ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ & ΔΙΚΤΥΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Για την απόκτηση διπλώματος του άνωθεν τμήματος

ΠΑΠΑΔΟΠΟΥΛΟΣ Χ. ΝΙΚΟΛΑΟΣ

ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΠΛΕΓΜΑΤΟΣ

ΕΠΙΒΑΕΠΟΝΤΕΣ ΚΑΘΗΓΗΤΕΣ:

ΧΟΥΣΤΗΣ ΗΛΙΑΣ – ΗΛΙΟΥΔΗΣ ΧΡΗΣΤΟΣ

ΒΟΛΟΣ , ΣΕΠΤΕΜΒΡΙΟΣ 2005

ΠΡΟΛΟΓΟΣ ΚΑΙ ΕΥΧΑΡΙΣΤΙΕΣ

Η συγκεκριμένη διπλωματική εργασία αποτελεί το επιστέγασμα μιας σκληρής δουλειάς που έλαβε χώρα στο πανεπιστήμιο, σε μια όμορφη πόλη τον Βόλο.
Η πραγματοποίηση αυτού μου του ονείρου, είναι δώρο Θεού, και αγαπημένων προσώπων.
Η πορεία αυτά τα χρόνια ήταν γεμάτη δυσκολίες και επιτυχίες, προκλήσεις αλλά και στιγμές ανταμοιβής των κόπων μου. Στην προσπάθειά μου αυτή είχα δίπλα μου ανθρώπους που με στήριξαν , με βοήθησαν και με ενέπνευσαν.
Θέλω λοιπόν να ευχαριστήσω τους επιβλέποντες καθηγητές μου τον κ. Χούστη Ηλία και τον κ. Ηλιούδη Χρήστο, οι οποίοι εκτός από λαμπροί και αναγνωρισμένοι επιστήμονες, είναι θαυμάσιοι άνθρωποι με ήθος, και αγάπη για το αντικείμενό τους. Τους ευχαριστώ που ήταν πρόθυμοι να με βοηθήσουν , πάντα κοντά μου , έτοιμοι να δώσουν λύση στα προβλήματα Ιδιαίτερα θέλω να ευχαριστήσω τον κ. Ηλιούδη , καθώς η γνωριμία μου μαζί του το 2003 και οι συμβουλές του σε όλη την διάρκεια των σπουδών του με ώθησαν ν'ασχοληθώ και να εντρυφήσω στον τομέα της ασφάλειας των υπολογιστών.
Επίσης, θέλω να ευχαριστήσω θερμά τον καθηγητή κ. Γιώργο Κακαρόντζα , για την υπομονή , τις συμβουλές και τις οδηγίες του, οι οποίες συνέβαλλαν σε σημαντικό βαθμό στην ολοκλήρωση της διπλωματικής μου εργασίας.
Τέλος θέλω να ευχαριστήσω μέσα απ'την καρδιά μου, την οικογένειά μου. Τους γονείς μου , οι οποίοι έκαναν πολλές θυσίες για να σπουδάσω. Τους ευχαριστώ για την αμέριστη αγάπη τους, την στήριξή τους αλλά πάνω απ'όλα για το παράδειγμα ζωής.
Αφιερώνω την διπλωματική μου εργασία στην οικογένειά μου και στον Πέτρο Πετρίδη που αν και ο ίδιος δεν μπόρεσε να σπουδάσει, έκανε τα πάντα ώστε εγώ ο εγγονός του να μπορέσω να φέρω εις πέρας τις σπουδές μου, επιτυχώς.
Τους ευχαριστώ όλους και ελπίζω να ανταποκρίθηκα και να συνεχίζω να ανταποκρίνομαι στις προσδοκίες τους.

