας. Απλά θα πρέπει να επιτρέπεται η αντιστοίχιση στο τοπικό περιβάλλον.

Σχέσεις εμπιστοσύνης μεταξύ χρηστών: όταν ένας χρήστης χρησιμοποιεί πολλαπλούς πόρους ταυτόχρονα, το σύστημα ασφαλείας δεν πρέπει να απαιτεί από τους πόρους να αλληλεπιδρούν μεταξύ τους για την διαμόρφωση του περιβάλλοντος ασφάλειας.

1.1.3Resource layer (στρώμα των πόρων)

Το στρώμα των πόρων στηρίζεται στα πρωτόκολλα επικοινωνίας και επικύρωσης του στρώματος συνδετικότητας για να καθορίσει τις διεπαφές (APIs και SDKs) για την ασφαλή διαπραγμάτευση, παρακολούθηση και έλεγχο στους μεμονωμένους πόρους. Οι εφαρμογές του στρώματος των πόρων καλούν λειτουργίες από το στρώμα δομής για πρόσβαση και έλεγχο σε τοπικούς πόρους, όμως αγνοούν άλλα ζητήματα και ενέργειες διότι ενδιαφέρονται εξ'ολοκλήρου για μεμονωμένους πόρους.
Δύο αρχικές κατηγορίες πρωτοκόλλων του στρώματος πόρων είναι οι παρακάτω:

Πρωτόκολλα πληροφοριών: τα πρωτόκολλα αυτά χρησιμοποιούνται για να λάβουν πληροφορίες για την δομή και την κατάσταση ενός πόρου όπως είναι η διαμόρφωση, το τρέχον φορτίο και η πολιτική χρήσης.

Πρωτόκολλα διαχείρισης: αυτά χρησιμοποιούνται για την διαπραγμάτευση πρόσβασης σε έναν κοινό πόρο καθορίζοντας για παράδειγμα τις απαιτήσεις των πόρων και την λειτουργία που εκτελείται, όπως τη δημιουργία διαδικασίας ή τη πρόσβαση στοιχείων. Ένα πρωτόκολλο μπορεί επίσης να παρακολουθεί την κατάσταση μιας λειτουργίας και να την ελέγχει, όπως π.χ. τερματισμός της λειτουργίας.

1.1.4Collective layer (συλλογικό στρώμα)

Το συλλογικό αυτό στρώμα περιέχει πρωτόκολλα και υπηρεσίες που δεν σχετίζονται με έναν συγκεκριμένο πόρο αλλά με μία συλλογή πόρων. Για αυτό τον λόγο καλείται και συλλογικό αυτό το στρώμα. Προσφέρει μια ευρεία ποικιλία διανομής υπηρεσιών χωρίς απαιτήσεις στον πόρο που μοιράζεται για τον λόγο ότι τα συστατικά του στηρίζονται τόσο στο στρώμα πόρων αλλά και στο στρώμα συνδετικότητας . Παραδείγματα:

Υπηρεσίες καταλόγου: επιτρέπουν στους χρήστες των εικονικών οργανισμών να ανακαλύψουν την ύπαρξη ιδιοτήτων των πόρων. Οι χρήστες μπορούν να ζητήσουν τους πόρους κατά όνομα ή με τις ιδιότητες τους όπως τύπος, διαθεσιμότητα ή φορτίο.

Ανακατανομή, χρονοπρογραμματισμός και υπηρεσίες μεσιτείας επιτρέπουν στους χρήστες των VO να ζητήσουν κατανομή ενός ή πολλών πόρων για ένα

συγκεκριμένο σκοπό και να προγραμματίσουν ανάθεση των στόχων στους κατάλληλους πόρους.

Έλεγχος και υπηρεσίες διάγνωσης όπου υποστηρίζουν έλεγχο των πόρων για πιθανά προβλήματα όπως αποτυχία, ανίχνευση παρείσφρησης, υπερφόρτωση κ.τ.λ.
Οι υπηρεσίες δημιουργίας αντιγράφων δεδομένων υποστηρίζονται από την διαχείριση των πόρων αποθήκευσης για την μεγιστοποίηση της απόδοσης πρόσβασης στοιχείων όσο αφορά τον χρόνο απόκρισης την αξιοπιστία και το κόστος.

Τα λειτουργικά συστήματα των πλεγμάτων επιτρέπουν στα γνωστά πρότυπα προγραμματισμού να χρησιμοποιούν διάφορες υπηρεσίες για εξεύρεσης πόρων, ασφάλειας, κατανομή πόρων κ.τ.λ.

Τα συστήματα διαχείρισης φόρτου εργασίας και πλαισίων συνεργασίας παρέχουν την δυνατότητα περιγραφής, χρησιμοποίησης και διαχείρισης πολύ-βηματικών, ασύγχρονων και πολύ συστατικών ροών εργασίας.

Οι υπηρεσίες ανακάλυψης λογισμικού ανακαλύπτουν και επιλέγουν την καλύτερη δυνατή πλατφόρμα εφαρμογής και εκτέλεσης λογισμικού βάσει των παραμέτρων που έχουν τεθεί για την επίλυση του προβλήματος.

Οι κοινοτικοί εξυπηρετητές πιστοποίησης επιβάλλουν κάποιες κοινοτικές πολιτικές και κυβερνούν την πρόσβαση στους πόρους παρέχοντας την ικανότητα αυτή στους κοινοτικούς χρήστες. Αυτοί οι servers επιβάλλουν μια σφαιρική πολιτική στηριζόμενη στις πληροφορίες των πόρων και στα πρωτόκολλα διοίκησης και ασφάλειας από τα στρώματα πόρων και συνδεσιμότητας αντίστοιχα.

Κοινοτικές υπηρεσίες λογιστικής και πληρωμής συγκεντρώνουν πληροφορίες που αφορούν την χρήση των πόρων με σκοπό την μέτρηση, λογιστική καθώς και περιορισμό χρηστών από μέλη της κοινότητας.

Οι υπηρεσίες συνεργασίας υποστηρίζουν την συντονισμένη ανταλλαγή πληροφοριών μέσα σε μεγάλες κοινότητες χρηστών, είτε σύγχρονα είτε ασύγχρονα.

2. Grid Security Infrastructure GSI (Υποδομή ασφάλειας πλέγματος)

Το GSI είναι μια προδιαγραφή για μυστική, μη παραποιήσιμη και ασφαλή επικοινωνία. Είναι ένα σύνολο εργασιών, βιβλιοθηκών και πρωτοκόλλων που χρησιμοποιούνται ώστε οι χρήστες και οι εφαρμογές του πλέγματος να έχουν πρόσβαση στους πόρους με ασφάλεια. Η υποδομή αυτή βασίζεται στην κρυπτογράφηση δημοσίου κλειδιού, σε πιστοποιητικά της μορφής X.509 και στο πρωτόκολλο Secure Sockets Layer (SSL) για μια ασφαλή επικοινωνία. Κάποιες προεκτάσεις των παραπάνω προτύπων προσφέρουν στους χρήστες μια εύκολη και μοναδική διαδικασία πρόσβασης (Single Sign-on) και μια μορφή αντιπροσώπευσης (Delegation).

Το GSI διαθέτει και κάποιες ιδιότητες που κάνουν την επικοινωνία ασφαλέστερη και ευκολότερη στο δίκτυο του πλέγματος.

- Στην επικοινωνία μεταξύ χρηστών για να είναι προσδιορισμένες οι ταυτότητές τους παρέχεται από το GSI η λεγόμενη *πιστοποίηση (authentication).*

- Ένα κανάλι επικοινωνίας που καθιερώνεται μεταξύ δύο χρηστών είναι ασφαλές με την βοήθεια της *κρυπτογράφησης (encryption),* της *μη-αποκήρυξης (non-repudiation)* και της *ακεραιότητας (integrity)* των στοιχείων/δεδομένων.

- Η *εξουσιοδότηση (authorization)* είναι άλλη μια ιδιότητα του GSI που δείχνει ποιος έχει δυνατότητα πρόσβασης σε πόρους ενός εικονικού

οργανισμού (VO) και ποιες είναι οι δυνατότητες για τα μέλη των εικονικών οργανισμών.

2.1 *Χρήσιμοι μηχανισμοί κρυπτογράφησης*

2.1.1 *DES (Data Encryption Standard) Πρότυπο κρυπτογράφησης στοιχείων*

Το πρότυπο κρυπτογράφησης στοιχείων DES είναι μια μορφή συμμετρικής κρυπτογράφησης η οποία δημοσιεύτηκε το 1977 από το Αμερικάνικο Γραφείο Προτύπων (US National Bureau of Standards).

Η DES χρησιμοποιεί ένα κλειδί των 56 bits και χαρτογραφεί ένα συρμό 64 bits εισαγωγής ενός αναγνώσιμου μηνύματος πάνω σε ένα συρμό 64 bits εξόδου ενός κρυπτογραφημένου μηνύματος.

Στις μέρες μας όμως με την ανάπτυξη της υπολογιστικής δύναμης ένα κλειδί 56 bits είναι σαφώς μικρό. Βέβαια το μέγεθος ενός κλειδιού αποτελεί μια από τις πιο αμφισβητούμενες πτυχές του αλγορίθμου αυτού.

Η δομή λειτουργίας του προτύπου κρυπτογράφησης DES έχει ως εξής:
Η είσοδος των 64 bits αρχικά μεταλλάσσεται και κατόπιν υποβάλλεται σε 16 κύκλους. Κάθε ένας από αυτούς του κύκλους παίρνει την έξοδο 64 bits του προηγούμενου κύκλου και ένα κλειδί 48 bits ανά κύκλο και παράγει μια 64 bits έξοδο. Τα κλειδιά ανά κύκλο είναι υποσύνολα των 48 bits, από το κλειδί των 56 bits. Μετά από τον κύκλο η 64 bits έξοδο υποβάλλεται σε αντίστροφη αρχική

μεταλλαγή. Η DES αποκρυπτογράφηση πραγματοποιείται εκτελώντας την διαδικασία αντίστροφα.

2.1.2Triple DES (3-DES):

Μια άλλη μορφή κρυπτογράφησης που είναι βασισμένη στην DES, είναι η 3-DES η οποία κρυπτογραφεί τα στοιχεία τρεις φορές χρησιμοποιώντας ένα διαφορετικό κλειδί για τουλάχιστον ένα από τα τρία περάσματα κρυπτογράφησης δίνοντας κλειδί μεγέθους 112-168 bits.

2.1.3RSA encryption

Η RSA κρυπτογράφηση πήρε την ονομασία της από τους εφευρέτες της R.Rivest, A.Shamir, L.Adelman. Παρέχει μυστικότητα και ψηφιακές υπογραφές και η ασφάλειά της βασίζεται στη δυσκολία επίλυσης προβλημάτων παραγοντοποίησης ακεραίων. Είναι ο πρώτος αλγόριθμος κατάλληλος για υπογραφές, κρυπτογραφήσεις και χρησιμοποιείται ευρέως σε πρωτόκολλα ηλεκτρονικού εμπορίου όπως επίσης και για μεταφορά βασικού υλικού (κλειδιά) από τον πελάτη (χρήστης) στον server (εξυπηρετητής) με ασφάλεια.

2.2 Χρήσιμοι καθορισμοί εννοιών

2.2.1 Transmission Control Protocol TCP (πρωτόκολλο ελέγχου μετάδοσης)

Το πρωτόκολλο αυτό στηρίζεται στη διεύθυνση IP για να καθορίσει ένα αξιόπιστο πρωτόκολλο παράδοσης στοιχείων [1] .

[1]http://en.wikipedia.org/wiki/Transmission_Control_Protocol

2.2.2 Network protocol (πρωτόκολλο διαδικτύου)

Το πρωτόκολλο διαδικτύου είναι μια επίσημη περιγραφή των μηνυμάτων και ένα σύνολο κανόνων για την ανταλλαγή μηνυμάτων [2].

2.2.3Resources (πόροι)

Οι πόροι είναι οι οντότητες που υπάρχει δυνατότητα διαμοιρασμού από τους χρήστες του πλέγματος και περιέχουν μερικές ικανότητες οι οποίες μπορούν να προσεγγιστούν μέσω του προγραμματισμού εφαρμογών διεπαφής (API) ή του πρωτοκόλλου. Οι πόροι αναφέρονται και με άλλους όρους όπως πελάτες (clients) ή hosts ή μέλη κ.α.

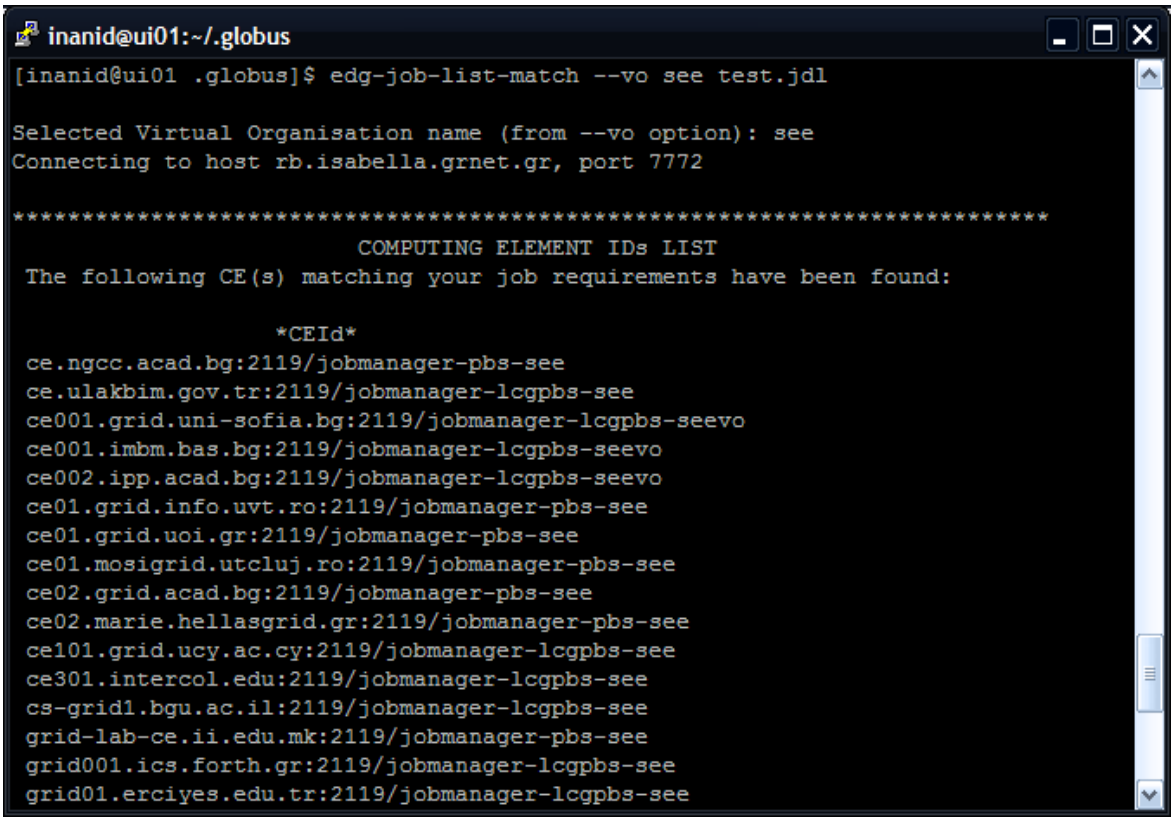
2.2.4User Interface UI (διεπαφή χρήστη)

Η διεπαφή χρήστη είναι απλά ένας ηλεκτρονικός υπολογιστής όπου κάθε χρήστης έχει έναν τοπικό λογαριασμό στον οποίο έχει εγκαταστήσει το ψηφιακό πιστοποιητικό του.

Επίσης θα πρέπει να βρίσκεται εγκατεστημένο το λειτουργικό Linux με όλα τα απαραίτητα λογισμικά πελάτη, APIs και εργαλεία για την ανάπτυξη και εκτέλεση εφαρμογών στο περιβάλλον του Grid. Ουσιαστικά μια διεπαφή χρήστη παρέχει το σημείο πρόσβασης ενός χρήστη για το πλέγμα δηλαδή το σημείο που ο χρήστης θα πιστοποιηθεί και εξουσιοδοτηθεί (authorization) για να χρησιμοποιήσει τους πόρους του πλέγματος.

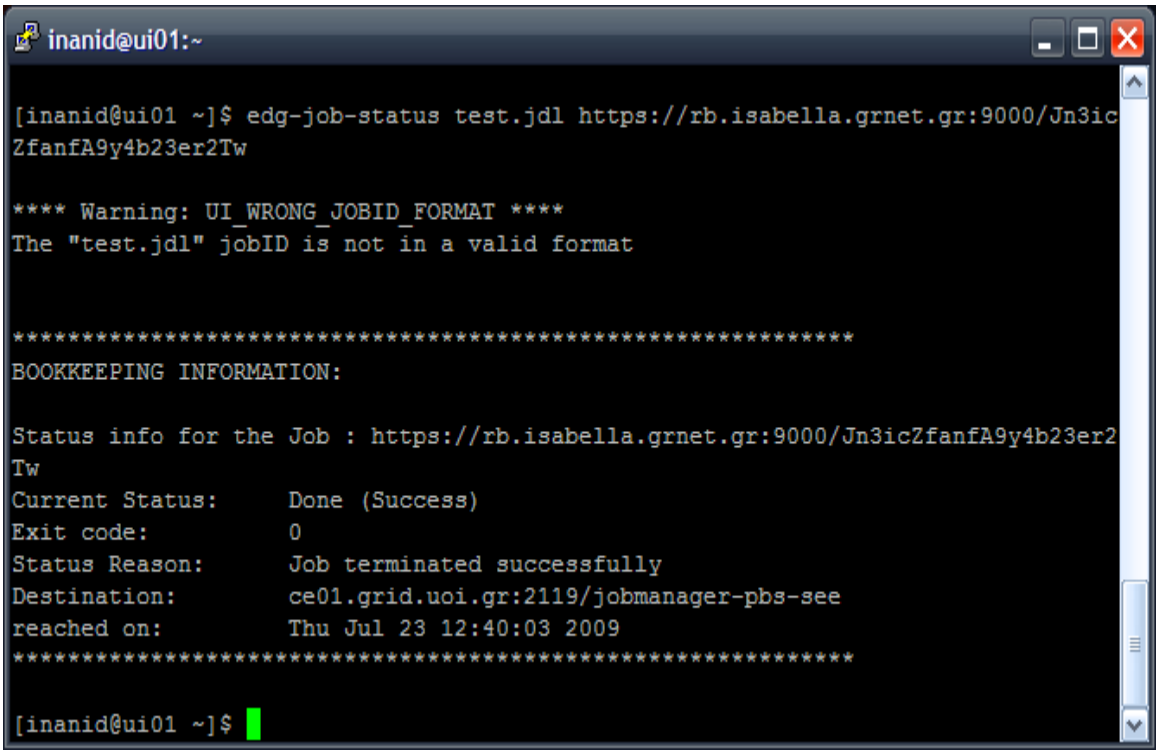
[2] http://en.wikipedia.org/wiki/Network_Protocol

Για υλοποίηση λειτουργιών μια διεπαφή παρέχει στους χρήστες είτε μια διασύνδεση γραμμής εντολών (Command Line User Interface) είτε μια γραφική διασύνδεση (Graphical User Interface). Μερικές από τις λειτουργίες φαίνονται παρακάτω:

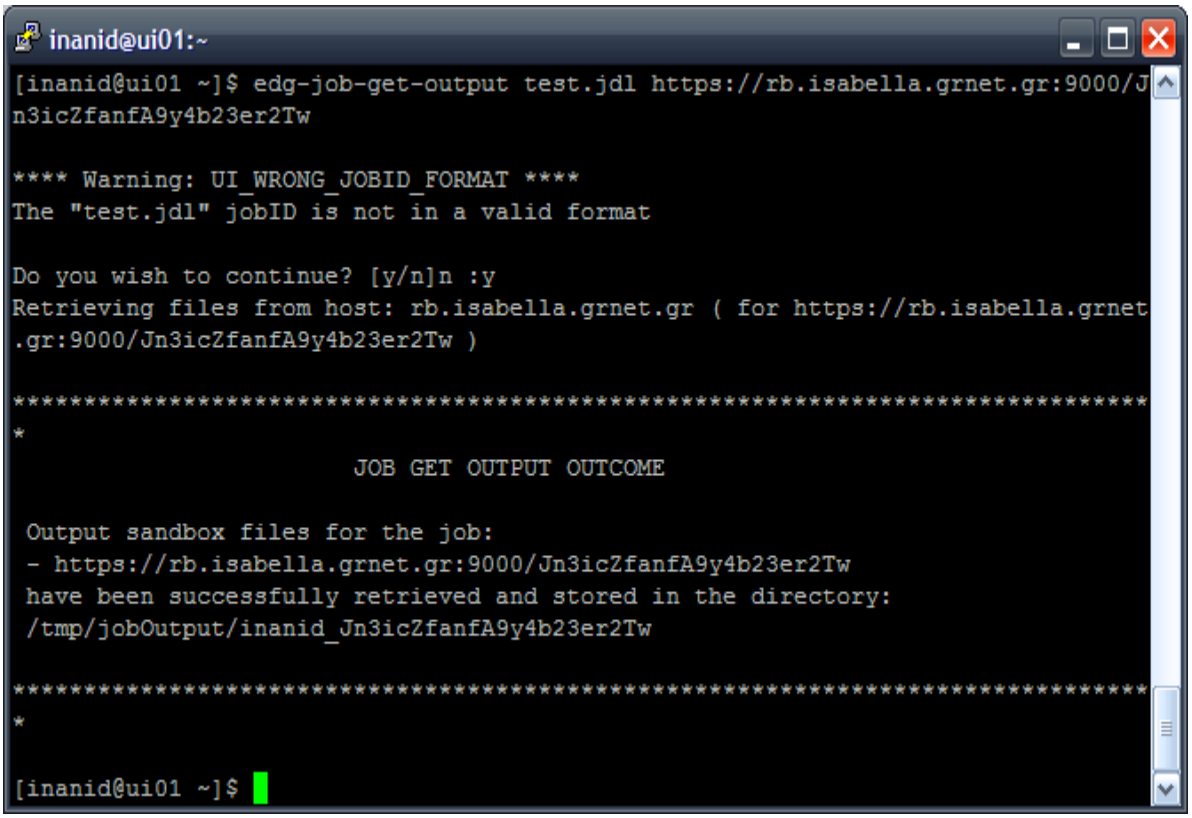


Εικόνα 3:Εύρεση των κατάλληλων υπολογιστικών στοιχείων και στοιχείων αποθήκευσης, τα οποία είναι διαθέσιμα και συμβατά με τις απαιτήσεις των εφαρμογών / εργασιών.

Εικόνα 4:Υποβολή μιας εργασίας (job submission)



Εικόνα 5:Έλεγχος και παρακολούθηση της εργασίας που εκτελείται.



Εικόνα 6:Λήψη αποτελεσμάτων των ολοκληρωμένων εργασιών.

2.2.5 Application Programming Interface API (προγραμματισμός εφαρμογών διεπαφής)

Ο προγραμματισμός εφαρμογών διεπαφής είναι ένα σύνολο από ρουτίνες για την διευκόλυνση της ανάπτυξης εφαρμογών. Καθορίζει ένα πρότυπο διεπαφής για επίκληση ενός ειδικού συνόλου από λειτουργίες. Μπορεί να είναι επίσης μια ειδική γλώσσα όπως για παράδειγμα μια συμβατική γλώσσα προγραμματισμού όπως C ή Java.

2.2.6 Trusted Third Parties TTP (εμπιστευόμενα τρίτα πρόσωπα Unconditionally - Trusted Parties (άνευ όρων εμπιστευόμενο πρόσωπο)

Είναι μια οντότητα που έχει την δυνατότητα πρόσβασης σε μυστικά και ιδιωτικά κλειδιά χρηστών

2.2.7 Functionallity Trusted Parties (λειτουργικά εμπιστευόμενο πρόσωπο)

Είναι μια οντότητα που υποτίθεται ότι είναι ειλικρινής και έμπιστη αλλά δεν έχει καμία πρόσβαση σε μυστικά αρχεία και κλειδιά χρηστών.

2.2.8 Storage Element SE (στοιχείο αποθήκευσης)

Παρέχει ομοιόμορφη πρόσβαση στους πόρους αποθήκευσης στοιχείων και μπορεί να υποστηρίξει διαφορετικά πρωτόκολλα πρόσβασης στοιχείων και διεπαφών (interfaces) για την πρόσβαση στα δεδομένα. Ένα SE μπορεί να ελέγχει απλούς σκληρούς δίσκους, μεγάλες συστοιχίες δίσκων καθώς επίσης και συστήματα μαζικής αποθήκευσης (Mass Storage Systems, MSS).

Όπως το Storage Element υποστηρίζει βιβλιοθήκες και APIs, έτσι και κάποιοι πόροι αποθήκευσης διαχειρίζονται από μια υπηρεσία διαχείρισης αποθηκευτικών πόρων (Storage Resource Management, SRM). Ο SRM είναι μια διεπαφή καθορισμού και ένα τμήμα μεσισμικού του οποίου λειτουργία είναι να παρασχεθεί η δυναμική κατανομή και η διαχείριση αρχείων στα κοινά στοιχεία αποθήκευσης (SE) του πλέγματος.

Αυτή η υπηρεσία επιτρέπει την διαχείριση των περιεχομένων των αποθηκευτικών πόρων. Παρακάτω φαίνονται κάποια είδη SE:

- Ένα είδος Storage Element είναι το κλασικό *(Classic Storage Element, CSE)* το οποίο είναι ένας βελτιστοποιημένος κεντρικός υπολογιστής του πρωτοκόλλου μεταφοράς αρχείων (FTP server) με την επικύρωση και την έγκριση του πλέγματος ο οποίος δεν διαθέτει υπηρεσία διαχείρισης αποθηκευτικών πόρων (SRM) αλλά συστήματα με σκληρούς δίσκους και ένα πρόγραμμα-εξυπηρετητή. Τα πιο κοινά διοικητικά χαρακτηριστικά γνωρίσματα δίσκων μεταβιβάζονται στα καθήκοντα διοικητών περιοχών. (Παραδείγματος χάριν, η διαστημική επιφύλαξη για VOs εκτελείται από το χώρισμα δίσκων).

Εικόνα 7:Στοιχείο αποθήκευσης (κλασικό)

- Άλλο ένα είδος SE είναι τα συστήματα μαζικής αποθήκευσης *(Mass Storage Systems, MSS)*. Το MSS παρέχει τα απαραίτητα εργαλεία και το υλικό για μία ασφαλή και αξιόπιστη μακροπρόθεσμη αποθήκευση των στοιχείων με γρήγορη πρόσβαση. Είναι ένα σύστημα το οποίο λειτουργεί όλες τις ώρες και ημέρες της εβδομάδος χωρίς την επέμβαση χειρισμού από κάποιο πρόσωπο. Αυτά τα στοιχεία μπορούν να προσεγγιστούν με ένα πακέτο υπηρεσίας πελάτη/κεντρικού υπολογιστή που προσαρμόζεται σύμφωνα με τις απαιτήσεις της κοινότητας χρηστών GSI. Το σύστημα αυτό παρέχει υπηρεσία διαχείρισης αποθηκευτικών πόρων (SRM). Ένα παράδειγμα συστημάτων MSS είναι ο HPSS και ο CASTOR.

Το σύστημα αποθήκευσης υψηλής επίδοσης (HPSS) είναι ένα σύγχρονο, ευέλικτο, σύστημα μαζικής αποθήκευσης. Έχει χρησιμοποιηθεί στο NERSC για αποθήκευση αρχείων από το 1998. Στο NERSC, τα στοιχεία αποθήκευσης διπλασιάζονται σχεδόν κάθε έτος. Στις 16 Αυγούστου 2007, υπήρχαν πάνω από 3.5 petabytes αποθηκευμένων στοιχείων σε περίπου 61 εκατομμύρια αρχεία. Το HPSS στηρίζει ένα μέσο ποσοστό μεταφοράς περισσότερων από 100 MB/s, 24 ώρες ανά ημέρα, με αιχμές στα 450 MB/s.

Τα συστήματα μαζικής αποθήκευσης στο Κέντρο Πυρηνικών Μελετών και Ερευνών (CERN) έχουν εξελιχθεί με την πάροδο του χρόνου για να καλύψουν τις αυξανόμενες απαιτήσεις. Το νέο προηγμένο σύστημα αποθήκευσης στο CERN (Cern Advanced STORage system, CASTOR) και το νέο διοικητικό στρώμα κρύπτης δίσκων του (CASTOR2) έχει αναπτυχθεί για να αντιμετωπίσει τις προκλήσεις που αυξάνονται από τα πειράματα χρησιμοποιώντας το νέο επιταχυντή που έχει κατασκευαστεί στο CERN και ονομάζεται Large Hadron Collider (LHC). Το σύστημα αυτό πρέπει να είναι σε θέση να αντιμετωπίσει τις εκατοντάδες των εκατομμυρίων των αρχείων, δεκάδες petabytes αποθήκευσης και να χειριστεί μια σταθερή ρυθμοαπόδοση αρκετών gigabytes ανά δευτερόλεπτο.

- Υπάρχει και ένα νέο είδος SE που αναπτύχθηκε πρόσφατα και ονομάζεται *Disk Pool Manager (DPM)* και είναι μια λύση για την διαχείριση των δίσκων αποθήκευσης (σκληρών δίσκων). Αποτελείται από ένα κεντρικό υπολογιστή dCache και από έναν ή περισσότερους κόμβους ‘’πισίνες’’. Ο κεντρικός υπολογιστής αντιπροσωπεύει το ενιαίο σημείο πρόσβασης στο SE στο δίσκο πισίνας κάτω από ένα ενιαίο εικονικό δέντρο συστημάτων αρχείων. Δεν υπάρχει κάποιος περιορισμός στο μέγεθος χωρητικότητας δίσκου που μπορεί να διαχειριστεί ο DPM και

ουσιαστικά προσφέρει μία εφαρμογή προδιαγραφών του διαχειριστή πόρων αποθήκευσης. Επίσης υπάρχει η δυνατότητα μετατροπής του κλασσικού SE σας σε DPM όπου δεν απαιτείται η μετακίνηση αρχείων. Πρέπει απλώς να καταστεί ο κεντρικός υπολογιστής DPM ενήμερος για τα αρχεία που είναι παρόντα στο στοιχείο αποθήκευσης (SE) ενός χρήστη. Είναι μια λειτουργία μεταδεδομένων και καμία πραγματική μετακίνηση αρχείων δεν απαιτείται.

2.2.9 Computing Element CE (υπολογιστικό στοιχείο)

Το υπολογιστικό στοιχείο CE ορίζεται σαν μια ουρά εργασιών (batch queue) που έχουν υποβληθεί από τους χρήστες του Grid. Η ονομασία των ουρών αναμονής είναι της μορφής: <*hostname*>:<*port*>/<*batch_queue_name*> Εργασίες διαφορετικού μεγέθους ή διαφορετικών εικονικών οργανισμών VO που βρίσκονται στο ίδιο σύστημα θεωρούνται σαν διαφορετικά Computing Elements. Τα CE συνεργάζονται με κάποιες υπο-υπηρεσίες του GSI που είναι οι ‘’εργάτες‘’ (*Worker Nodes, WN*), ένα σύστημα διαχείρισης τοπικών πόρων (*Local Resource Management System, LRMS*) και έναν (‘θυρωρό’ *Gatekeeper*) ο οποίος είναι το σημείο επικοινωνίας με το υπόλοιπο δίκτυο του Grid. Ο θυρωρός (είναι γνωστός και σαν πύλη του Grid (*Grid Gate, GG*)) είναι υπεύθυνος για την αποδοχή και ανάθεση των εργασιών στους εργάτες (Worker Nodes) οι οποίοι τις εκτελούν και στέλνουν τα αποτελέσματα πίσω στον Resource Broker. Να σημειωθεί ότι όλες οι απαραίτητες βιβλιοθήκες, εντολές και APIs για την εκτέλεση διάφορων ενεργειών στο πλέγμα, βρίσκονται διαθέσιμα στους Worker Nodes.

2.2.10 Information Service IS (υπηρεσία πληροφοριών)

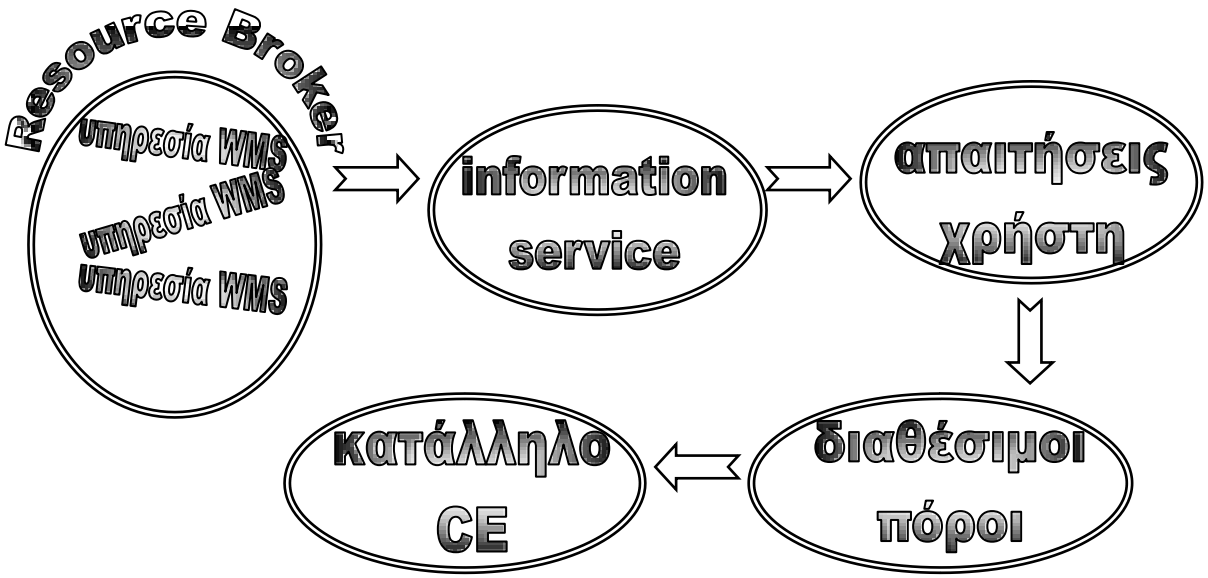
Η υπηρεσία πληροφοριών IS παρέχει πληροφορίες σχετικά με τους πόρους και την κατάσταση αυτών. Η υπηρεσία αυτή παίζει σημαντικό ρόλο στο δίκτυο του

πλέγματος διότι μέσω αυτής της υπηρεσίας και των πληροφοριών που παρέχει μπορούν να εντοπιστούν τα διαθέσιμα Computing Elements για την εκτέλεση των εργασιών. Επίσης μπορούν να εντοπιστούν και τα διαθέσιμα Storage Elements τα οποία κρατάνε αντίγραφα διαφόρων απαραίτητων αρχείων και καταλόγων.

2.2.11 Workload Management System WMS (υπηρεσία διαχείρισης φόρτου εργασίας)

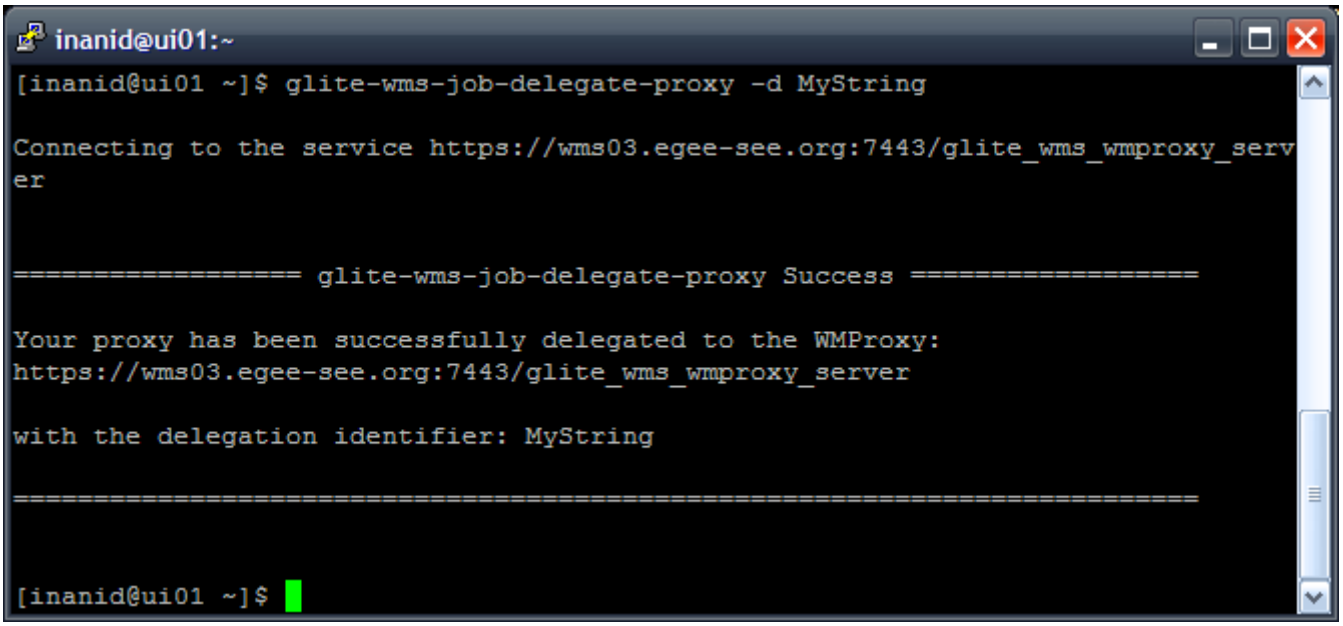
Η υπηρεσία διαχείρισης φόρτου εργασίας WMS είναι υπεύθυνη για τις υποβληθείσες εργασίες (από τους χρήστες) και την ανάθεση αυτών στο κατάλληλο Computing Element. Η καταλληλότητα του CE εξαρτάται με τις απαιτήσεις της εργασίας και τους διαθέσιμους πόρους. Για αυτό το σκοπό η υπηρεσία WMS βρίσκει πληροφορίες από την υπηρεσία πληροφοριών (Information Service,IS) και τους καταλόγους αρχείων. Ο ‘’μεσάζων εργασιών‘’ (*Resource Broker, RB*) είναι το σύστημα στο οποίο εγκαθίστανται οι υπηρεσίες WMS. Ο RB είναι αυτός που ταιριάζει τις απαιτήσεις ενός χρήστη με τους διαθέσιμους πόρους στο πλέγμα.

Να σημειωθεί ότι η υποβολή μιας εργασίας απαιτεί πιστοποίηση μέσω του GSI μεταξύ του User Interface και του Resource Broker καθώς επίσης και μεταξύ του Resource Broker και του Computing Element.



Εικόνα 8:Διασυνδέσεις της υπηρεσίας διαχείρισης φόρτου εργασίας.

Με την εντολή *glite-wms-job-delegate-proxy -d MyString* το πληρεξούσιο ενός χρήστη αντιπροσωπεύεται από το WMproxy το οποίο είναι ένα στοιχείο του WMS και είναι υπεύθυνο για την υποδοχή εισερχόμενων αιτήσεων από το User Interface (π.χ. υποβολή εργασιών, αφαίρεση εργασιών κ.τ.λ.) . Εφόσον το πληρεξούσιο είναι έγκυρο τότε οι αιτήσεις περνάνε στα άλλα στοιχεία του WMS (υπολογιστικό στοιχείο, υπηρεσία πληροφοριών, μεσάζων εργασίας κ.α.) Στην παρακάτω οθόνη προβολής φαίνεται η αίτηση για αντιπροσώπευση του πληρεξούσιου από την υπηρεσία WMproxy με προσδιοριστικό αντιπροσωπείας το MyString.



Εικόνα 9:Αντιπροσώπευση του πληρεξούσιου από την υπηρεσία WMProxy.

2.2.12 Data Management System DMS (σύστημα διαχείρισης δεδομένων)

Το σύστημα διαχείρισης δεδομένων δίνει την δυνατότητα στους χρήστες να μετακινούν αρχεία / δεδομένα από και προς το Grid, να τα αντιγράφουν σε διάφορες τοποθεσίες και να τα εντοπίζουν με την βοήθεια κάποιων πρωτοκόλλων όπως το GridFTP και ένα σύστημα πληροφοριών καταλόγου (Replica Location Service, RLS).

3. Εικονικοί οργανισμοί & μηχανισμοί κρυπτογραφίας

3.1 Virtual Organizations (εικονικοί οργανισμοί)

Ένας χρήστης για να πιστοποιηθεί και να χρησιμοποιήσει την υπηρεσία του πλέγματος εκτελώντας χρήσιμες εργασίες (π.χ. υποβολή εργασιών, μεταφορές αρχείων, αντίγραφα αρχείων κ.τ.λ.) στο περιβάλλον του grid θα πρέπει πρώτα να έχει εγγραφεί σε έναν εικονικό οργανισμό (Virtual Organization). Ο εικονικός οργανισμός (VO) είναι μια εταιρική, μη κερδοσκοπική και παραγωγική οντότητα η οποία χρησιμοποιεί τηλεπικοινωνιακά εργαλεία για να επιτρέψει, να διατηρήσει και να στηρίξει τις σχέσεις μελών στα κατανεμημένα περιβάλλοντα εργασίας. Είναι μια ομάδα από πιστοποιημένους χρήστες του grid με κοινές απαιτήσεις και ενδιαφέροντα οι οποίοι είναι σε θέση να συνεργαστούν με άλλα μέλη της ομάδας ή και από άλλους οργανισμούς ανεξαρτήτως γεωγραφικής θέσης.