Παπαδόπουλος Χ. Νικόλαος
Βόλος , Σεπτέμβριος 2005

Πίνακας περιεχομένων

ΕΙΣΑΓΩΓΙΚΟ ΜΕΡΟΣ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ 5

1.1 ΓΕΝΙΚΑ 5
1.2 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΕΧΝΟΛΟΓΙΑΣ GRID COMPUTING 6
1.3 ΑΝΑΓΚΗ ΓΙΑ ΕΦΑΡΜΟΓΗ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΥΠΟΛΟΓΙΣΤΙΚΗ ΠΛΕΓΜΑΤΟΣ (Grid Computing Security) 8
1.4 ΑΝΤΙΚΕΙΜΕΝΟ ΚΑΙ ΣΤΟΧΟΙ ΤΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ 9
1.5 ΔΟΜΗ ΤΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ 9

1° ΜΕΡΟΣ : ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ (GRID SYSTEM SECURITY) 11

ΚΕΦΑΛΑΙΟ 2: ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ (Grid Computing) 12

2.1 ΕΙΣΑΓΩΓΗ 13
2.2 ΒΑΣΙΚΑ ΘΕΜΑΤΑ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ 14
2.2.1 Αύξηση συνολικής επεξεργαστικής ισχύος μέσω παραλληλίας 15
2.2.2 Διαχείριση και συντονισμένος διαμοιρασμός πόρων 16
2.2.3 Δυναμική Διαχείριση φόρτου εργασίας 16
2.2.4 Ευελιξία-κλιμακωσιμότητα 17
2.2.5 Ασφάλεια σε περιβάλλον πλέγματος (Grid Security) 18
2.2.6 Διεπιφάνεια Χρήστη (User Interface) 18
2.2.7 Διαχείριση Δεδομένων (Data Management) 19
2.3 ΠΡΟΕΠΙΣΚΟΠΗΣΗ ΣΥΣΤΑΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ (Grid Computing Components) 21
2.3.1 Μια απλή προσέγγιση στην αρχιτεκτονική πλέγματος 21
2.3.1.1 Επίπεδο δικτύου (Network Layer) 22
2.3.1.2 Επίπεδο πόρων (Resource Layer) 22
2.3.1.3 Επίπεδο ενδιάμεσου λογισμικού (Middleware layer) 22
2.3.1.4 Επίπεδο εφαρμογών και υπηρεσιών (Application & Serviceware Layer) 23
2.3.2 Μια διαφορετική προσέγγιση στην αρχιτεκτονική πλέγματος 23
2.3.2.1 Επίπεδο δομής-συγκρότησης (fabric layer) 23
2.3.2.2 Επίπεδο σύνδεσης (connectivity layer) 24
2.3.2.3 Επίπεδο διαχείρισης πόρων (Resource layer) 24
2.3.2.4 Επίπεδο συλλογικής διαχείρισης (Collective layer) 24
2.3.2.5 Επίπεδο εφαρμογής (application layer) 25
2.4 ΠΡΟΕΠΙΣΚΟΠΗΣΗ ΤΩΝ ΕΦΑΡΜΟΓΩΝ ΤΟΥ ΠΛΕΓΜΑΤΟΣ 25
2.4.1 Εφαρμογές υπολογιστικής πλέγματος 25
2.4.1.1 Κατανεμημένη υπέρ-υπολογιστική (Distributed Supercomputing) 26
2.4.1.2 Υπολογιστική υψηλής απόδοσης (High throughput Computing) 27

2.4.1.3 Υπολογιστική κατ'απαίτηση (On demand Computing)....28
2.4.1.4 Υπολογιστική διεξοδικών δεδομένων (Data-Intensive Computing)....29
2.4.1.5 Υπολογιστική σύμπραξης (Collaborative Computing)....30
2.5 ΕΙΚΟΝΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ (Virtual Organization)....31
2.5.1 Ορισμός....31
2.5.2 Η ανάγκη για εικονικούς οργανισμούς....32
2.5.3 Δυνατότητες εικονικών οργανισμών....33
2.6 ΑΡΧΙΤΕΚΤΟΝΙΚΑ ΜΟΝΤΕΛΑ ΠΛΕΓΜΑΤΟΣ (Grid Architecture models)....33
2.6.1 Επιλογή αρχιτεκτονικού μοντέλου....33
2.7 SERVICE ORIENTED ARCHITECTURE (SOA)....36
2.7.1 Μοντέλο αρχιτεκτονικής SOA....37
2.8 WEB SERVICES ΑΡΧΙΤΕΚΤΟΝΙΚΗ (WSA)....38
2.9 ΒΑΣΙΚΑ ΘΕΜΑΤΑ ΤΗΣ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ OGSA....39
2.9.1 Ορισμός Αρχιτεκτονικής OGSA....39
2.9.2 Χαρακτηριστικά της αρχιτεκτονικής OGSA....40
2.9.3 Χρήση μηχανισμών της OGSA για δομές VO....43
2.10 ΠΡΟΤΥΠΟΠΟΙΗΣΗ ΥΠΗΡΕΣΙΩΝ ΠΛΕΓΜΑΤΟΣ (Grid Services standardization)....44
2.10.1 Εξέλιξη προτύπων Web υπηρεσιών....44
2.11 ΤΟ ΠΡΟΤΥΠΟ OGSI....45
2.12 ΣΥΜΠΕΡΑΣΜΑΤΑ....46