Ένας εικονικός οργανισμός ορίζει τα εξής:

- οι πόροι οι οποίοι είναι διαθέσιμοι
- οι πιστοποιημένοι χρήστες που τους επιτρέπεται η πρόσβαση στο περιβάλλον του πλέγματος
- με ποιον τρόπο και κάτω από ποιες συνθήκες έχουν οι χρήστες πρόσβαση και κάνουν χρήση του grid

Επίσης υπάρχει η δυνατότητα για κάποιον που είναι αντιπρόσωπος μιας κοινότητας να δημιουργήσει τον δικό του VO. Για παράδειγμα, μια φοιτητική κοινότητα μπορεί να προβεί σε μια τέτοια ενέργεια προκειμένου να δώσει πρόσβαση στους φοιτητές να χρησιμοποιήσουν την υπηρεσία του grid.

Η διαδικασία δημιουργίας ενός εικονικού οργανισμού είναι η παρακάτω:

- Ονομασία του VO
- Διαδικασία αποδοχής του VO
- Εγκατάσταση
- Ενσωμάτωση
- Οργάνωση

Ακόμη υπάρχει η δυνατότητα για κάποιον διοικητή ενός συστήματος να δώσει πρόσβαση στους πόρους του σε έναν ορισμένο εικονικό οργανισμό. Προκειμένου να υποστηριχθεί ο νέος οργανισμός, ο διοικητής του συστήματος θα πρέπει να διαμορφώσει κατάλληλα την πλατφόρμα βάσης του ώστε να κατακτήσει διαθέσιμους τους πόρους σε αυτό τον VO. Η διαμόρφωση βάσης μπορεί να γίνει αυτόματα χρησιμοποιώντας τα κατάλληλα εργαλεία και σχεδιαγράμματα διαμόρφωσης. Υπάρχουν αρκετά παραδείγματα χρηστών που επιθυμούν δημιουργία εικονικών οργανισμών όπως είναι:

- Φοιτητές από διαφορετικά πανεπιστήμια οι οποίοι χρησιμοποιούν την υπολογιστική δύναμη για τις εφαρμογές που χρειάζονται.
- Φυσικοί από διάφορα ερευνητικά ιδρύματα οι οποίοι περιπλέκονται στις ίδιες πειραματικές εφαρμογές χρησιμοποιώντας την υπηρεσία του πλέγματος για αναλύσεις δεδομένων που αφορούν τα πειράματα.
- Αστρονόμοι που αναλύουν δεδομένα από πολλαπλά τηλεσκόπια από όλο τον κόσμο.
- Ο κλάδος της βιοιατρικής που όπου συνίσταται ένας μεγάλος αριθμός επιστημόνων / ιατρών που εργάζονται σε διαφορετικούς τομείς και χώρες για τον ίδιο σκοπό.

3.2 ***Virtual Organization Membership Service VOMS (υπηρεσία μελών των εικονικών οργανισμών)***

Η πιστοποίηση ενός χρήστη του πλέγματος για την πρόσβαση και χρήση των πόρων μπορεί να πραγματοποιηθεί με δύο εναλλακτικούς τρόπους. Ο πρώτος επιτυγχάνεται με την βοήθεια της υπηρεσίας μελών των εικονικών οργανισμών (VOMS) όπου το proxy πιστοποιητικό ενός χρήστη μπορεί να επεκταθεί με πληροφορία σχετικά με τον εικονικό οργανισμό που ανήκει ο χρήστης, τις ομάδες του εικονικού οργανισμού στις οποίες ανήκει ο χρήστης και τον ρόλο που έχει ο χρήστης στον συγκεκριμένο VO. Μερικές από τις ικανότητες μιας υπηρεσίας VOMS φαίνονται παρακάτω:

- Δίνει επιπλέον πληροφορίες για τους ρόλους του VO,τους χρήστες και τις ομάδες του.
- Κάθε VO έχει μία μονάδα δεδομένων η οποία περιέχει ομάδες μελών, ικανότητες, ρόλους και πληροφορίες για κάθε χρήστη.
- Ο χρήστης επικοινωνεί με τον VOMS εξυπηρετητής ζητώντας πληροφορίες έγκρισης.
- Ο εξυπηρετητής στέλνει τις πληροφορίες έγκρισης στον χρήστη (πελάτη) οι οποίες περιέχονται στο πληρεξούσιο πιστοποιητικό (proxy).

Ο VOMS παρέχει ένα τρόπο πιστοποίησης του χρήστη προκειμένου να χρησιμοποιήσει έναν συγκεκριμένο πόρο στο δίκτυο του πλέγματος.

3.2.1Grid-mapfile

Υπάρχει άλλος ένας ανάλογος τρόπος πιστοποίησης του χρήστη που πραγματοποιείται με τον μηχανισμό του αρχείου *grid-mapfile (αρχείο*

χαρτογράφησης). Ένα τέτοιο αρχείο βρίσκεται σε κάθε πόρο ο οποίος προσφέρεται για το δίκτυο του πλέγματος και δουλειά αυτού του αρχείου είναι η αντιστοίχηση των θεμάτων των πιστοποιητικών των χρηστών σε τοπικούς χρήστες.

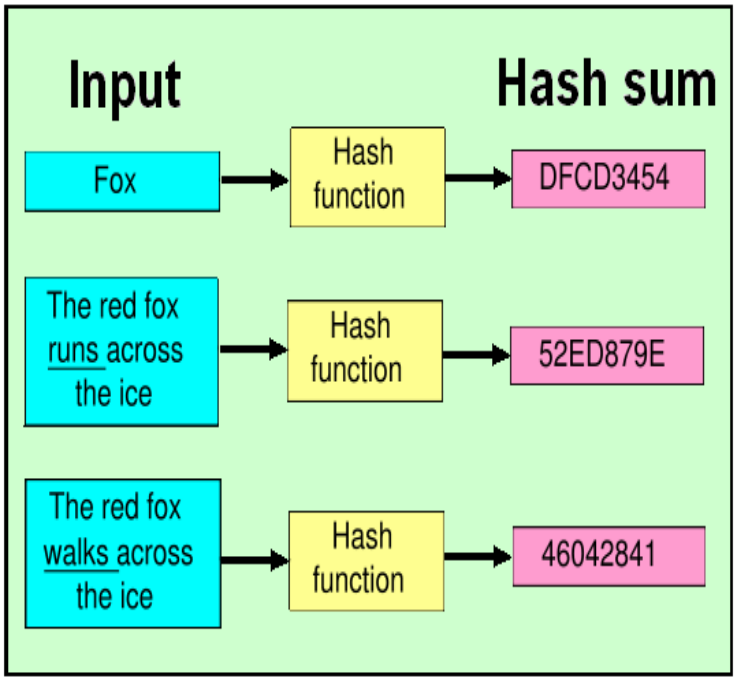
Όταν ένας χρήστης κάνει μια αίτηση για την χρήση ενός πόρου και φτάσει στο αντίστοιχο σύστημα του πόρου, το θέμα του πιστοποιητικού που φαίνεται στο proxy ελέγχεται σε σχέση με τα περιεχόμενα του grid-mapfile για το αν υπάρχει κάποιος τοπικός χρήστης που αντιστοιχείται σε αυτό το πιστοποιητικό. Εάν βρεθεί τοπικός χρήστης τότε χρησιμοποιείται για την πρόσβαση στον πόρο.

3.3 Hash function

Η σημασιολογική έννοια της λέξης ‘’hash‘’ στην ελληνική γλώσσα είναι : λιανίζω, κόβω σε κομμάτια. Παρόμοια οι λειτουργίες hash έχουν μια παρεμφερή έννοια για ένα υπολογιστικό πλέγμα. Οι λειτουργίες hash δέχονται ένα μήνυμα το οποίο διαιρούν / κόβουν σε κομμάτια. Το νέο αυτό μήνυμα είναι το αποτέλεσμα της hash λειτουργίας που ονομάζεται hash αξία ή hash αποτέλεσμα ή hash κωδικός ή συνοπτικό μήνυμα (hash-value or hash-result or hash-code, message digest) και μπορεί να ενεργήσει σαν μια συνοπτική αντιπροσώπευση του μηνύματος από το οποίο υπολογίστηκε. Τα στοιχεία/δεδομένα/μηνύματα που κωδικοποιούνται συχνά αποκαλούνται απλά σαν ‘’μήνυμα’’ .

Στην κρυπτογραφία ο MD5 (Message – Digest algorithm 5) είναι μία ευρέως χρησιμοποιούμενη λειτουργεία hash με 128-bit hash αποτέλεσμα. Επίσης έχει υιοθετηθεί για μία ευρεία ποικιλία εφαρμογών ασφάλειας και συνήθως χρησιμοποιείται για τον έλεγχο ακεραιότητας των δεδομένων / στοιχείων.

Ένα παράδειγμα λειτουργιών hash είναι οι κώδικες επικύρωσης μηνυμάτων (Message Authentication Codes, MAC) οι οποίοι επιτρέπουν επικύρωση μηνυμάτων με τη βοήθεια τεχνικών συμμετρικών αλγόριθμων. Οι αλγόριθμοι MAC δέχονται σαν είσοδο ένα κλειδί και ένα μήνυμα και παράγουν μια έξοδο καθορισμένου μήκους όπου είναι ανέφικτη η αντιγραφή της χωρίς την παρουσία του κλειδιού. Συγκεκριμένα μια λειτουργία hash χαρτογραφεί σειρές από bits ενός αυθαίρετου πεπερασμένου μήκους σε σειρές καθορισμένου μήκους.



Με την βοήθεια της διπλανής εικόνας παρατηρούμε ότι μια είσοδο (Input) αυθαίρετου μήκους μετά την λειτουργία hash παράγεται ένα αποτέλεσμα (Hash-sum) καθορισμένου μήκους.

Εικόνα 10:Λειτουργία hash.

Κύριες ιδιότητες hash λειτουργιών

- Είναι εξαιρετικά εύκολος ο υπολογισμός ενός hash μηνύματος για οποιαδήποτε δεδομένα στοιχεία.
- Είναι απίθανο στην πράξη να υπολογιστεί ένα κείμενο που έχει δεδομένο hash.
- Είναι εξαιρετικά δύσκολο, δύο διαφορετικά μηνύματα όσο παρεμφερή κι αν είναι, να έχουν το ίδιο hash.

Οι hash λειτουργίες χρησιμοποιούνται για πολλούς και ποικίλους λόγους στον κλάδο της κρυπτογραφίας. Οι πρακτικές εφαρμογές περιλαμβάνουν ακεραιότητα στοιχείων (data integrity), ψηφιακές υπογραφές (digital signatures) και διάφορες εφαρμογές για ασφάλεια πληροφοριών. Όπως για λόγους ασφαλείας και απόδοσης οι περισσότεροι αλγόριθμοι ψηφιακών υπογραφών διευκρινίζουν ότι μόνο αφομοίωση του μηνύματος υπογράφεται και όχι ολόκληρο το μήνυμα. Επίσης οι hash λειτουργίες βρίσκουν χρήση και για την παραγωγή ψευδοτυχαίων bits.

3.4 Digital signature (ψηφιακή υπογραφή)

Μια ψηφιακή υπογραφή είναι ένας τύπος ασύμμετρης κρυπτογραφίας που χρησιμοποιείται για να μιμηθεί τις ιδιότητες μιας χειρόγραφης υπογραφής σε χαρτί. Αποτελείται από τρεις αλγόριθμους οι οποίοι είναι:

- Αλγόριθμος παραγωγής κλειδιών (key generator algorithm) : Ο αλγόριθμος αυτός επιλέγει ένα ιδιωτικό (private key) ή ένα δημόσιο κλειδί (public key) τυχαία από ένα σύνολο πιθανών τέτοιων κλειδιών, και τα αντιστοιχεί σε ζευγάρια.

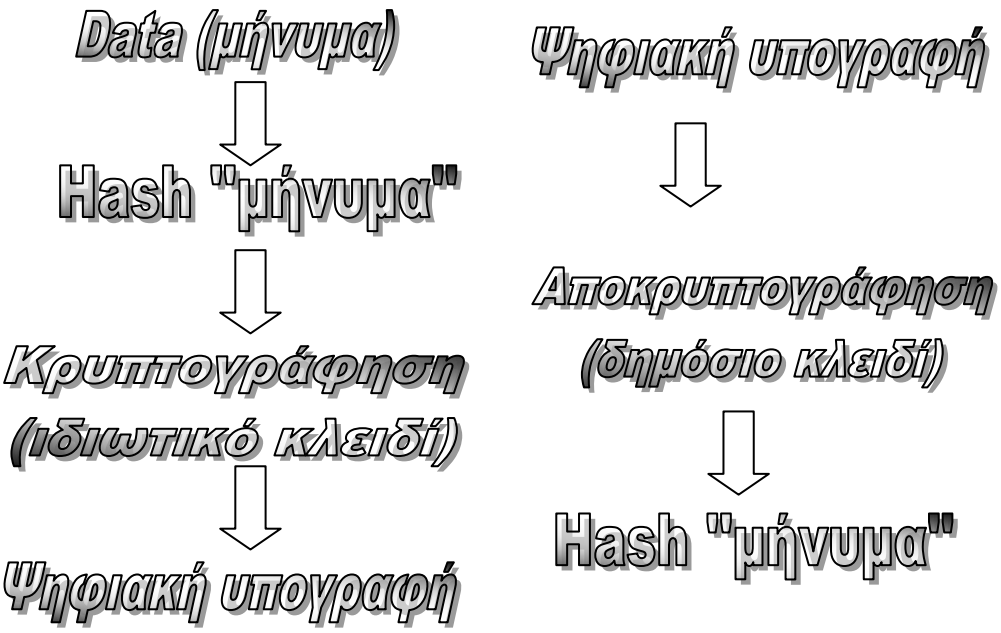
- Αλγόριθμος υπογραφών (Signature algorithm) : Έχοντας το ιδιωτικό κλειδί ενός χρήστη και ένα μήνημα παράγει την ψηφιακή υπογραφή του συγκεκριμένου χρήστη.

- Αλγόριθμος επαλήθευσης (Verification algorithm) : Αυτός ο αλγόριθμος έχοντας ένα μήνυμα, ένα ιδιωτικό κλειδί και μια υπογραφή μπορεί είτε να δεχτεί είτε να απορρίψει κάνοντας επαλήθευση των στοιχείων.

Μια ψηφιακή υπογραφή παρέχει επικύρωση (authentication) ενός μηνύματος, ακεραιότητα στοιχείων (data integrity), και μη αποκήρυξη (non-repudation) που σημαίνει ότι η επικύρωση ενός μηνύματος μπορεί να ελεγχθεί δημόσια και όχι μόνο από τον προοριζόμενο παραλήπτη. Τα μηνύματα αυτά μπορεί να είναι οτιδήποτε όπως για παράδειγμα ένα ηλεκτρονικό μήνυμα ή ακόμη και ένα μήνυμα που στέλνεται σε ένα περίπλοκο κρυπτογραφικό πρωτόκολλο. Ουσιαστικά μια ψηφιακή υπογραφή είναι ένας αριθμός εξαρτώμενος από κάποια μυστικά που βρίσκονται στο περιεχόμενο ενός μηνύματος και που μόνο ο υπογράφων γνωρίζει. Οι υπογραφές πρέπει να είναι επαληθεύσιμες σε διαφωνίες που προκύπτουν, όπως όταν ένας χρήστης υπογράψει ένα έγγραφο και κάποιος προσπαθήσει να αποκηρύξει/αμφισβητήσει την υπογραφή αυτή, τότε ένα αμερόληπτο τρίτο πρόσωπο πρέπει να είναι σε θέση να επιλύσει το θέμα δίκαια χωρίς απαίτηση πρόσβασης σε μυστικές πληροφορίες (private key) του υπογραφόμενου.

Η πιστοποίηση είναι ένας τρόπος για ένα τρίτο έμπιστο πρόσωπο (Certificate Authority, CA πιστοποιούσα αρχή) να δεσμεύσει την ταυτότητα ενός χρήστη με ένα δημόσιο κλειδί (public key) ώστε αργότερα άλλες οντότητες να μπορούν να επικυρώσουν ένα δημόσιο κλειδί χωρίς την βοήθεια ενός τρίτου εμπιστευόμενου προσώπου (CA).

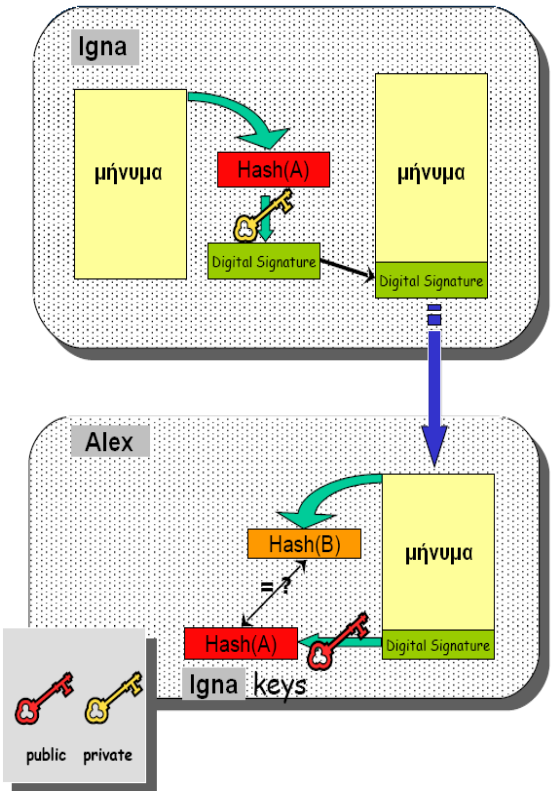
Οι ψηφιακές υπογραφές δημιουργούνται κρυπτογραφώντας ένα ‘’μήνυμα’’ (hash) των δεδομένων με το ιδιωτικό κλειδί (private key) ενός χρήστη. Το αποτέλεσμα του κρυπτογραφημένου μηνύματος είναι η ψηφιακή υπογραφή. Το συγκεκριμένο hash όμως μπορεί να αποκρυπτογραφηθεί **μόνο και μόνο** από το δημόσιο κλειδί (public key) του χρήστη.



Εικόνα 11:Ψηφιακή υπογραφή.

- ✓ Ο Ιγνάτιος (Igna) υπολογίζει το ‘’μήνυμα’’ (Hash A) του μηνύματος.
- ✓ Ο Igna κρυπτογραφεί το hash χρησιμοποιώντας το δικό του private key. Το κρυπτογραφημένο hash είναι η ψηφιακή υπογραφή (digital signature).
- ✓ Ο Igna στέλνει το μήνυμα στον Alex.

- ✓ Ο Alex υπολογίζει το ‘’μήνυμα’’ (hash B) του μηνύματος και το ελέγχει με το hash A, αποκωδικοποιώντας το με το δικό του public key.
- ✓ Αν τα δύο hash είναι ίσα τότε το μήνυμα δεν έχει τροποποιηθεί και άρα έχει γίνει ο αμοιβαίος έλεγχος ταυτότητας (mutual authentication).



Εικόνα 12:Ψηφιακή υπογραφή.

Βλέποντας την παραπάνω διαδικασία της ψηφιακής υπογραφής εύλογα αναρωτιέται κανείς ‘’πως ένας τυχαίος χρήστης έχει το σωστό public key του χρήστη με τον οποίο επιθυμεί να συνεργαστεί;‘’ Η απάντηση έρχεται από την ενότητα *Public Key Infrastructure* που ακολουθεί.

3.5 Public Key Infrastructure PKI

Στην κρυπτογραφία το PKI είναι μια ρύθμιση που συνδέει τα δημόσια κλειδιά με τις αντίστοιχες ταυτότητες χρηστών με την βοήθεια μιας πιστοποιούσας αρχής (certificate authority, CA). Η σύνδεση μεταξύ δημόσιων κλειδιών και ταυτοτήτων των χρηστών καθιερώνεται μέσω της εγγραφής και η διαδικασία έκδοσης μπορεί να πραγματοποιηθεί είτε από ένα λογισμικό μιας πιστοποιούσας αρχής CA είτε κάτω από ανθρώπινη επίβλεψη. Ο ρόλος του PKI που υλοποιεί την σύνδεση αυτή καλείται αρχή εγγραφής (*Registration Authority, RA*).

3.6 Middleware (μεσισμικό)

Το μεσισμικό είναι λογισμικό υλοποίησης υποδομών πλέγματος και εγκαθίσταται σε κόμβους με προεγκατεστημένο λειτουργικό σύστημα Linux. Αποτελείται από ένα σύνολο υπηρεσιών που επιτρέπουν στις πολλαπλές διαδικασίες να εκτελούνται σε μία ή περισσότερες μηχανές αλληλεπιδρώντας μέσω ενός δικτύου. Αυτή η τεχνολογία εξελίχθηκε για να παρέχει διαλειτουργικότητα υπέρ της κίνησης στις συνεπείς κατανεμημένες αρχιτεκτονικές, οι οποίες χρησιμοποιούνται για να υποστηρίξουν και να απλοποιήσουν τις σύνθετες διανεμημένες εφαρμογές. Το middleware ακολουθεί αρχές της σύγχρονης τεχνολογίας πληροφοριών και βασίζεται σε υπηρεσίες XML, SOAP,Web και αρχιτεκτονικές προσανατολισμού υπηρεσιών (architectures of orientation of services).

Οι υπηρεσίες μεσισμικού παρέχουν ένα πιο λειτουργικό σύνολο διεπαφών προγραμματισμού (programming interface) για να επιτρέψουν στην εφαρμογή να υλοποιεί τις παρακάτω ενέργειες:

- Να εντοπίσει μέσω του δικτύου και να παρέχει κατά συνέπεια στην αλληλεπίδραση με μια άλλη υπηρεσία ή
- Να είναι ανεξάρτητη από τις υπηρεσίες δικτύου
- Να είναι αξιόπιστη και διαθέσιμη πάντα όταν συγκρίνεται με το λειτουργικό σύστημα και τις υπηρεσίες δικτύου.

Το μεσισμικό είναι μια τεχνολογία λογισμικού που επιτρέπει την ολοκλήρωση της επιχειρηματικής εφαρμογής. Περιγράφει ειδικό λογισμικό που διασυνδέει δύο ή περισσότερες εφαρμογές λογισμικού και τους επιτρέπει να ανταλλάξουν στοιχεία ενώ εκτελούνται σε έναν εικονικό υπολογιστή όπως είναι το πλέγμα.
Το grid στηρίζεται σε αυτό το προηγμένο ‘’ενδιάμεσο‘’ λογισμικό που ονομάζεται μεσισμικό (middleware) που διασυνδέει τους πόρους και τις εφαρμογές.

Το μεσισμικό grid (middleware grid) παρέχει στους χρήστες ένα σύνολο από υπηρεσίες που φαίνονται παρακάτω:

- Βρίσκει κατάλληλες θέσεις για την εκτέλεση μιας εφαρμογής
- Βελτιστοποιεί την χρήση των πόρων
- Οργανώνει αποδοτική πρόσβαση στα δεδομένα
- Εξετάζει την πιστοποίηση (authentication) στις διαφορετικές διοικητικά κατανεμημένες περιοχές που χρησιμοποιούνται
- Πραγματοποιεί τις εργασίες ενώ ελέγχει την πρόοδο αυτών
- Μεταφέρει τα αποτελέσματα πίσω στον τελικό χρήστη

Το middleware έχει την ικανότητα να βρίσκει αυτόματα τα δεδομένα, τις ανάγκες των χρηστών και την υπολογιστική δύναμη για να τα αναλύσει. Επίσης ισορροπεί το φορτίο σε διαφορετικούς πόρους και χειρίζεται την ασφάλεια, την λογιστική και τον έλεγχο. Παραδείγματα μεσισμικού είναι ο Condor, LCG, Globus Toolkit.

3.7 Κλειδιά: ιδιωτικό και δημόσιο κλειδί (private and public key) Κωδικός πρόσβασης (pass phrase)

Στην κρυπτογραφία ένα κλειδί είναι μια πληροφορία, μια παράμετρος η οποία καθορίζει την λειτουργική παραγωγή ενός αλγόριθμου. Βέβαια ο αλγόριθμος αυτός δεν θα είχε κανένα αποτέλεσμα χωρίς την παρουσία του κλειδιού.

Κατά την μέθοδο της κρυπτογράφησης το κλειδί διευκρινίζει τον ιδιαίτερο μετασχηματισμό όπου το κομμάτι κρυπτογραφείται, και αντίστροφα αποκρυπτογραφείται κατά την μέθοδο της αποκρυπτογράφησης. Τα κλειδιά χρησιμοποιούνται και σε άλλους κρυπτογραφικούς αλγόριθμους όπως στην ψηφιακή υπογραφή (digital signature) και στους κώδικες επικύρωσης μηνυμάτων (Message Authentication Codes, MAC).

Η διαδικασία στην οποία χρησιμοποιούμε το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση είναι γνωστή και ως συμμετρική κρυπτογράφηση. Στην δεκαετία του 70’ ανακαλύφθηκε μια κατηγορία κρυπτογραφικών αλγορίθμων όπου χρησιμοποιούσαν ένα ζευγάρι κλειδιών, ένα για την κρυπτογράφηση και ένα για την αποκρυπτογράφηση. Αυτοί οι ασύμμετροι αλγόριθμοι αφήνουν το ένα κλειδί (*public key=δημόσιο κλειδί*) να βρίσκεται δημοσιοποιημένο και το άλλο (*private key=ιδιωτικό κλειδί)* πρέπει να βρίσκεται κρυμμένο μέσα στον υπολογιστή του χρήστη σε μια θέση που μόνο ο ίδιος γνωρίζει. Για την αποφυγή

υποκλοπής του ιδιωτικού κλειδιού, το αρχείο που το περιέχει κρυπτογραφείται μέσω ενός κωδικού πρόσβασης γνωστό και ως *pass phrase.*

Ένας πιστοποιημένος χρήστης του πλέγματος θα πρέπει να εισάγει τον κωδικό πρόσβασης (pass phrase) που απαιτείται για την αποκρυπτογράφηση του αρχείου που περιέχει το ιδιωτικό κλειδί. Πρωτότυπη είναι και η χρήση ‘’έξυπνων καρτών‘’ για την αποθήκευση των ιδιωτικών κλειδιών αντί στον σκληρό δίσκο ενός Η/Υ, που το καθιστά ακόμη πιο δύσκολο για άλλους να αποκτήσουν πρόσβαση στο αρχείο με το ιδιωτικό κλειδί.

Το δημόσιο κλειδί δεν χρειάζεται να φυλάσσεται μυστικά αλλά να είναι ευρέως διαθέσιμο για όλους. Το μόνο που απαιτείται είναι η επικύρωση (αυθεντικότητα) για να εγγυηθεί ότι ο χρήστης και κάτοχος ενός δημοσίου κλειδιού, είναι ο μόνος που κατέχει το αντίστοιχο ιδιωτικό κλειδί. Ένα πλεονέκτημα τέτοιων συστημάτων είναι ότι η παροχή αυθεντικών δημόσιων κλειδιών είναι ευκολότερη από την διανομή μυστικών κλειδιών με ασφάλεια. Επίσης ένα κλειδί μπορεί να θεωρηθεί σαν ένα σύνολο από bits όπου όσα περισσότερα bits τόσο πιο ισχυρό το κλειδί. Το μέγεθος εξαρτάται ανάλογα με τον αλγόριθμο κρυπτογράφησης, π.χ. ένα κλειδί μεγέθους 128 bits μπορεί να είναι μεγάλο για κάποιους αλγόριθμους ή μικρό για κάποιους άλλους.

3.8 Cryptography (κρυπτογραφία)

Ένα από τα πιο βασικά κομμάτια της υποδομής ασφάλειας του πλέγματος (GSI) είναι η κρυπτογραφία.

Κρυπτογραφία είναι η μελέτη μαθηματικών τεχνικών, σχετικών με την ασφάλεια δεδομένων όπως:

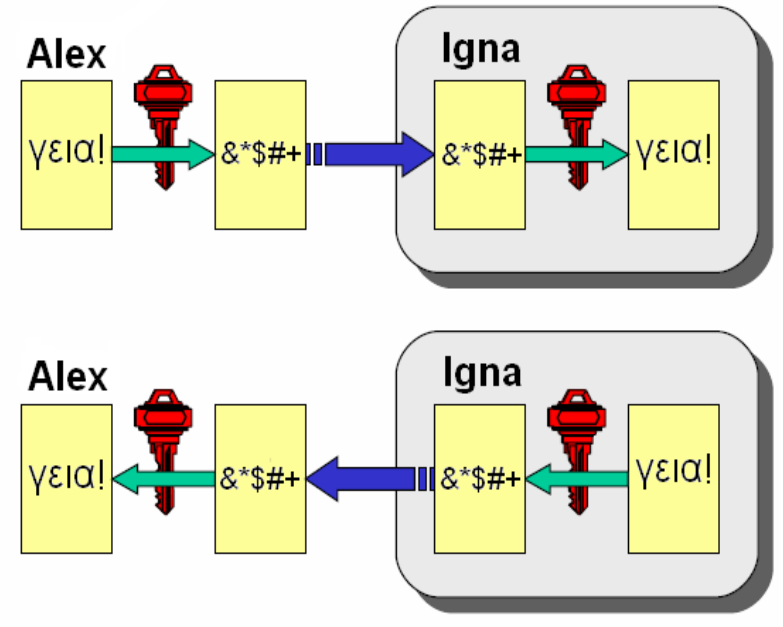
- ✓ εμπιστευτικότητα (confidentiality)
- ✓ ακεραιότητα στοιχείων (data integrity)
- ✓ πιστοποίηση οντοτήτων (entity authentication)
- ✓ και πιστοποίηση προέλευσης στοιχείων (data origin authentication).

Κατά την διαδικασία αυτή χρησιμοποιείται ένας μαθηματικός αλγόριθμος όπου με την βοήθεια κάποιων κλειδιών γίνεται η κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Υπάρχουν δύο είδη κρυπτογράφησης: η συμμετρική και η ασύμμετρη.

3.8.1Συμμετρική κρυπτογράφηση (symmetric encryption)

Η συμμετρική κρυπτογράφηση καλείται η διαδικασία στην οποία το ίδιο κλειδί χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση.
Κατά την διαδικασία της συμμετρικής κρυπτογράφησης ένα κλειδί χρησιμοποιείται για τον μηχανισμό της κρυπτογράφησης και αποκρυπτογράφησης όπως φαίνεται στην εικόνα.

Εικόνα 13:Συμμετρική κρυπτογράφηση.



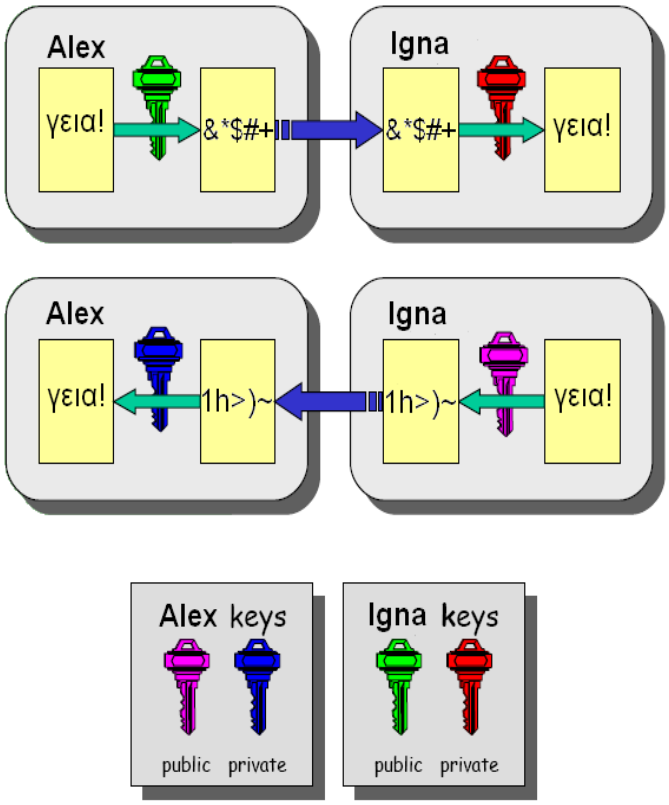
3.8.2Ασύμμετρη κρυπτογράφηση (asymmetric encryption)

Κατά την διαδικασία αυτή ο χρήστης έχει στην κατοχή του ένα ζευγάρι κλειδιών, το ιδιωτικό (private key) και το δημόσιο (public key) κλειδί. Το δημόσιο κλειδί καθορίζει τον μετασχηματισμό της κρυπτογράφησης και το αντίστοιχο ιδιωτικό κλειδί και μόνο αυτό, καθορίζει τον μετασχηματισμό της αποκρυπτογράφησης.

Παράδειγμα

Ο χρήστης Alex (Αλέξανδρος) επιθυμεί να επικοινωνήσει με τον Igna (Ιγνάτιος) στέλνοντας του ένα μήνυμα =**m**. Ο Alex λαμβάνει ένα αυθεντικό αντίγραφο του δημοσίου κλειδιού =**e** του Igna και το χρησιμοποιεί για τον μετασχηματισμό της κρυπτογράφησης =**Ee**. Στην συνέχεια ο Alex στέλνει το κρυπτογραφημένο μήνυμα **c=Ee(m)** στον χρήστη Α.

Ο Igna χρησιμοποιεί το ιδιωτικό του κλειδί =**d** για να αποκρυπτογραφήσει το **c** εφαρμόζοντας τον μετασχηματισμό αποκρυπτογράφησης =**Dd** ώστε να λάβει το αρχικό μήνυμα **m=Dd(c)**.



⇒ Ο χρήστης Alex κρυπτογραφεί ένα τυχαίο μήνυμα με το δημόσιο κλείδί του Ιγνάτιου (Igna) .

⇒ Ο Igna αποκρυπτογραφεί το μήνυμα με το δικό του ιδιωτικό κλειδί.

⇒ Με τον τρόπο αυτό εκτός του χρήστη Alex μόνο ο χρήστης Igna μπορεί να αποκρυπτογραφήσει το μήνυμα αυτό.

Εικόνα 14:Ασύμμετρη κρυπτογράφηση.

3.8.3Πλεονεκτήματα / μειονεκτήματα συμμετρικής και ασύμμετρης κρυπτογράφησης

Ο κύριος στόχος της ασύμμετρης κρυπτογράφησης είναι η παροχή μυστικότητας ή εμπιστευτικότητας. Δεδομένου ότι ο μετασχηματισμός κρυπτογράφησης του χρήστη Α είναι δημόσια γνώση, η συμμετρική κρυπτογράφηση δεν παρέχει επικύρωση προέλευσης και ακεραιότητας στοιχείων. Τέτοιες διαβεβαιώσεις παρέχονται μέσω χρήσης κάποιων πρόσθετων τεχνικών όπως π.χ. κωδικών επικύρωσης μηνυμάτων (Message Authentication Codes, MAC) και ψηφιακών υπογραφών (digital signatures).

Η ασύμμετρη κρυπτογράφηση είναι τυπικά πιο αργή σε σχέση με τους αλγόριθμους της συμμετρικής. Για τον λόγο αυτό η συμμετρική χρησιμοποιείται περισσότερο στην πράξη για μεταφορά κλειδιών που χρησιμοποιούνται στη συνέχεια για μαζική κρυπτογράφηση στοιχείων με την βοήθεια κάποιων συμμετρικών αλγόριθμων και εφαρμογών όπως επικύρωση και ακεραιότητα στοιχείων. Για παράδειγμα, κρυπτογράφηση μικρών στοιχείων όπως κωδικοί πιστωτικών καρτών και PINs.

Πλεονεκτήματα συμμετρικής κρυπτογράφησης

- Έχει μεγάλους ρυθμούς απόδοσης στοιχείων (ταχύτητα)
- Τα κλειδιά που χρησιμοποιούνται είναι σχετικά σύντομα (μικρού μεγέθους)
- Μπορεί να υιοθετηθεί σαν μια πρωταρχική δομή για κατασκευή διάφορων κρυπτογραφικών μηχανισμών όπως hash functions (λειτουργίες hash) και ψηφιακές υπογραφές (digital signatures)

Μειονεκτήματα συμμετρικής κρυπτογράφησης

- Σε μια επικοινωνία μεταξύ δύο ατόμων το κλειδί πρέπει να παραμείνει μυστικό και από τους δύο.
- Σε μεγάλα δίκτυα υπάρχουν πολλά ζευγάρια κλειδιών που πρέπει να ρυθμίζονται και συνεπώς η καλή διαχείριση απαιτεί την χρήση ενός άνευ όρων εμπιστευόμενου προσώπου (Unconditionally Trusted Parties)

- Μεταξύ μιας επικοινωνίας δύο χρηστών, σε τέτοιου είδους κρυπτογραφήσεις υπαγορεύεται ότι τα κλειδιά πρέπει να αλλάζουν συχνά, ίσως και σε κάθε σύνοδο επικοινωνίας.

- Στους μηχανισμούς ψηφιακής υπογραφής απαιτούνται τυπικά είτε η χρήση ενός τρίτου εμπιστευόμενου προσώπου είτε μεγάλα κλειδιά για δημόσια λειτουργία επαλήθευσης.

Πλεονεκτήματα ασύμμετρης κρυπτογράφησης

- Μόνο το ιδιωτικό κλειδί πρέπει να παραμείνει μυστικό και η αυθεντικότητα των δημοσίων κλειδιών πρέπει να εγγυάται.

- Η διαχείριση των κλειδιών σε ένα δίκτυο απαιτεί την παρουσία μόνο ενός λειτουργικά εμπιστευόμενου προσώπου (Functionality Trusted Parties) και όχι ενός άνευ όρων εμπιστευόμενου προσώπου.

- Ένα ζευγάρι κλειδιών (ιδιωτικό / δημόσιο) ενός χρήστη, ανάλογα με τον τρόπο χρήσης του μπορεί να παραμείνει αμετάβλητο ακόμα και μετά από πολλές συνόδους επικοινωνίας.

- Το κλειδί που χρησιμοποιείται για να περιγράψει την δημόσια λειτουργία επαλήθευσης είναι σχετικά πολύ μικρότερο από αυτό που χρησιμοποιείται στην συμμετρική κρυπτογράφηση.

- Σε ένα μεγάλο δίκτυο ο αριθμός των απαραίτητων κλειδιών μπορεί να είναι μικρότερος από ότι στην συμμετρική κρυπτογράφηση.

Μειονεκτήματα ασύμμετρης κρυπτογράφησης

- Οι ρυθμοί απόδοσης (ταχύτητα) είναι χαμηλότεροι σε σχέση με την συμμετρική.

- Τα μεγέθη των κλειδιών είναι πολύ μεγαλύτερα σε σχέση με αυτά της συμμετρικής.

4. Πρωτόκολλα και πιστοποιητικά

4.1 Πιστοποιούσα αρχή (Certificate authority, CA)

Η πιστοποιούσα αρχή είναι μια οντότητα η οποία παρέχει ψηφιακά πιστοποιητικά (digital certificates) στους χρήστες. Είναι ένα παράδειγμα ενός τρίτου εμπιστευόμενου προσώπου (Third Trusted Parties, TTP) το οποίο εμπιστεύονται απόλυτα οι χρήστες του πλέγματος.

Μια CA εκδίδει ψηφιακά πιστοποιητικά τα οποία περιέχουν ένα δημόσιο κλειδί (public key) και μια ταυτότητα του χρήστη. Ουσιαστικά επιβεβαιώνει ότι το δημόσιο κλειδί που περιλαμβάνεται στο πιστοποιητικό ανήκει στο πρόσωπο ή στον οργανισμό ή στον κεντρικό υπολογιστή (server) ή σε μια άλλη οντότητα η οποία αναφέρεται στο πιστοποιητικό.

Η υποχρέωση μιας CA σε τέτοια θέματα είναι να ελέγχουν και να επαληθεύουν τα πιστοποιητικά των υποψηφίων έτσι ώστε οι χρήστες και τα άλλα συμβαλλόμενα μέρη να μπορούν να εμπιστευθούν τις πληροφορίες που περιέχονται στο πιστοποιητικό. Η ταυτότητα ενός χρήστη πρέπει να είναι μοναδική για κάθε πιστοποιούσα αρχή CA.

Εάν ένας χρήστης εμπιστεύεται την CA και μπορεί να ελέγξει την υπογραφή της που φαίνεται στο πιστοποιητικό, έπειτα μπορεί να ελέγξει ότι ένα συγκεκριμένο δημόσιο κλειδί πράγματι ανήκει στο πρόσωπο το οποίο προσδιορίζεται στο πιστοποιητικό.

Μια CA έχει την δυνατότητα να υπογράψει η ίδια τα πιστοποιητικά της (self-signed).

Στην Ελλάδα υπεύθυνη πιστοποιούσα αρχή για την έκδοση πιστοποιητικών είναι η HellasGrid-CA που λειτουργεί και εδρεύει στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.