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ ΠΛΕΓΜΑΤΟΣ (Grid Security)....47

3.1 ΕΙΣΑΓΩΓΗ....48
3.2 ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΕΓΜΑΤΟΣ....50
3.2.1 Απαιτήσεις ασφάλειας πλέγματος....50
3.2.2 Η πρόκληση ολοκλήρωσης (Integration Challenge)....52
3.2.3 Η πρόκληση διαλειτουργικότητας (Interoperability Challenge)....52
3.2.4 Η πρόκληση έμπιστων σχέσεων....53
3.2.5 Απαιτήσεις ασφάλειας πλέγματος....54
3.3 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΕΓΜΑΤΟΣ (Grid Security Policy)....56
3.4 ΜΟΝΤΕΛΟ ΑΣΦΑΛΕΙΑΣ ΠΛΕΓΜΑΤΟΣ....59
3.4.1 Αρχιτεκτονική ασφάλειας πλέγματος (Grid Security Architecture)....59
3.4.2 Υπηρεσίες ασφάλειας πλέγματος (Grid Security Services)....63
3.5 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΣΦΑΛΕΙΑΣ OGSA....65
3.5.1 Προσδιορισμός ονομασίας (Naming)....65
3.5.2 Μετατροπή μεταξύ περιοχών ασφάλειας (Translating between Security realms)....66
3.5.3 Μηχανισμός αυθεντικοποίησης....66
3.5.4 Εξουσιοδότηση....67
3.6 ΑΣΦΑΛΕΙΑ ΕΙΚΟΝΙΚΩΝ ΟΡΓΑΝΙΣΜΩΝ (Virtual Organization Security)....67
3.6.1 Πολιτική ασφάλειας σε εικονικούς οργανισμούς....69
3.7 ΣΥΜΠΕΡΑΣΜΑΤΑ....71

ΜΕΡΟΣ 2: ΠΡΟΤΥΠΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ GRID SECURITY....72

ΚΕΦΑΛΑΙΟ 4: GRID SECURITY INFRASTRUCTURE (GSI).....73
4.1 ΕΙΣΑΓΩΓΗ.....74
4.1.1 Ορισμός.....75
4.2 ΑΠΑΙΤΗΣΕΙΣ GSI.....75
4.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ GSI.....76
4.3.1 Υποδομή δημόσιου κλειδιού (PKI).....77
4.3.2 Αρχή πιστοποίησης Πλέγματος (Grid CA).....78
4.3.3 Απόκτηση ψηφιακού πιστοποιητικού από CA.....79
4.3.4 Αυθεντικοποίηση και εξουσιοδότηση.....80
4.4 ΠΛΗΡΕΞΟΥΣΙΑ-ΕΚΧΩΡΗΣΗ ΔΙΚΑΙΩΜΑΤΩΝ (Delegation).....82
4.4.1 X.509 Πιστοποιητικά πληρεξουσιότητας (Proxy Certificates).....82
4.4.2 Περιεχόμενα X.509 proxy πιστοποιητικών.....83
4.4.3 Καθολική Πιστοποίηση (Single Sign-On).....84
4.4.4 Εκχώρηση δικαιωμάτων χρήσης (Delegation).....86
4.5 ΑΣΦΑΛΕΙΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΜΕΣΩ SSL/TLS.....88
4.6 ΣΥΣΤΗΜΑ ΑΜΕΣΗΣ ΑΠΟΘΗΚΕΥΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΠΛΕΓΜΑΤΟΣ (MyProxy).....90
4.7 ΑΣΦΑΛΕΙΑ ΥΠΟΔΟΜΗΣ ΠΛΕΓΜΑΤΟΣ (Grid Infrastructure Security).....93
4.8 ΣΥΜΠΕΡΑΣΜΑΤΑ.....94