4.2 Αίτηση απόκτησης πιστοποιητικού (Certificate request)

Προκειμένου ένας χρήστης να αποκτήσει ένα ψηφιακό πιστοποιητικό πρέπει να χρησιμοποιήσει τις κατάλληλες εντολές στο User Interface UI. Κατά την διαδικασία αυτή παράγεται ένα ζευγάρι κρυπτογραφικών κλειδιών, ένα δημόσιο και ένα ιδιωτικό κλειδί καθώς και μια αίτηση πιστοποιητικού. Αφού αποκτήσει πρόσβαση στο User Interface UI ο χρήστης εισάγει την παρακάτω εντολή για την αίτηση πιστοποιητικού: **grid-cert-request-init.** Μετά από αυτό ο χρήστης εισάγει έναν κωδικό το λεγόμενο pass phrase για την προστασία του ιδιωτικού κλειδιού και συμπληρώνει την αίτηση πιστοποιητικού με προσωπικές πληροφορίες του. Με την ολοκλήρωση αυτού του βήματος δημιουργείται ένας κατάλογος ***.globus*** μέσα στον κατάλογο *$HOME* του Η/Υ του χρήστη. Μέσα σ'αυτόν τον κατάλογο παράγονται δύο αρχεία, *το userkey.pem* και το *user-cert-request.pem*

userkey.pem: αυτό το αρχείο περιέχει το ιδιωτικό κλειδί που είναι συνδεδεμένο με το πιστοποιητικό, το οποίο πρέπει να τεθεί υπό όρους έτσι ώστε η ανάγνωσή του να επιτρέπεται μόνο από τον ιδιοκτήτη. Στο ίδιο αρχείο περιέχεται και το pass phrase το οποίο ζητήθηκε νωρίτερα για την δημιουργία κλειδιών.

user-cert-request.pem: σ'αυτό το αρχείο περιέχεται το δημόσιο κλειδί , το όνομα του χρήστη και το όνομα της CA που το αντιπροσωπεύει. Το αρχείο αυτό αργότερα στέλνεται στην πιστοποιούσα αρχή η οποία μετά από την έγκριση και την υπογραφή της θα το επιστρέψει (συνήθως με αποστολή e-mail) στον χρήστη.

Το πιστοποιητικό για να χρησιμοποιηθεί στο δίκτυο πλέγματος θα πρέπει να είναι της μορφής *.pem*. Μετά την αποστολή του πιστοποιητικού από την CA, ο χρήστης το αποθηκεύει στον κατάλογο .globus με την ονομασία *usercert.pem.* Παρόλα αυτά ο χρήστης θα πρέπει να βεβαιώσει την αρχή επικύρωσης ότι όντως είναι αυτός που ισχυρίζεται ότι είναι και αυτό μπορεί να επιτευχθεί με την προσκόμιση της αστυνομικής ταυτότητας του χρήστη στην αρχή εγγραφής (Registration Authority, RA) όπως φαίνεται στο σχήμα απόκτησης πιστοποιητικού.

Παρακάτω φαίνεται η οθόνη προβολής για αίτηση πιστοποιητικού με την εντολή grid-cert-request-init στην πράξη:

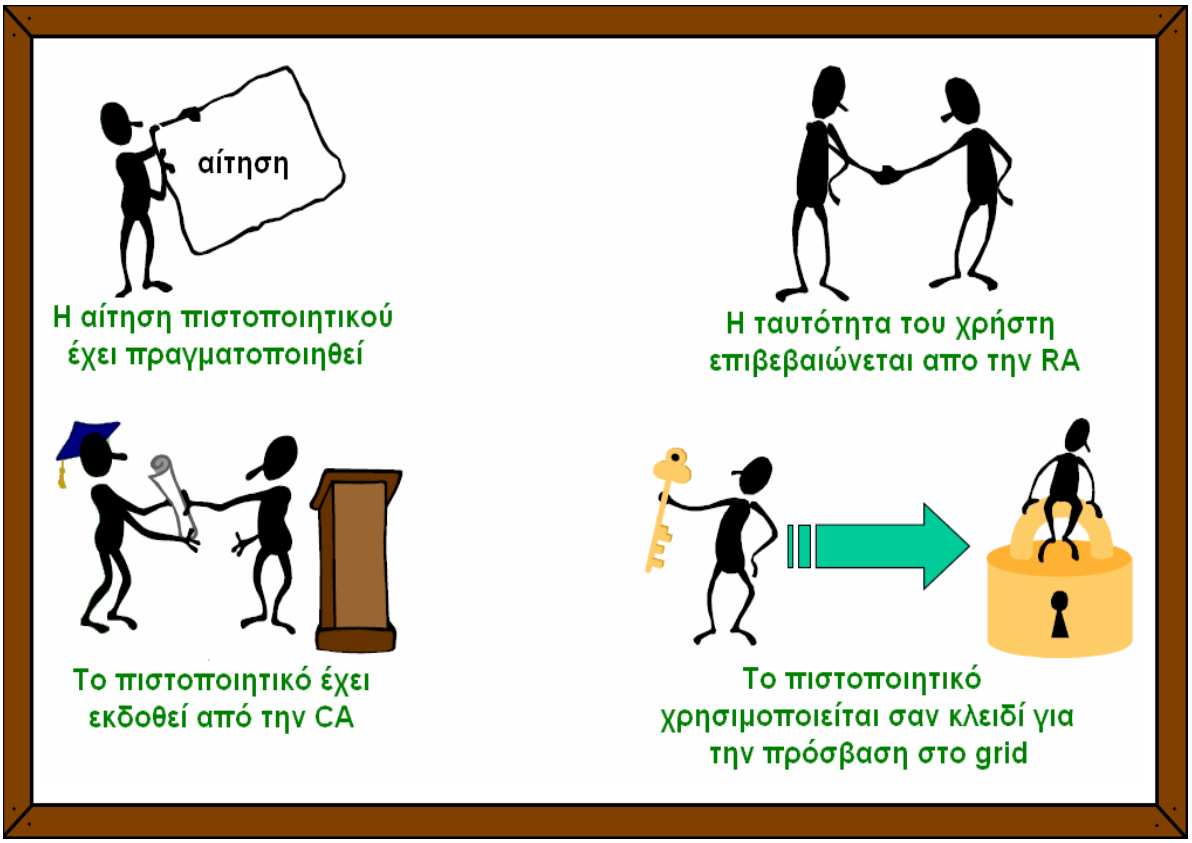
```
inanid@ui01  :~/.globus$ grid-cert-request
Enter your name, e.g., Ignatios Nanidis
A certificate request and private key is being created.
You will be asked to enter a PEM pass phrase.
This pass phrase is akin to your account password,
and is used to protect your key file.
If you forget your pass phrase, you will need to
obtain a new certificate.

/usr/local/globus/bin/grid-cert-request:
Using configuration from /etc/grid-security/globus-user-ssl.conf
Generating a 1024 bit RSA private key
............++++++
...++++++
writing new private key to '/home/inanid  /.globus/userkey.pem'
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
```

Εικόνα 15:Αίτηση απόκτησης πιστοποιητικού.

Για την ολοκλήρωση της διαδικασίας θα πρέπει ο χρήστης να στείλει στην CA ένα e-mail δείχνοντας την αποδοχή του για τις πολιτικές υπό τις οποίες

εκδόθηκε το πιστοποιητικό. Επίσης το ιδιωτικό κλειδί και το πιστοποιητικό τα οποία βρίσκονται στον κατάλογο .globus θα πρέπει να μορφοποιηθούν στο σύστημα από το οποίο ο χρήστης έστειλε το e-mail. Για να γίνει αυτό θα πρέπει τα δυο αυτά αρχεία που βρίσκονται στο .globus να μετατραπούν και να συνδυαστούν σε ένα ενιαίο αρχείο με την κατάληξη *.PKCS#12*.



Εικόνα 16:Διαδικασία απόκτησης πιστοποιητικού.

4.3 Digital Certificates (Ψηφιακά Πιστοποιητικά)

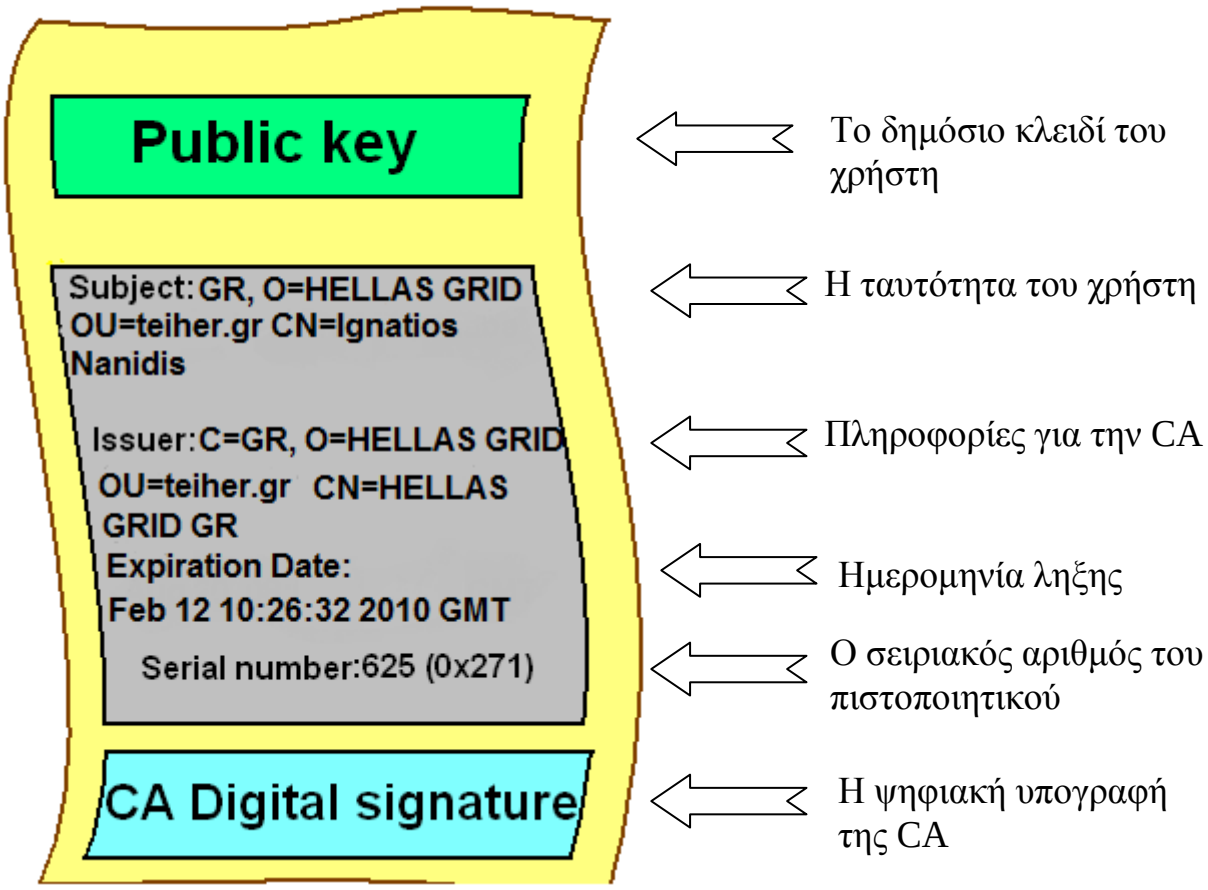
Τα πιστοποιητικά είναι ψηφιακά έγγραφα που ενσωματώνουν μια ψηφιακή υπογραφή για να δεσμεύσουν ένα δημόσιο κλειδί και μια ταυτότητα.

Ουσιαστικά πιστοποιούν ότι ένα ορισμένο δημόσιο κλειδί ανήκει σε έναν ιδιαίτερο χρήστη. Το κάθε πιστοποιητικό είναι μια μη παραποιήσιμη ηλεκτρονική ταυτότητα για την πρόσβαση στο περιβάλλον του πλέγματος, η οποία εκδίδεται και υπογράφεται από ένα τρίτο πρόσωπο που καλείται πιστοποιούσα αρχή (Certificate Authority, CA).

Το πιστοποιητικό αναγνωρίζει τον χρήστη ή την υπηρεσία και περιέχει πληροφορίες ζωτικής σημασίας για τον προσδιορισμό της ταυτότητάς τους.

Ένα πιστοποιητικό περιλαμβάνει:

- ένα όνομα το οποίο ταυτοποιεί τον χρήστη ή το αντικείμενο που το πιστοποιητικό αντιπροσωπεύει
- το δημόσιο κλειδί που αναφέρεται στο θέμα
- την ταυτότητα της CA που έχει υπογράψει το πιστοποιητικό και πιστοποιεί ότι το δημόσιο κλειδί και η ταυτότητα ανήκουν στον χρήστη που αναφέρεται στο θέμα
- την ψηφιακή υπογραφή της συγκεκριμένης CA
- την ημερομηνία λήξης πιστοποιητικού
- το serial number του πιστοποιητικού



Εικόνα 17:Ψηφιακό X509 με τα περιεχόμενα του.

Να σημειωθεί ότι ένα τρίτο πρόσωπο (CA) χρησιμοποιείται για να πιστοποιήσει το σύνδεσμο μεταξύ του δημόσιου κλειδιού και του θέματος του πιστοποιητικού. Η σχέση μεταξύ της CA και του πιστοποιητικού της πρέπει να καθορίζεται μέσω ενός μη-κρυπτογραφημένου μέσου, αλλιώς το σύστημα δεν είναι αξιόπιστο. Τα πιστοποιητικά του GSI είναι κωδικοποιημένα σε μορφή x.509, μια πρότυπη μορφή για πιστοποιητικά καθορισμένη από το Internet Engineering Task Force (IETF). Το πιστοποιητικό είναι της μορφής X.509 το οποίο είναι ένα ευρέως διαδεδομένο πρότυπο που έχει ένα ακριβές ιεραρχικό σύστημα από CAs για την έκδοση των πιστοποιητικών.

Τα πιστοποιητικά αυτά μπορούν να χρησιμοποιηθούν και από άλλα λογισμικά βασισμένα σε δημόσια κλειδιά (public key) συμπεριλαμβανομένων των εμπορικών περιηγητών ιστοχώρων από τη Microsoft και Netscape. Η κατοχή ενός ψηφιακού πιστοποιητικού από τον χρήστη 'Alex' είναι για να αποδείξει σε όλους ότι το δημόσιο κλειδί είναι πραγματικά δικό του και του επιτρέπει μια ασφαλή επικοινωνία με τον χρήστη 'Igna'.

4.3.1Πιστοποίηση μεταξύ δύο χρηστών (mutual authentication)

Αν δύο χρήστες έχουν πιστοποιητικά, και εμπιστεύονται τις CAs που τα υπέγραψαν, τότε οι δύο χρήστες μπορούν να αποδείξουν ο ένας στον άλλον ότι είναι αυτοί που ισχυρίζονται. Αυτό είναι γνωστό ως αμοιβαίος έλεγχος ταυτότητας (mutual authentication) .Το GSI χρησιμοποιεί το Secure Socket Layer (SSL) για το πρωτόκολλο του αμοιβαίου ελέγχου ταυτότητας ,το οποίο περιγράφεται παρακάτω. (το SSL είναι γνωστό και με ένα νέο, πρότυπο IETF όνομα: Transport Layer Security, TLS).

Για να μπορεί να γίνει ο αμοιβαίος έλεγχος ταυτότητας, οι εμπλεκόμενοι χρήστες πρέπει πρώτα να εμπιστευτούν τις πιστοποιούσες αρχές που υπέγραψαν το πιστοποιητικό του καθενός.

Για την αμοιβαία επικύρωση ο χρήστης (Α) δημιουργεί μια σύνδεση με έναν δεύτερο χρήστη (Β). Για να ξεκινήσει η διαδικασία επικύρωσης, ο Α στέλνει στον Β το πιστοποιητικό του. Το πιστοποιητικό λέει στον Β ποιος ισχυρίζεται ότι είναι ο Α, ποιο είναι το δημόσιο κλειδί του και ποια CA χρησιμοποιήθηκε για την έγκριση αυτού. Ο Β θα βεβαιωθεί πρώτα ότι το πιστοποιητικό του είναι έγκυρο, ελέγχοντας την ψηφιακή υπογραφή της CA για να σιγουρευτεί ότι όντως υπέγραψε το πιστοποιητικό και ότι δεν ήταν πλαστό.(Σε αυτό το σημείο πρέπει ο Β να εμπιστευτεί το CA που υπέγραψε το πιστοποιητικό του Α).

Μόλις ο Β ελέγξει το πιστοποιητικό του Α, πρέπει μετά να σιγουρευτεί ότι ο Α είναι αυτός που αναγνωρίστηκε στο πιστοποιητικό. Ο Β κρυπτογραφεί ένα τυχαίο μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Α και το στέλνει στον Α ζητώντας του να το αποκρυπτογραφήσει. Ο Α αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί και το στέλνει πίσω. Εάν το αποτέλεσμα είναι το αρχικό τυχαίο μήνυμα, τότε ο Β γνωρίζει ότι ο Α είναι αυτός που ισχυρίζεται. Τώρα που ο Β εμπιστεύεται την ταυτότητα του Α, η ίδια διαδικασία πρέπει να συμβεί αντίστροφα. Σε αυτό το σημείο, ο Α και ο Β έχουν δημιουργήσει μια σύνδεση μεταξύ τους και είναι βέβαιοι ότι γνωρίζουν ο ένας την ταυτότητα του αλλού. Ωστόσο για να πετύχει μια τέτοια διαδικασία όλοι οι χρήστες θα πρέπει να εμπιστεύονται τις πιστοποιούσες αρχές που υπέγραψαν τα ψηφιακά πιστοποιητικά.

4.3.2Λίστα εμπιστευόμενων αρχών πιστοποίησης

Αυτό το θέμα εμπιστοσύνης είναι στην κρίση των χρηστών, διότι δεν υπάρχουν κάποιοι αλγόριθμοι ή εφαρμογές που να αποφασίζουν αν μια CA είναι αξιόπιστη ή όχι. Όμως στο σύστημα χρησιμοποίησης του δημόσιου κλειδιού υπάρχει μία λίστα από εμπιστευόμενες πιστοποιούσες αρχές που περιλαμβάνει τις ψηφιακές υπογραφές συγκεκριμένων CAs που εμπιστεύονται οι χρήστες. Εν συνεχεία κάθε πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί αυτών των CAs και έτσι μπορούν οι χρήστες να ελέγχουν τις ψηφιακές υπογραφές. Αν και είναι στην κρίση των χρηστών ποιες πιστοποιούσες αρχές θα εμπιστευτούν, υπάρχουν κάποιες οι οποίες είναι αρκετά γνωστές και συμπεριλαμβάνονται εξ ορισμού σε πολλά συστήματα δημόσιου κλειδιού. (Για παράδειγμα πολλοί περιηγητές ιστοχώρων περιλαμβάνουν συνήθως τα πιστοποιητικά VeriSign και GlobalSign, επειδή πολλοί ιστοχώροι χρησιμοποιούν πιστοποιητικά που εκδίδονται από τις παραπάνω αρχές έτσι ώστε να επικυρώνονται σε αυτούς τους περιηγητές ιστοχώρων).

Εύλογα όμως αναρωτιέται ένας χρήστης ποιος υπέγραψε το πιστοποιητικό της πιστοποιούσας αρχής της οποίας εμπιστεύεται;

Η απάντηση είναι μια άλλη πιστοποιούσα αρχή.

Αυτό επιτρέπει την δημιουργία ιεραρχιών ανάμεσα στις πιστοποιούσες αρχές με τέτοιο τρόπο ώστε αν κάποιος χρήστης δεν εμπιστεύεται μια πιστοποιούσα αρχή '**X**' (η οποία δεν βρίσκεται στον κατάλογο του) αλλά μπορεί να εμπιστεύεται κάποια CA 'Y' ανώτερη, η οποία έχει υπογράψει το πιστοποιητικό της 'X' και άρα την καθιστά και αυτή έμπιστη για τον χρήστη.

4.3.3Κατάλογος ανάκλησης πιστοποιητικών (Certificate Revocation List)

Ένα πιστοποιητικό μπορεί να ανακληθεί αν ανακαλυφθεί ότι το ιδιωτικό κλειδί έχει υποκλαπεί ή εάν η σχέση που ενσωματώνεται στο πιστοποιητικό μεταξύ ενός δημοσίου κλειδιού και μιας οντότητας έχει αλλάξει ή είναι ανακριβής. Αυτό μπορεί να οφείλεται σε συχνή αλλαγή εργασιών ή ονομάτων από τον χρήστη.

Αν και η ανάκληση είναι σπάνιο φαινόμενο, τα πιστοποιητικά πρέπει πάντα να ελέγχονται. Ο έλεγχος αυτός γίνεται με την βοήθεια ενός καταλόγου ανάκλησης πιστοποιητικών (Certificate Revocation List, CRL) όπου εκεί βρίσκονται ακυρωμένα ή ανακλημένα πιστοποιητικά.

Η εξασφάλιση ότι ένας τέτοιος κατάλογος είναι ακριβής και ενημερωμένος είναι λειτουργία κάποιων πυρήνων που βρίσκονται σε κεντρικά PKI. Επίσης υπάρχει και η ''απευθείας σύνδεση σε πρωτόκολλα κατάστασης πιστοποιητικών'' (Online Certificate Status Protocols, OCSP). Εκεί

χρησιμοποιείται ένα κεντρικός υπολογιστής (server) για ανάλυση του CRL καταλόγου και επιστροφή της απάντησης στον πελάτη (χρήστη) χωρίς να χρειαστεί ο ίδιος να προβεί σε ανάκτηση και ερμηνεία του καταλόγου

4.4 Secure Socket Layer (SSL) & Transport Layer Security (TLS)

Το SSL καθώς και το TLS είναι κρυπτογραφικά πρωτόκολλα τα οποία παρέχουν ασφαλή επικοινωνία στο διαδίκτυο όπως π.χ. web browsing, emails κ.τ.λ. (SSL και TLS αν και με κάποιες μικρές διαφορές είναι ουσιαστικά τα ίδια).

Το SSL πρωτόκολλο επιτρέπει μια ασφαλή επικοινωνία μέσω ενός δικτύου και σκοπό έχει να αποτρέψει κάποιον να κρυφακούσει ή να επηρεάσει ή να παραποιήσει μηνύματα. Παρέχει πιστοποίηση μεταξύ των δύο άκρων και ιδιαίτερη επικοινωνία μέσω του διαδικτύου χρησιμοποιώντας την μέθοδο της κρυπτογραφίας. Συγκεκριμένα μόνο ο κεντρικός υπολογιστής (server) πιστοποιείται ενώ ο πελάτης όχι, που σημαίνει ότι ο χρήστης που είναι είτε ένα άτομο είτε μια εφαρμογή είτε ένας web browser μπορεί να είναι βέβαιος με ποιον επικοινωνεί. Το επόμενο ανώτερο επίπεδο ασφαλείας είναι και οι δύο άκρες να είναι σίγουρες με ποιον επικοινωνούν κάτι που επιτυγχάνεται με τον αμοιβαίο έλεγχο ταυτότητας (mutual authentication).

Λειτουργία

Ένας SSL πελάτης (χρήστης) και ένας server διαπραγματεύονται μια σύνδεση μεταξύ τους χρησιμοποιώντας μια μέθοδο ‘’χειραψίας‘’ (handshake). Κατά την διαδικασία αυτή πελάτης και server συμφωνούν σε διάφορες παραμέτρους που χρησιμοποιούνται για να καθιερωθεί μια ασφαλής επικοινωνία.

Η διαδικασία ξεκινάει όταν ένας πελάτης συνδεθεί με ένα διαθέσιμο SSL-server ζητώντας ασφαλή σύνδεση και παρουσιάζει ένα κατάλογο από κρυπτογραφήματα και hash λειτουργίες. Από αυτή την λίστα ο server επιλέγει το πιο ισχυρό κρυπτογράφημα και hash λειτουργία τα οποία υποστηρίζουν και ειδοποιούν τον πελάτη για την απόφαση.

Ο server στέλνει ένα ψηφιακό πιστοποιητικό με στοιχεία που τον αφορούν όπως το όνομα του server, όνομα της CA που υπέγραψε το πιστοποιητικό και το δημόσιο κλειδί του server. Ο πελάτης κρυπτογραφεί ένα τυχαίο αριθμό χρησιμοποιώντας το δημόσιο κλειδί του server και το στέλνει σ'αυτόν. Με τη σειρά του ο server αποκρυπτογραφεί χρησιμοποιώντας το δικό του ιδιωτικό κλειδί. Αυτό γίνεται και αντίστροφα για επικύρωση του πελάτη. Αυτή είναι μια διαδικασία χειραψίας (handshake) η οποία είναι ουσιαστικά ένας αμοιβαίος έλεγχος ταυτότητας (mutual authentication).

4.4.1 OpenSSL

Το openSSL είναι μια εφαρμογή πρωτοκόλλου του SSL. Η βιβλιοθήκη πυρήνων (γραμμένη σε γλώσσα προγραμματισμού C) εφαρμόζει βασικές κρυπτογραφικές λειτουργίες και παρέχει διάφορες λειτουργίες χρησιμότητας. Η χρήση της βιβλιοθήκης του openSSL επιτρέπεται σε διάφορες γλώσσες υπολογιστών που είναι διαθέσιμες.

Το openSSL υποστηρίζει και ένα αριθμό διαφορετικών κρυπτογραφικών αλγόριθμων όπως:

- κρυπτογραφήματα: DES,IDEA,RC2,RC4,Blowfish
- κρυπτογραφικές λειτουργίες hash : MD5,MD2,SHA

- κρυπτογραφήσεις δημοσίων κλειδιών: RSA,DSA

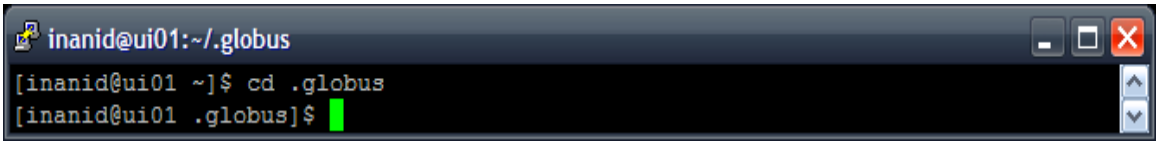
Με την βοήθεια της εργαλειοθήκης του openSSL και παρεχόμενων εντολών μπορούμε να δημιουργήσουμε, να ελέγξουμε και να μετατρέψουμε διαφορετικά είδη αρχείων καθώς και να διαχειριστούμε τα αρχεία των πιστοποιητικών.

Παραδείγματα εντολών

- **openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -outcert.p12:** μετατροπή του πιστοποιητικού από μορφή αρχείου .pem (Grid) σε .pkcs12 (Web browser certificate format)
- **openssl pkcs12 -nocerts -in cert.12 -out userkey.pem:** μετατροπή του πιστοποιητικού από μορφή αρχείου .pkcs12 (web browser certificate format) σε .pem (Grid).
- **openssl x509 -noout -in usercert.pem -issuer:** με αυτή την εντολή φαίνεται μόνο ο εκδότης του πιστοποιητικού.

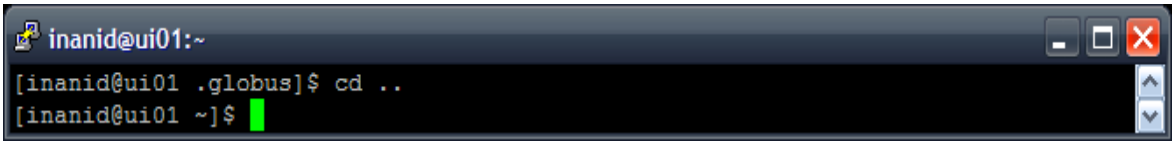
Εικόνα 18:openssl x509 –noout –in usercert.pem –issuer

ΠΡΟΣΟΧΗ ! ! !
Οι εντολές όπως η *openssl x509 -noout -in usercert.pem –issuer* που εμφανίζει τον εκδότη του πιστοποιητικού και περιέχει το αρχείο usercert.pem χρειάζονται ιδιαίτερη μεταχείριση. Για την ολοκλήρωση της είναι απαραίτητο ο χρήστης να εισέλθει πρώτα στον κατάλογο *.globus* με την εντολή **cd .globus**



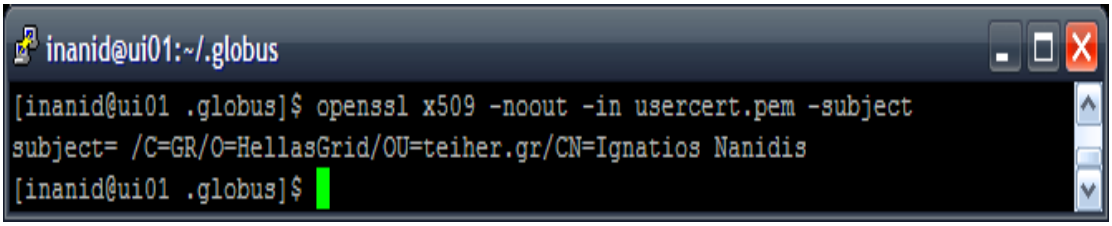
Εικόνα 19:cd .globus

και έπειτα να πληκτρολογήσει την εντολή που χρειάζεται για τον εκδότη του πιστοποιητικού. Χωρίς αυτή την μικρή λεπτομέρεια το αρχείο *usercert.pem* που ζητείται από την εντολή είναι αδύνατο να βρεθεί διότι βρίσκεται μέσα στον κατάλογο *.globus* γι'αυτό και απαιτείται να ανοίξουμε τον κατάλογο αυτό σε πρώτη φάση.
Για να βγούμε από τον κατάλογο *.globus* πληκτρολογούμε την εντολή **cd ..** όπως φαίνεται παρακάτω:



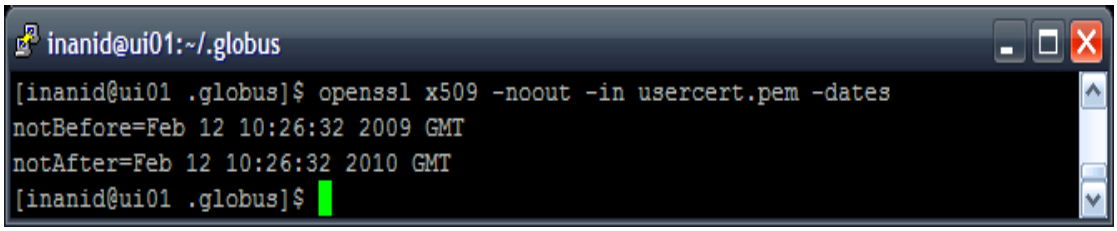
Εικόνα 20:cd ..

- **openssl x509 -noout -in usercert.pem -subject:** το όνομα του θέματος.



Εικόνα 21:openssl x509 –noout –in usercert.pem -subject

- **openssl x509 -noout -in usercert.pem -dates:** η περίοδος εγκυρότητας.

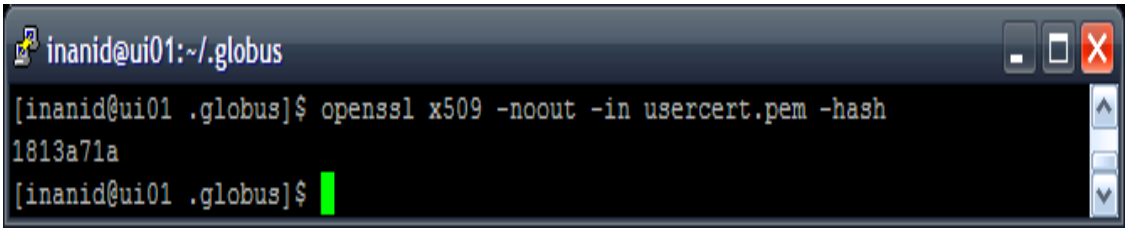


Εικόνα 22:openssl x509 –noout –in usercert.pem -dates

- **openssl x509 -noout -in usercert.pem -issuer -subject -dates:**
  δυνατότητα ενός χρήστη να δει το όνομα του θέματος, τον εκδότη και την περίοδο εγκυρότητας του πιστοποιητικού.

Εικόνα 23:openssl x509 –noout –in usercert.pem –issuer –subject -dates

- **openssl x509 -noout -in usercert.pem -hash:** η hash αξία ενός πιστοποιητικού.



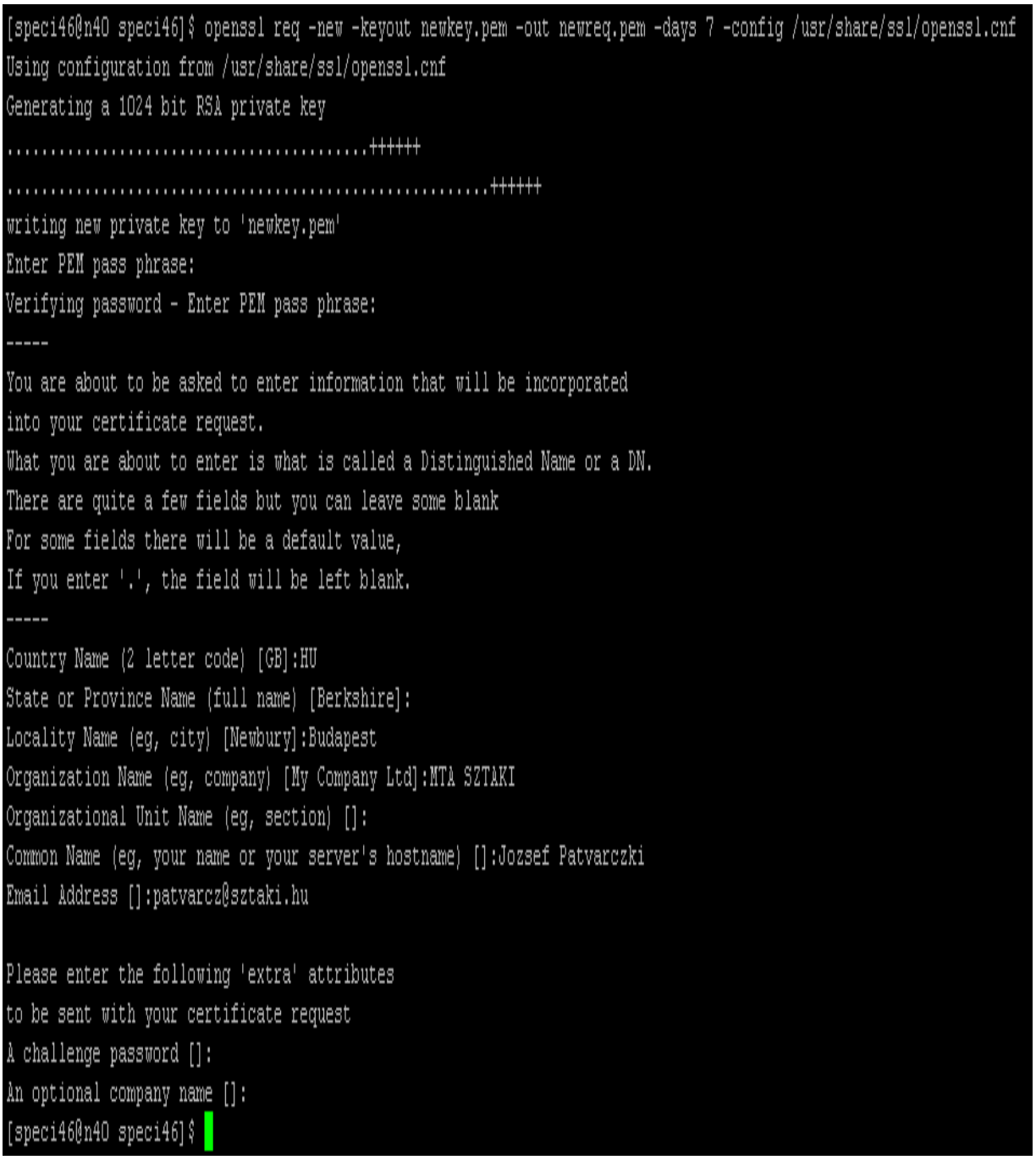
Εικόνα 24:openssl –noout –in usercert.pem -hash

- **openssl req -in newreq.pem -noout -verify -key userkey.pem –config:** έλεγχος του private key από τον χρήστη.

Επίσης υπάρχει η δυνατότητα αίτησης πιστοποιητικού από έναν χρήστη με την βοήθεια του openssl, εισάγοντας στον User Interface την εντολή :

Openssl req -new -keyout newkey.pem -out new req.pem -day 7- config

Μετά την εισαγωγή της παραπάνω εντολής εμφανίζεται η οθόνη προβολής για την αίτηση του πιστοποιητικού με την βοήθεια του openssl όπως φαίνεται παρακάτω:



Εικόνα 25:Αίτηση πιστοποιητικού με τη βοήθεια του Openssl

Κατά την διαδικασία αυτή δημιουργούνται κάποιες διεργασίες οι οποίες είναι:

→ δημιουργία RSA (ή DES) ιδιωτικού κλειδιού

→ προτρέπεται ο χρήστης να εισάγει το pass phrase του

→ αφού γίνει η επικύρωση ζητούνται στοιχεία που αφορούν τον χρήστη όπως το όνομα του, όνομα χώρας, επαρχίας, τοποθεσίας, οργανισμού που ανήκει ο χρήστης, διεύθυνση email κ.τ.λ.

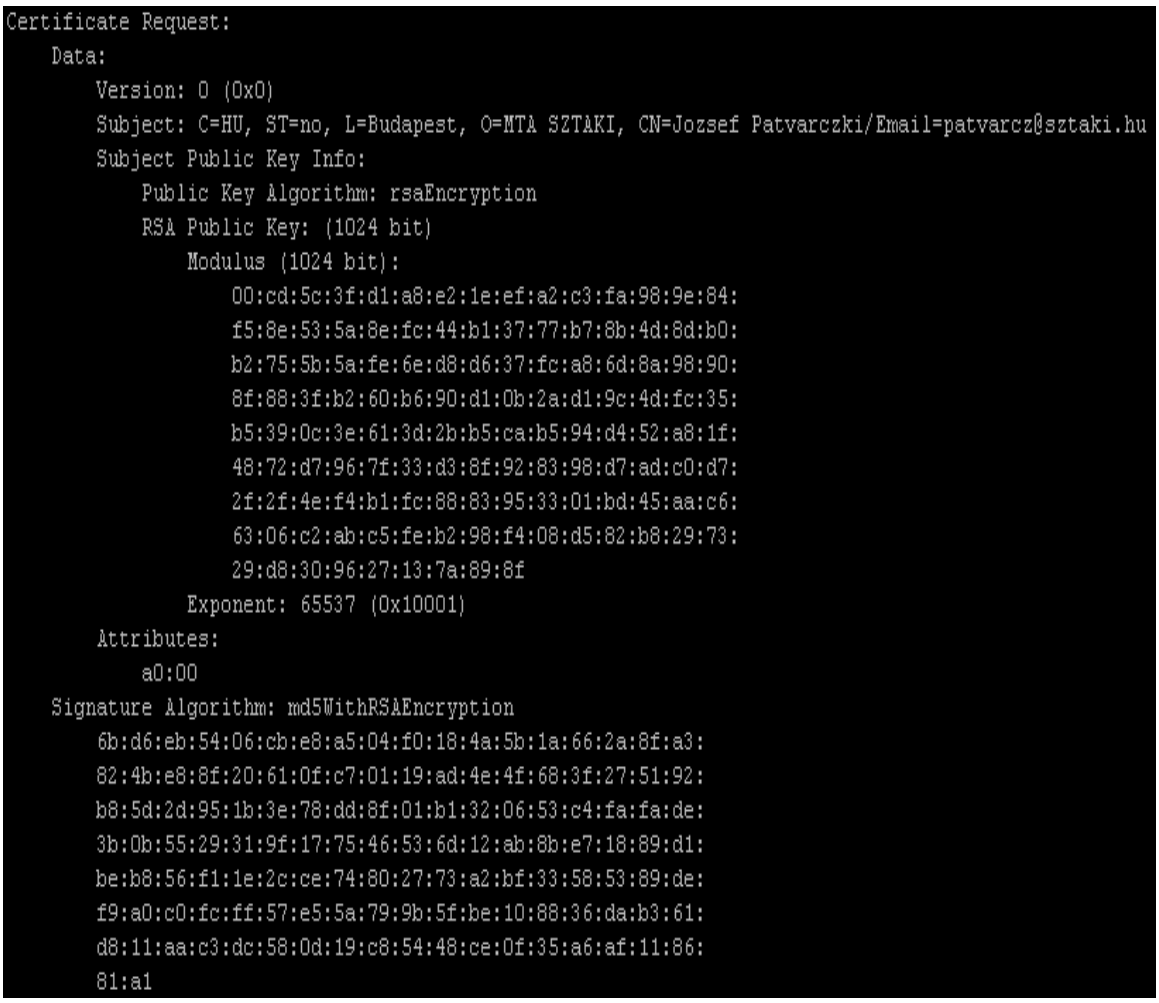
→ μετά την συμπλήρωση των στοιχείων η αίτηση είναι έτοιμη για αποστολή

Εικόνα 26:Η μορφή της αίτησης σε μη αναγνώσιμη μορφή.