ΚΕΦΑΛΑΙΟ 5: GLOBUS TOOLKIT- ΥΛΟΠΟΙΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΓΝΩΣΤΑ GRID PROJECTS.....95

5.1 ΕΙΣΑΓΩΓΗ.....96
5.2 ΤΙ ΕΙΝΑΙ ΤΟ GLOBUS TOOLKIT.....96
5.2.1 Τυπικό σενάριο χρήσης Globus.....97
5.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ GLOBUS-TOOLKIT.....97
5.3.1 Διαχειριστής ανάθεσης πόρων (Grid resource allocation Manager-GRAM).....99
5.3.2 Υπηρεσία Παρακολούθησης και ανακάλυψης πόρων (Monitoring and Discovery Service-MDS).....102
5.3.3 GridFTP.....103
5.3.4 Υπηρεσία Εξουσιοδότησης ομάδων χρηστών (Community Authorization Service CAS).....104
5.4 ΜΟΝΤΕΛΟ ΑΣΦΑΛΕΙΑΣ OGSA.....106
5.5 ΥΛΟΠΟΙΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΕ GRID PROJECTS.....107
5.5.1 Unicore (**Uni**form **I**nterface to **Co**mputer **Re**sources).....107
5.5.1.1 Λειτουργικότητα UNICORE.....107
5.5.1.2 Χαρακτηριστικά ασφάλειας UNICORE --Υποδομή δημοσίου κλειδιού (UNICORE PKI).....108
5.5.1.3 Εξουσιοδότηση.....108
5.5.2 Information Power Grid (I.P.G).....109
5.5.3 European DataGrid.....110
5.5.3.1 Ασφάλεια DataGrid.....111
5.5.4 Earth Grid System (ESG).....112
5.5.4.1 Προκλήσεις του ESG.....113
5.5.4.2 Ασφάλεια ESG.....113
5.5.5 E.G.E.E Project (Enabling Grids for E-science in Europe).....115

5.5.5.1 Ασφάλεια EGEE....116
5.5.6 Health Grids....117
5.5.6.1 GEMSS (Grid-enabled Medical Simulation Services)....118
5.5.6.2 Ασφάλεια GEMSS....118
5.6 ΣΥΜΠΕΡΑΣΜΑΤΑ....119