Για τον λόγο ότι η αίτηση του πιστοποιητικού έχει την μορφή που φαίνεται στην παραπάνω εικόνα προβολής, ο χρήστης έχει την δυνατότητα μετατροπής της αίτησης σε αναγνώσιμο κείμενο με τις παρακάτω ενέργειες:

- κάνοντας login σε ένα User Interface
- cd .globus
- εισάγοντας την εντολή **openssl req -in newreq.pem -noout -text -config**

Αφού ο χρήστης εκτελέσει τις παραπάνω εντολές εμφανίζεται η ακόλουθη οθόνη προβολής:



Εικόνα 27:Πληροφορίες της αίτησης πιστοποιητικού.

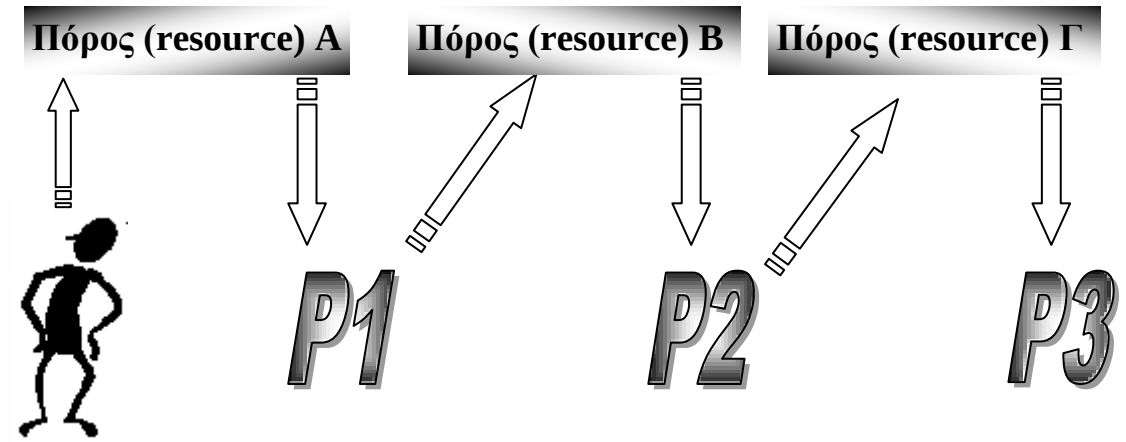
4.4.2Delegation and single sign on

Το GSI παρέχει μια σειρά από δυνατότητες για την ευκολότερη και καλύτερη δυνατή πρόσβαση ενός χρήστη στο περιβάλλον του πλέγματος. Μια προέκταση του πρωτοκόλλου SSL (Service Socket Layer) μειώνει τον αριθμό εισαγωγών του pass phrase από τον χρήστη κάθε φορά που εισέρχεται στο πλέγμα.

Αν κάποιος χρήστης εκτελεί μια εργασία ή έναν υπολογισμό στο Grid και απαιτείται αμοιβαία επικύρωση (mutual authentication) για καθένα από τους πολλαπλούς πόρους που χρησιμοποιούνται ή αν υπάρχουν τοπικοί ή μακρινοί πράκτορες που ζητούν υπηρεσίες εξ ονόματος ενός χρήστη τότε μπορεί να

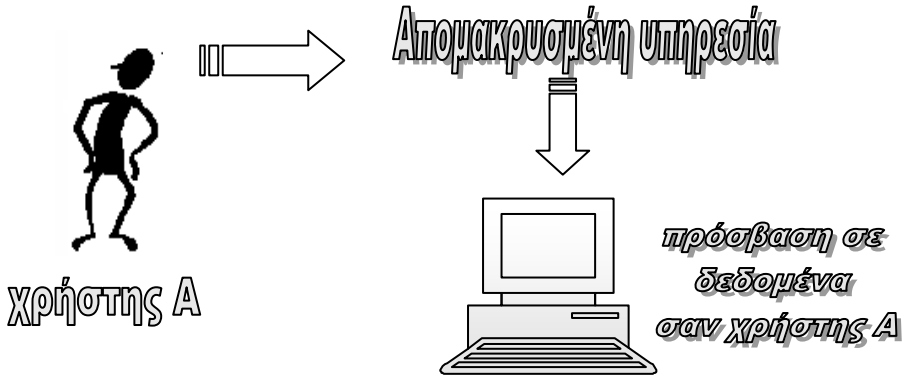
αποφευχθεί η συνεχής καταγραφή του pass phrase από τον χρήστη. Αυτό επιτυγχάνεται με την δημιουργία ενός πληρεξούσιου πιστοποιητικού (proxy certificate).

Single sign-on: Δεν χρειάζεται η συνεχής εισαγωγή κωδικών από τον χρήστη όταν χρησιμοποιεί πολλαπλούς πόρους.



Εικόνα 28:Single sign-on (αυτό-εγγραφή).

Delegation: Ένας χρήστης δημιουργεί ένα προσωρινής διάρκειας πιστοποιητικό (proxy) και δίνει την δυνατότητα σε μία άλλη οντότητα για να ενεργεί για λογαριασμό του χρήστη.

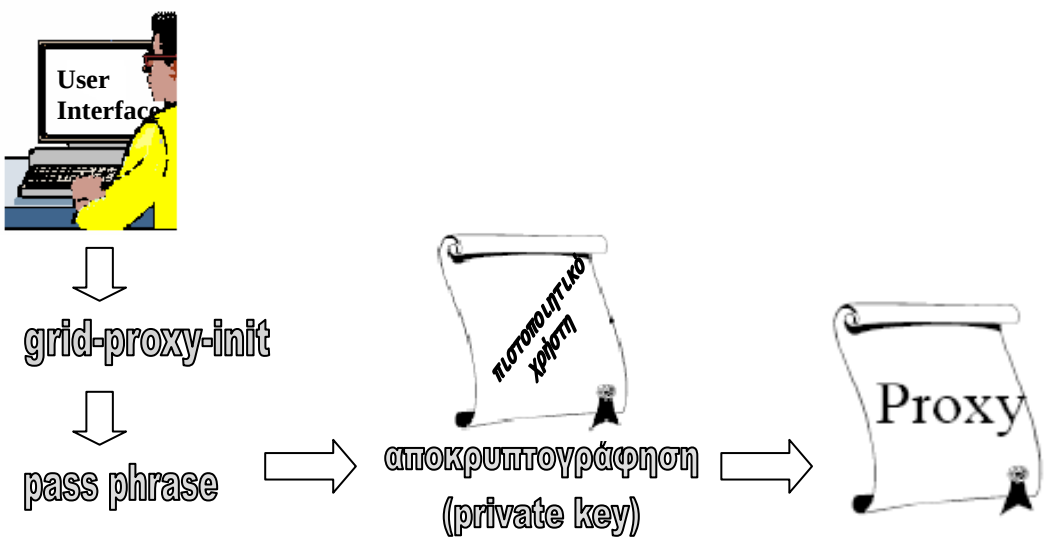


Εικόνα 29:Delegation (αντιπροσώπευση)

4.5 ***Proxy certificate (πληρεξούσιο πιστοποιητικό)***

Ένα πληρεξούσιο (proxy) είναι ένα εξουσιοδοτημένο πιστοποιητικό το οποίο επικυρώνει τον χρήστη σε κάθε ασφαλή επικοινωνία. Χρησιμοποιείται συχνά σε συστήματα ασφαλείας όταν μια οντότητα επιθυμεί να χορηγήσει σε μια άλλη οντότητα μερικά από τα προνόμιά της. Επίσης υποστηρίζονται και κάποια σημαντικά χαρακτηριστικά όπως αντιπροσώπευση (delegation) και αμοιβαίος έλεγχος ταυτότητας (mutual authentication).

Για την δημιουργία ενός πιστοποιητικού proxy απαιτείται η πρόσβαση σε έναν User Interface από έναν χρήστη και η εισαγωγή της εντολής: **grid-proxy-init**
Μετά από αυτό ζητείται από τον χρήστη να εισάγει το pass phrase για την αποκρυπτογράφηση του ιδιωτικού του κλειδιού το οποίο χρησιμοποιείται για την υπογραφή του proxy πιστοποιητικού από τον ίδιο τον χρήστη και όχι από κάποια CA. (Το ιδιωτικό κλειδί του χρήστη δεν εκτίθεται μετά την υπογραφή του proxy).



Εικόνα 30:Διαδικασία απόκτησης πληρεξούσιου πιστοποιητικού (proxy).

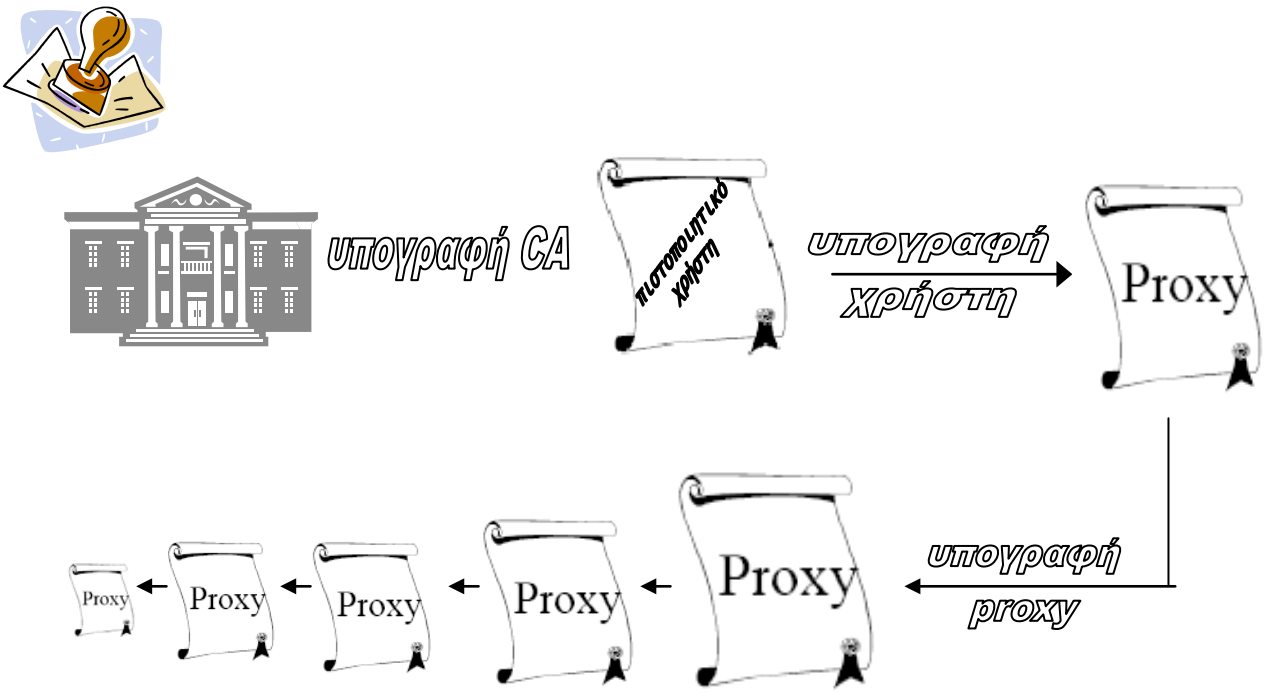
Έτσι δημιουργείται το proxy πιστοποιητικό το οποίο περιέχει δικό του δημόσιο και ιδιωτικό κλειδί (public & private key).

Επίσης περιέχει και την ταυτότητα του ιδιοκτήτη η οποία είναι ελαφρώς τροποποιημένη δείχνοντας ότι πρόκειται για πληρεξούσιο (proxy). Σαν ένα επιπλέον μέτρο ασφάλειας το proxy έχει περιορισμένο χρόνο εγκυρότητας, συνήθως 12 ώρες (με δυνατότητα αλλαγής χρονικού περιθωρίου από τον χρήστη).

Το ιδιωτικό κλειδί του proxy δεν κρυπτογραφείται σε κάποιο μυστικό αρχείο. Αποθηκεύεται απλά σε ένα τοπικό αρχείο εφόσον ο χρόνος εγκυρότητας του είναι περιορισμένος. Μετά την δημιουργία και αποθήκευση του πληρεξούσιου με το αντίστοιχο ιδιωτικό κλειδί, μπορούν να χρησιμοποιηθούν από τον χρήστη για αμοιβαίο έλεγχο ταυτότητας (mutual authentication). Όμως με την δημιουργία ενός proxy ο αμοιβαίος έλεγχος ταυτότητας διαφέρει ελαφρώς.

4.5.1 Αμοιβαίος έλεγχος ταυτότητας με την κατοχή ενός proxy πιστοποιητικού

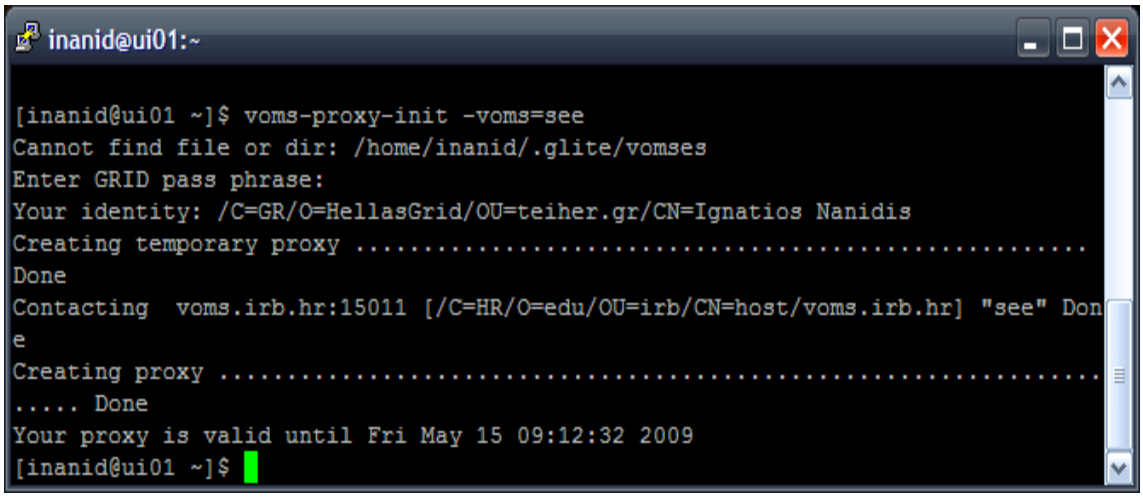
Ο απομακρυσμένος χρήστης λαμβάνει το proxy πιστοποιητικό υπογεγραμμένο από τον ιδιοκτήτη καθώς επίσης και το ψηφιακό πιστοποιητικό του ιδιοκτήτη. Το δημόσιο κλειδί του ιδιοκτήτη που λήφθηκε με το ψηφιακό πιστοποιητικό του χρησιμοποιείται για την επικύρωση της υπογραφής του στο proxy πιστοποιητικό. Έπειτα το δημόσιο κλειδί της CA χρησιμοποιείται για την επικύρωση της υπογραφής της στο ψηφιακό πιστοποιητικό του χρήστη. Έτσι δημιουργείται μια αλυσίδα εμπιστοσύνης από την CA στον χρήστη και έπειτα στο proxy.



Εικόνα 31:Επικύρωση υπογραφής.

Εντολές proxy certificate

- **voms-proxy-init --voms see:** δίνεται η εντολή στον virtual organization (see) για την δημιουργία του proxy.



Εικόνα 32:voms-proxy-init –voms=see

ΠΡΟΣΟΧΗ !!!!!

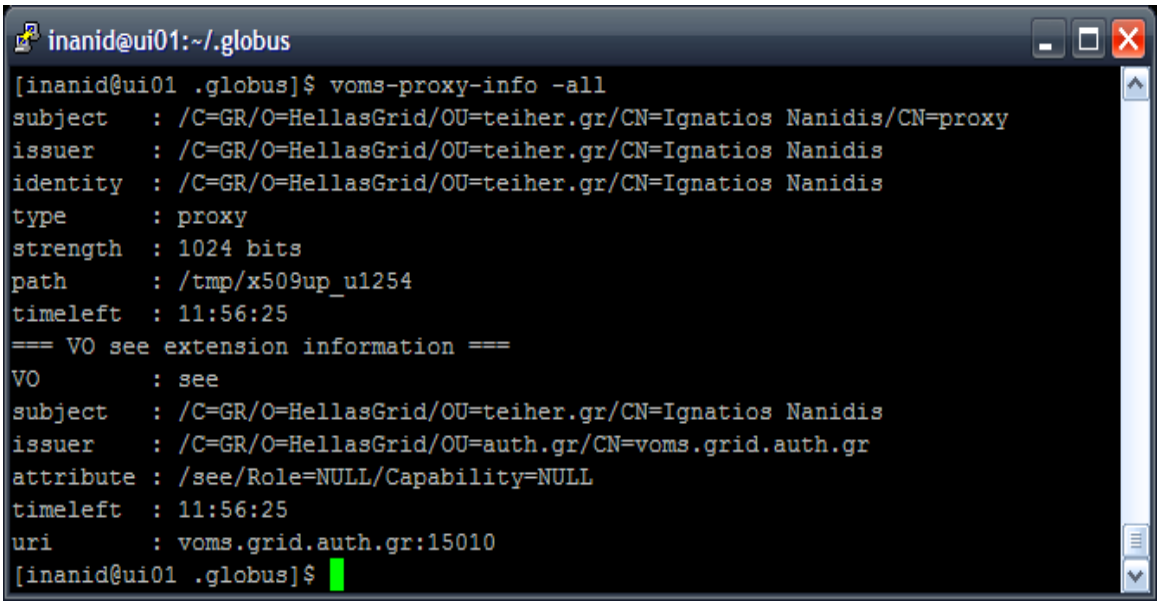
Με την εντολή *voms-proxy-init –voms=see* δημιουργείται το πληρεξούσιο και δηλώνεται και ο εικονικός οργανισμός στον οποίο ανήκει ο χρήστης παρέχοντας περισσότερη ασφάλεια. Ενώ με την εντολή *grid-proxy-init* εισέρχεται στο γενικότερο δίκτυο του grid απροστάτευτος με εντονότερο τον κίνδυνο υποκλοπής των στοιχείων / πληροφοριών του.

- **voms-proxy-init --voms see-hours 24:** προσδιορίζεται ο χρόνος εγκυρότητας του proxy σε 24 ώρες.

- **voms-proxy-init --voms see-bits 512:** προσδιορίζεται το μέγεθος του κλειδιού του πιστοποιητικού.

- **voms-proxy-init --voms see-status:** δίνει πληροφορίες για την κατάσταση της δουλειάς που έχουμε αναθέσει.

- **voms-proxy-info –all:** με την εντολή αυτή δίνονται πληροφορίες σχετικές με το proxy.



Εικόνα 33:voms-proxy-info -all

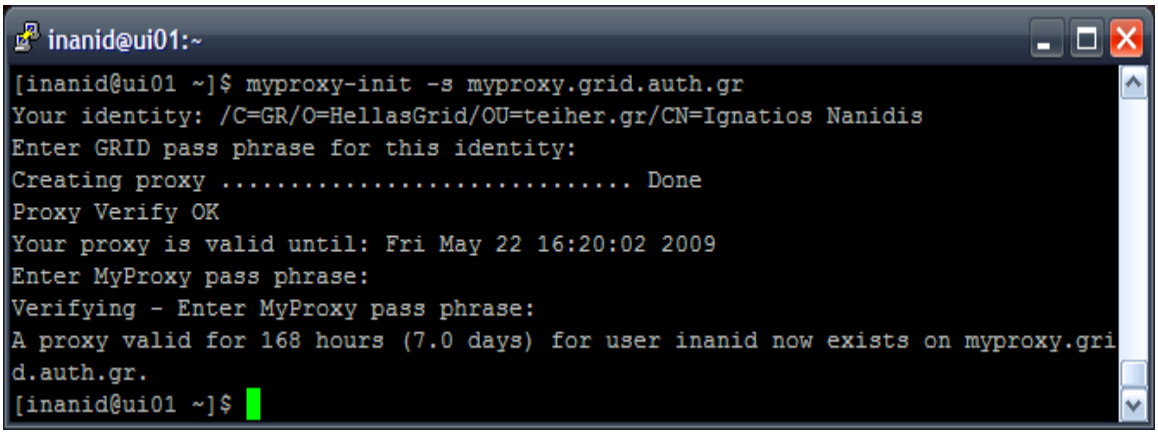
- **voms-proxy-destroy:** με την εντολή αυτή καταστρέφεται το proxy certificate, και χρησιμοποιείται μόνο για την έξοδο από το δίκτυο του grid.