ΜΕΡΟΣ 3: ΠΕΙΡΑΜΑΤΙΚΗ ΥΛΟΠΟΙΗΣΗ-ΣΥΜΠΕΡΑΣΜΑΤΑ....121

ΚΕΦΑΛΑΙΟ 6: ΠΕΡΙΒΑΛΛΟΝ ΠΕΙΡΑΜΑΤΙΚΗΣ ΕΦΑΡΜΟΓΗΣ ΑΣΦΑΛΕΙΑΣ ΣΕ ΥΠΟΛΟΓΙΣΤΙΚΗ ΠΛΕΓΜΑΤΟΣ....122

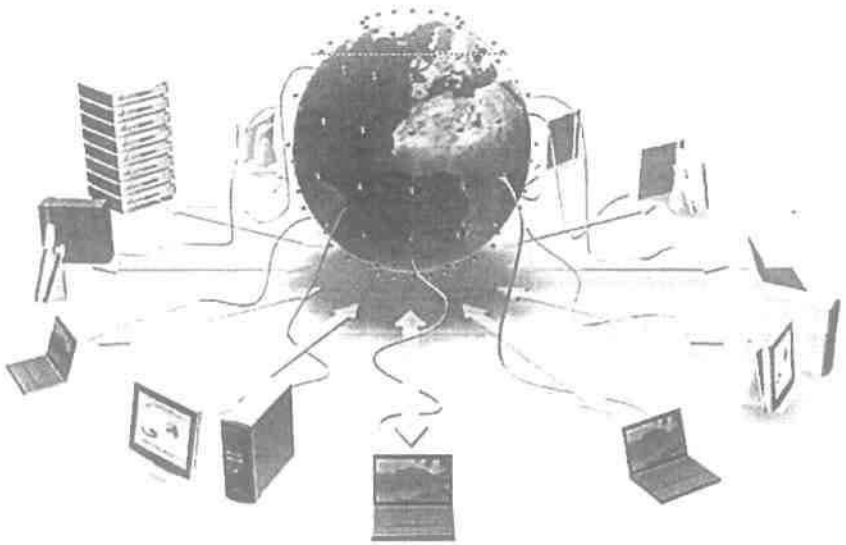
6.1 ΕΙΣΑΓΩΓΗ....123
6.2 ΤΟ ΠΕΡΙΒΑΛΛΟΝ ΥΛΟΠΟΙΗΣΗΣ....123
6.2.1 Τοπολογία πλέγματος συστημάτων....123
6.3 ΣΕΝΑΡΙΟ ΧΡΗΣΗΣ....124
6.4 ΔΙΑΔΙΚΑΣΙΑ ΕΓΚΑΤΑΣΤΑΣΗΣ ΑΣΦΑΛΟΥΣ ΠΛΕΓΜΑΤΟΣ....124
6.4.1 Δημιουργία λογαριασμών για τη χρήση του Globus....125
6.4.2 Εγκατάσταση του Globus Toolkit 4.0....125
6.4.3 Εγκατάσταση της αρχής πιστοποίησης (Simple CA installation) στο κεντρικό μηχάνημα....126
6.4.4 Εγκατάσταση του GSI στο κεντρικό μηχάνημα....127
6.4.5 Έκδοση και υπογραφή πιστοποιητικού server (host certificate)..127
6.4.6 Εγκατάσταση simpleCA στους Grid-clients....128
6.4.7 Εγκατάσταση υπηρεσίας NFS στο πλέγμα....128
6.4.8 Έκδοση και υπογραφή πιστοποιητικού χρήστη....129
6.4.9 Δημιουργία πληρεξούσιου χρήστη (Grid-Proxy-Init)....130
6.5 ΕΦΑΡΜΟΓΗ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ....131
6.6 ΣΥΜΠΕΡΑΣΜΑΤΑ....132

ΚΕΦΑΛΑΙΟ 7: ΣΥΜΠΕΡΑΣΜΑΤΑ-ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ

7.1 ΤΟ ΜΕΛΛΟΝ ΚΑΙ Η ΔΥΝΑΜΙΚΗ ΤΗΣ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ....133
7.2 ΤΟ ΠΑΡΩΝ ΚΑΙ ΤΟ ΜΕΛΛΟΝ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ (Grid System Security)....133
7.3 ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ ΤΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ....136
7.3.1 HealthGrids....136
7.3.2 Έρευνα και ανάπτυξη μηχανισμών δημιουργίας ασφαλών Web-based Grid Portals....137

Βιβλιογραφικές αναφορές....139

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ



Grid Computing

1.1 ΓΕΝΙΚΑ

Τα τελευταία χρόνια, η ραγδαία εξάπλωση του Internet σε συνδυασμό με τη διαθεσιμότητα δικτύων κορμού υψηλών ταχυτήτων και τη τεχνολογική ανάπτυξη των υπολογιστών, αλλά και του λογισμικού, έχουν δημιουργήσει μια νέα δυναμική στην κλασσική έννοια του όρου "υπολογιστικό περιβάλλον". Σημαντικός αριθμός υπολογιστικών πόρων , όπως υπολογιστική ισχύς, δεδομένα, υπηρεσίες, επιστημονικά όργανα κτλ, βρίσκονται κατανεμημένοι σε όλο τον κόσμο, δημιουργώντας την ανάγκη για ασφαλή , ομοιόμορφη, αξιόπιστη και απομακρυσμένη πρόσβαση μέσω δικτύων, ώστε να αξιοποιηθούν ικανοποιητικά οι δυνατότητες που αυτοί παρέχουν.