4.6 Long term proxy -MyProxy-

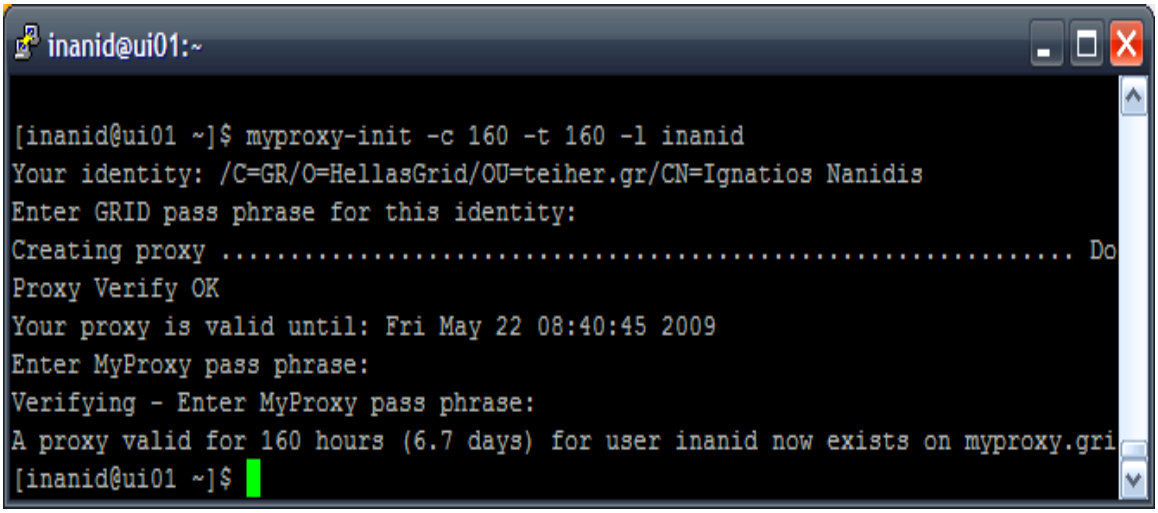
Το proxy έχει περιορισμένο χρόνο εγκυρότητας συνήθως 12 ώρες και θα υπήρχε μεγάλο ρίσκο δημιουργώντας ένα proxy για περισσότερο χρόνο διότι θα υπήρχε κίνδυνος υποκλοπής του. Και αυτό επειδή το ιδιωτικό κλειδί του proxy δεν κρυπτογραφείται σε κάποιο κωδικοποιημένο αρχείο αλλά απλά αποθηκεύεται σε ένα τοπικό αρχείο του Η/Υ του χρήστη.

Υπάρχουν κάποιες εργασίες στο πλέγμα που χρειάζονται αρκετό χρόνο για την διεκπεραίωσή τους και υπάρχει περίπτωση να λήξει το proxy πιστοποιητικό πριν τελειώσει η εργασία, προκαλώντας αποτυχία εκτέλεσης της εργασίας και σφάλματα πιστοποίησης για όλες τις μετέπειτα αιτήσεις πρόσβασης στην υπηρεσία ή τον πόρο. Για την αποφυγή τέτοιων καταστάσεων η υπηρεσία διαχείρισης φόρτου εργασίας (Workload Management Service, WMS) επιτρέπει στον χρήστη την δημιουργία ενός μακροπρόθεσμου πληρεξούσιου (long term proxy) γνωστό και ως ‘’MyProxy‘’ το οποίο έχει χρόνο εγκυρότητας (σε μόνιμη κατάσταση) 168 ώρες = 1 εβδομάδα. Η εντολή με την οποία δημιουργείται το MyProxy είναι:

Myproxy –init –s myproxy.grid.auth.gr (όνομα server)



Εικόνα 34:Δημιουργία μακροπρόθεσμου πληρεξούσιου.



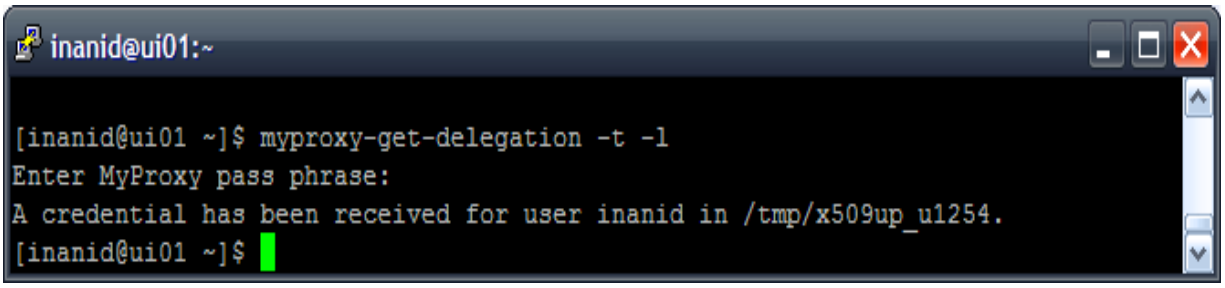
Εικόνα 35:Δημιουργία μακροπρόθεσμου πληρεξούσιου με την επιλογή ωρών εγκυρότητας.

Από την παραπάνω εντολή (εικ.26) φαίνεται η δυνατότητα επιλογής διάρκειας εγκυρότητας του MyProxy (ώρες). Επίσης υπάρχει δυνατότητα ανανέωσης του MyProxy από τον χρήστη. Κάτι τέτοιο χρειάζεται σε περίπτωση μακροπρόθεσμων εργασιών χωρίς αποτυχία διεκπεραίωσης τους.

Η ανανέωση είναι ουσιαστικά μια δημιουργία ενός νέου MyProxy αφού χρησιμοποιείται η ίδια εντολή: MyProxy –init –s –t

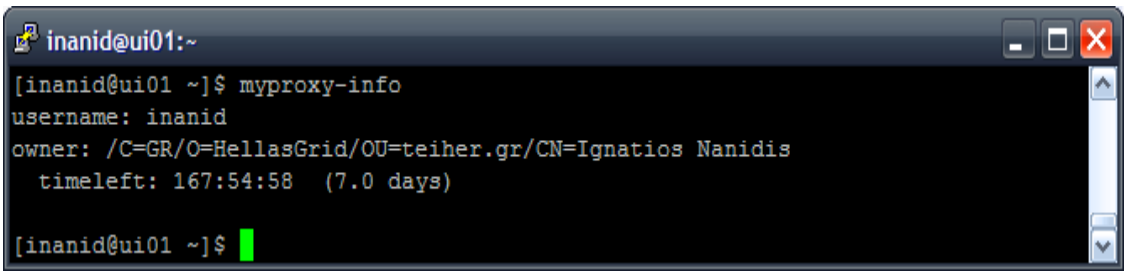
Όπου –s το hostname του MyProxy server και –t ο χρόνος εγκυρότητας σε ώρες. Μια σημαντική ικανότητα που παρέχει το MyProxy είναι η δημιουργία αντιπροσώπευσης (delegation). Επιτρέπει σε έναν χρήστη την πρόσβαση σε έναν User Interface χωρίς την ανάγκη προσωπικών πιστοποιητικών και κρυπτογραφημένων αρχείων. Η εντολή για την δημιουργίας αντιπροσωπείας είναι:

myproxy -get -delegation -t (ώρες) **-l** (όνομα χρήστη)



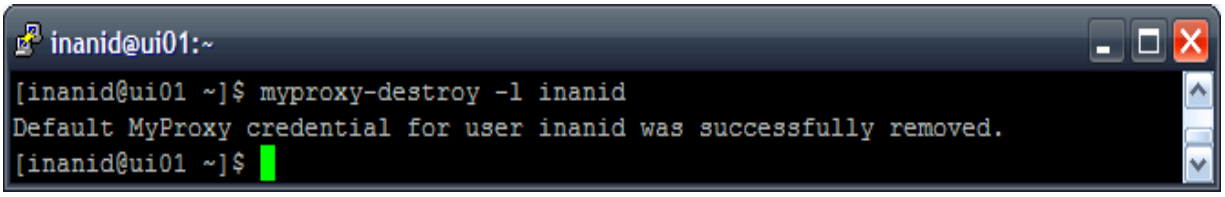
Εικόνα 36:Δημιουργία αντιπροσώπευσης (delegation).

myproxy –info: Για την ανάκτηση πληροφοριών σχετικές με το MyProxy (όνομα, ιδιοκτήτη, υπολειπόμενο χρόνο εγκυρότητας)



Εικόνα 37:Πληροφορίες του μακροπρόθεσμου πληρεξούσιου.

myproxy –destroy –s: Για καταστροφή και μετακίνηση του πιστοποιητικού MyProxy από τον κεντρικό υπολογιστή MyProxy server.



Εικόνα 38:Ακύρωση του MyProxy.

4.6.1Ανανέωση πληρεξούσιου (Proxy Renewal)

Η υπηρεσία Resource Broker έχει μια σημαντική εφαρμογή που καλείται *Proxy Renewal (ανανέωση πληρεξούσιου*). Αυτή η υπό-υπηρεσία έχει την ευθύνη να ανανεώνει τα πληρεξούσια κοντά στον χρόνο λήξης, τα οποία χρησιμοποιούνται στην υποβολή εργασιών που εκτελούνται αυτή την περίοδο. Λίγα λεπτά πριν την λήξη του proxy, η Resource Broker έρχεται σε επαφή με τον MyProxy server και ζητάει την ανανέωση του πιστοποιητικού.

5. Η υποδομή του HellasGrid

Η υποδομή του HellasGrid αποτελείται 6 υπολογιστικές συστοιχίες με συνολική ισχύ 768 CPUs (384-dual) καθώς και πάνω από 90 TB αποθηκευτικού χώρου, 30 με τη μορφή δίσκων και 60 με τη μορφή βιβλιοθηκών ταινιών (tape libraries). Οι συστοιχίες που αποτελούν τους κόμβους του πλέγματος θα φιλοξενηθούν σε τρία ιδρύματα στην Αθήνα, δύο στην Θεσσαλονίκη, ένα στην Πάτρα και ένα στο Ηράκλειο Κρήτης (εικόνα 29).

Η υπολογιστική ισχύς και οι αποθηκευτικοί πόροι μοιράζονται μεταξύ όλων των χρηστών του HellasGrid ανεξάρτητα αν βρίσκονται μέσα ή έξω από τα ιδρύματα που φιλοξενούν τους πόρους με τις κοινές πολιτικές πρόσβασης για όλους τους χρήστες. Η πολιτική αυτή προστατεύεται από την ομάδα της GRNET που εδρεύει στο Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ)

Η εγκατάσταση των συστοιχιών έχει λάβει χώρα σε δύο φάσεις:
Στην πρώτη φάση η υποδομή HellasGrid αποτελείται από τον κόμβο **HG-01-GRNET** που καλείται *Isabella* με

- 34 Dual CPU συστήματα στα 2.8GHz, 1GB RAM, 2x70GB HDD, 2x Gbit
- ολοκληρωμένο σύστημα IBM FAStT900 storage area network
- 2x Redundant Fiber Channel Controllers με 1GB Cache ο καθένας
- 70x146.8=10,276 TB raw storage capability
- Tape Library με δυνατότητα έως 30TB με ενσωματωμένο έλεγχο.

Η συγκεκριμένη φάση έχει ολοκληρωθεί από την IBM τον Δεκέμβριο του 2004.

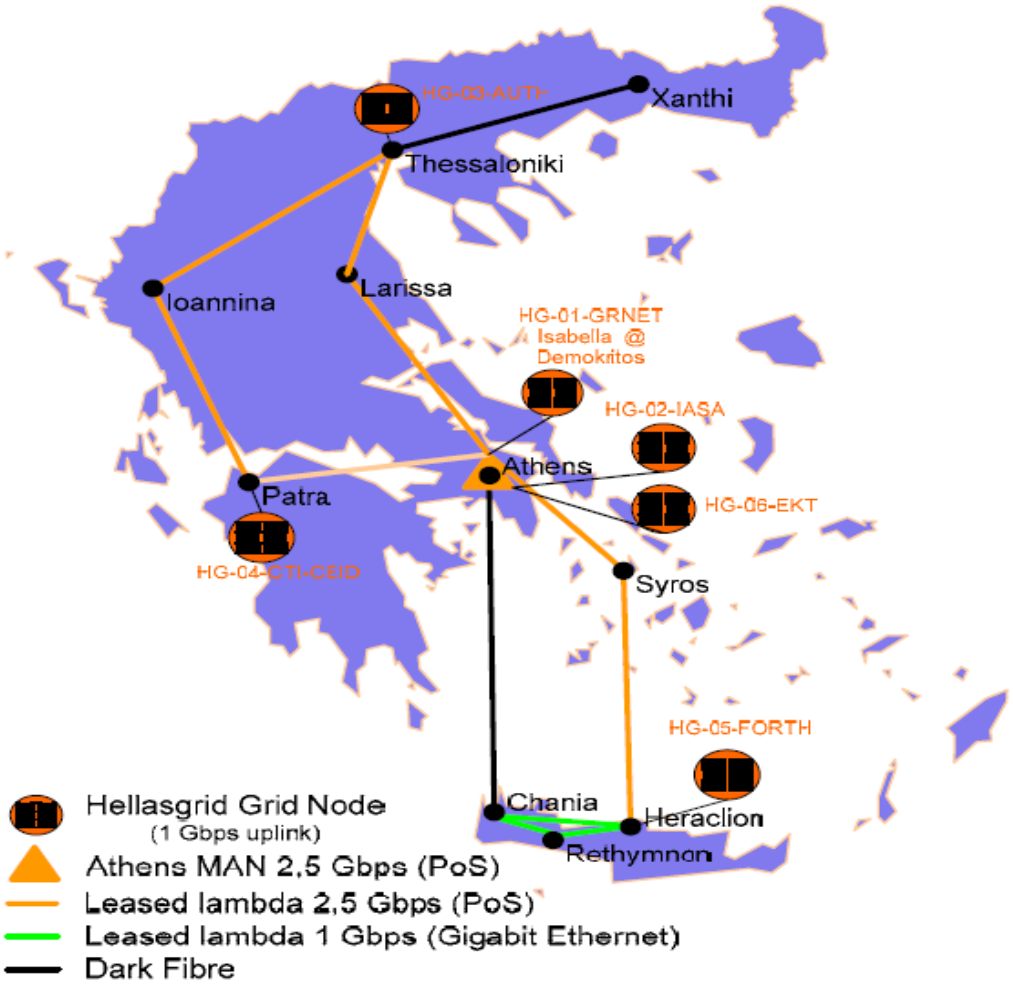
Στην δεύτερη φάση αναπτύχθηκαν πέντε ακόμη κόμβοι λειτουργίας όπου στόχος είναι η οργάνωση, ο συντονισμός και η οργάνωση κεντρικών λειτουργιών και υπηρεσιών που είναι απαραίτητες για την ομαλή λειτουργία της υποδομής πλέγματος. Η εγκατάσταση εξοπλισμού των κόμβων πραγματοποιήθηκε ως εξής:

HG-01-GRNET:	Επέκταση του υπάρχοντος κόμβου του ΕΔΕΤ στο ΕΚΕΦΕ Δημόκριτος: Συστοιχία με 32 Dual CPUs, 10 TB SAN Storage, 10 TB Tape Storage.
HG-02-IASA:	Στο Ινστιτούτο Επιταχυντικών Συστημάτων και Εφαρμογών (ΙΕΣΕ) - που στεγάζεται στο Εθνικό Καποδιστριακό Πανεπιστήμιο Αθηνών: Συστοιχία με 66 Dual CPUs Servers, 4,2TB SAN Storage.
HG-03-AUTH:	Στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης: Συστοιχία με 64 Dual CPUs Servers, 4TB SAN Storage.
HG-04-CTI-CEID:	Στο Ερευνητικό Ακαδημαϊκό Ινστιτούτο Τεχνολογίας Υπολογιστών (ΕΑ-ΙΤΥ) στην Πάτρα: Συστοιχία με 64 Dual CPUs Servers, 4 TB SAN Storage.
HG-05-FORTH:	Στο Ίδρυμα Τεχνολογίας και Έρευνας (ΙΤΕ) στο Ηράκλειο Κρήτης: Συστοιχία με 64 Dual CPUs Servers, 4,2TB SAN Storage.
HG-06-EKT:	Στο Εθνικό Κέντρο Τεκμηρίωσης: Συστοιχία με 128 Dual CPUs Servers, 12 TB SAN Storage.

Όλοι οι κόμβοι του HellasGrid είναι ενσωματωμένοι με το περιφερειακό κέντρο διαδικασιών της νοτιανατολικής Ευρώπης (SEE ROC) και με την πανευρωπαϊκή υποδομή υπολογιστικού πλέγματος του EGEE. Επίσης έχει εγκατεστημένη την τελευταία έκδοση ενδιάμεσου λογισμικού GLite (v3.0.2 as of 2006/Q3) και κάθε συστοιχία προσφέρει υπηρεσίες υπολογιστικού πλέγματος όπως Computing Element (CE) για την προσφορά υπολογιστικής ισχύος, Storage Element (SE) για την προσφορά αποθηκευτικού χώρου και Monitoring Element (MON) για την παρακολούθηση των παραπάνω υπηρεσιών και την παροχή στατιστικών.

Το περιφερειακό κέντρο διαδικασιών (SEE ROC) σε συνεργασία με το HellasGrid προσφέρει επίσης και τις παρακάτω υπηρεσίες πλέγματος όπως:

- Πιστοποιούσα αρχή (CA)
- Υπηρεσία MyProxy
- Υπηρεσία διαχείρησης εικονικού οργανισμού (VOMS)
- Μεσίτες των πόρων (RB)
- Υπηρεσία διαχείρησης φόρτου εργασίας (WMS)
- Κατάλογος αρχείων (LFC)



Εικόνα 39:Η υποδομή του HellasGrid. (Ιανουάριος 2010).

Το HellasGrid είναι η μεγαλύτερη υποδομή πλέγματος στη νοτιοανατολική Ευρώπη την οποία διαχειρίζεται η ΕΔΕΤ, προς όφελος των ελληνικών ερευνητικών και εκπαιδευτικών κοινοτήτων , και μια από τις σταθερότερες υποδομές στο ευρωπαϊκό επίπεδο. Η υποδομή HellasGrid είναι πλήρως ενσωματωμένη στην πανευρωπαϊκή υποδομή πλέγματος EGEE, προσφέροντας περισσότερους από 40,000 κεντρικούς επεξεργαστές και 10 PetaBytes αποθηκευτικού χώρου.

Οι πόροι της υποδομής είναι ελληνικοί ερευνητές που χρησιμοποιούνται και από τα ευρωπαϊκά προγράμματα. Κατά τη διάρκεια των τελευταίων ετών ένας σημαντικός και αυξανόμενος αριθμός χρηστών από τους διάφορους επιστημονικούς τομείς (φυσική, βιοτεχνολογία, χημεία υπολογισμού, τεχνολογία πληροφοριών, μετεωρολογία κ.λπ.) χρησιμοποιεί την υποδομή HellasGrid για τις ανάγκες υπολογισμού τους. Αυτή η υποδομή διατίθεται δωρεάν στις ευρωπαϊκές ερευνητικές και ακαδημαϊκές κοινότητες για την εφαρμογή των καθημερινών τους αναγκών και προγραμμάτων.

Η υποδομή HellasGrid προσαρμόζεται συνεχώς και αντιστοιχεί στα αιτήματα των χρηστών της, ενώ η επέκταση των προσφερθέντων πόρων της έχει οργανωθεί έτσι ώστε οι πρόσθετες ανάγκες υπολογισμού που προκύπτουν μέσα στα επόμενα έτη θα είναι σε θέση να καλυφθούν.

6. Πηγές αναφοράς

- http://en.wikipedia.org/wiki/Application_programming_interface
- http://en.wikipedia.org/wiki/Middleware
- https://twiki.cern.ch/twiki/bin/view/EGEE/DECHFirstJobs#User_Interface_UI
- http://webmaster.iu.edu/tool_guide_info/webserve_putty.shtml
- http://egee.itep.ru/User_Guide.html#SECTION00052300000000000000
- http://egee.itep.ru/User_Guide.html#SECTION00067000000000000000
- http://egee-uig.web.cern.ch/egee-uig/production_pages/ProxyRenewal.html
- http://grid006.mporzio.astro.it/job_submission.html
- http://wiki.gsi.de/cgi-bin/view/Grid/DigitalCertificates#Digital_certificates
- http://www.globus.org/security/public-key-cryptography.html
- http://www.globus.org/security/overview.html
- http://www.grid.auth.gr/pki/seegrid-ca/documents/certificateImport/InternetExplorer.php
- http://security.ncsa.uiuc.edu/research/grid-howtos/usefulopenssl.php
- www.csl.ee.upatras.gr/egee/files/Enter%20the%20Grid.pdf
- www.globus.org/alliance/publications/papers/anatomy.pdf
- http://en.wikipedia.org/wiki/Transmission_Control_Protocol
- http://www.nordugrid.org/
- www.bioinfogrid.eu/project-events/.../11_dms-architecture-2006-en.pdf
- http://docs.huihoo.com/globus/gt3-tutorial/ch10s04.html
- http://en.wikipedia.org/wiki/User_interface
- http://www.globus.org
- http://www.glite.org
- http://www.globus.org/security/GSI3/GT3-Security-HPDC.pdf