Προκειμένου να γίνει περισσότερο κατανοητή η έννοια της υπολογιστικής πλέγματος (Grid Computing) μπορεί να γίνει παρομοίωση του με ένα τεράστιο δίκτυο ηλεκτρικής ενέργειας, το οποίο παρέχει ηλεκτρικό ρεύμα στα σπίτια και στις επιχειρήσεις καθημερινά. Ο καθένας μπορεί να κάνει χρήση αυτού του ενεργειακού δικτύου, π.χ μπαίνοντας σε ένα δωμάτιο και ανοίγοντας το διακόπτη για τα φώτα. Ανάλογη μπορεί να είναι και η χρήση ενός υπολογιστικού δικτύου, καθώς μέσω αυτού μπορούν να προστεθούν πολλοί υπολογιστικοί πόροι-συσκευές σε οποιοδήποτε επιστημονικό ή βιομηχανικό περιβάλλον πλέγματος.

Γενικά με τον όρο **πλέγμα υπολογιστικών συστημάτων** αναφερόμαστε στο σύνολο της υποδομής, υλικό και λογισμικό , κατάλληλα διασυνδεδεμένης μέσω δικτύων υψηλών ταχυτήτων , καθώς και των απαραίτητων υπηρεσιών για τη δημιουργία ενός ενιαίου υπερ-υπολογιστικού περιβάλλοντος, που αν και είναι γεωγραφικά διασπαρμένο, εμφανίζεται με τρόπο διαφανή σε όλους τους χρήστες του.

Αναμφισβήτητα, η συγκεκριμένη τεχνολογία, έχει πολλές δυνατότητες, οι οποίες αρχίζουν σιγά-σιγά να αξιοποιούνται από επιχειρηματικούς , επιστημονικούς και εκπαιδευτικούς φορείς.

1.2 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΕΧΝΟΛΟΓΙΑΣ Grid Computing

Είναι γεγονός ότι στον σύγχρονο κόσμο, οι υπολογιστές έχουν γίνει εξαιρετικά ισχυροί σε σύγκριση με ότι ήταν πριν π.χ 5 χρόνια. Ακόμη και οι προσωπικοί (οικιακής χρήσης) υπολογιστές που πωλούνται στο εμπόριο, είναι υπολογιστικά ισχυροί για την ολοκλήρωση σύνθετων υπολογισμών , πράγμα το οποίο δεν θα μπορούσαμε να φανταστούμε καν πριν μια δεκαετία[32].
Οι επιχειρήσεις, προκειμένου να λύσουν δύσκολα υπολογιστικά (και όχι μόνο) προβλήματα , απαιτούν λύσεις που θα προσφέρουν μεγάλη υπολογιστική ισχύ, με το μικρότερο δυνατό κόστος [32] . Οι απαιτήσεις τους μάλιστα σε τομείς όπως ποιότητα και απόδοση των υπολογιστικών εφαρμογών αυξάνονται συνεχώς, με αποτέλεσμα η εκτέλεση τέτοιων υπολογισμών όπως μοντελοποίηση διάφορων σεναρίων, μελέτη γονιδιακών ταιριασμάτων, εκτέλεση αστροφυσικών προσομοιώσεων κτλ, να ξεπερνά τις δυνατότητες και την διαθεσιμότητα του ήδη υπάρχοντος υπολογιστικού εξοπλισμού σε μια εταιρεία.

Σύμφωνα με το [1], στους περισσότερους οργανισμούς, υπάρχουν πολλοί αχρησιμοποίητοι υπολογιστικοί πόροι. Μάλιστα, η πλειοψηφία των επιτραπέζιων υπολογιστών (desktop) είναι απασχολημένοι λιγότερο από το 5% του συνολικού χρόνου εργασίας τους. Ακόμα και οι εξυπηρετητές πολλών επιχειρήσεων ή οργανισμών είναι για κάποιο χρονικό διάστημα αδρανείς.
Η τεχνολογία Grid Computing, παρέχει λοιπόν ένα πλαίσιο για την αξιοποίηση των 'αδρανών' υπολογιστικών πόρων , αυξάνοντας έτσι την αποδοτικότητα της χρήσης τους.
Παρακάτω δίνονται ορισμένα πλεονεκτήματα που μπορούν να αποκομίσουν διάφορες εταιρείες, οργανισμοί φορείς κτλ [32]:

- Ένας χρηματοοικονομικός οργανισμός, που επεξεργάζεται και διαχειρίζεται διάφορες εφαρμογές οικονομίας, συνεργάζεται με άλλες εταιρείες (κυρίως οικονομικά τμήματά) για αύξηση της υπολογιστικής ισχύος του που θα συμβάλλει στην γρηγορότερη επεξεργασία οικονομικών μοντέλων. Αυτό από μόνο του έχει ως αποτέλεσμα ο πελάτης να είναι ευχαριστημένος για την γρηγορότερη εξυπηρέτησή του από τον οργανισμό.

- Μία ομάδα από επιστήμονες που μελετούν την ατμόσφαιρα, συλλέγουν καθημερινά τεράστιες ποσότητες πειραματικών δεδομένων. Αυτοί οι επιστήμονες χρειάζονται μέσα αποθήκευσης δεδομένων με συγκεκριμένες δυνατότητες, που θα τους επιτρέψει να έχουν γρήγορη και ασφαλή πρόσβαση σε αυτά. ανάλογα και με τις απαιτήσεις τους. Με την χρήση αποθηκευτικών πόρων μέσα σε ένα πλέγμα, οι απαιτήσεις τους αυτές θα ικανοποιηθούν διευκολύνοντας έτσι την επιστημονική τους έρευνα.

- Οι κοινότητες των on-line multiplayer παιχνιδιών στο Internet απαιτούν ένα μεγάλο αριθμό από υπολογιστές (game-servers) που θα αποτελούν ένα υπολογιστικό πλέγμα, αντί για ένα και μόνο εξυπηρετητή παιχνιδιών. Αυτό επιτρέπει σε παίκτες από όλο τον κόσμο να αλληλεπιδρούν μεταξύ τους σε

πραγματικό χρόνο, χάρη στις πολλές δυνατότητες (κυρίως επεξεργαστικής ισχύος) των υπολογιστικών πλεγμάτων.

- Ένας κυβερνητικός οργανισμός, που ειδικεύεται στις φυσικές καταστροφές, όπως π.χ χημική διαρροή αερίων, μπορεί να χρειαστεί να συνεργαστεί με διαφορετικές υπηρεσίες προκειμένου να μελετήσει και να καταστρώσει καλύτερα τα πλάνα της για τη διαχείριση μιας τέτοιας κρίσεων. Τέτοιου είδους οργανισμοί πολλές φορές χρειάζεται να προσομοιώσουν πολλά υπολογιστικά μοντέλα που σχετίζονται με τη διαρροή τέτοιων χημικών αερίων, για να υπολογίσουν με ποια ταχύτητα διαχύνεται στο περιβάλλον , την έκταση της διαρροής και πως αυτή μπορεί να επηρεάσει την ανθρώπινη υγεία. Με τη χρήση λοιπόν υπολογιστικών πλεγμάτων , μπορεί να αυξηθεί η παρεχόμενη ασφάλεια τους πολίτες και να εξασφαλιστεί πολύτιμος χρόνος στην αντιμετώπιση τέτοιων ζητημάτων.

Στις μέρες μας, η τεχνολογία Grid Computing προσφέρει πολλές λύσεις για την αντιμετώπιση προβλημάτων όπως τα παραπάνω. Και αυτό γιατί παρέχει εκείνα τα χαρακτηριστικά όπως ασφάλεια, κλιμακωσιμότητα και υψηλή απόδοση, που θα συμβάλλουν στην αρτιότερη λειτουργία του κάθε φορέα που κάνει χρήση αυτής της τεχνολογίας.

Συνοπτικά, μερικά από τα πλεονεκτήματα της δυναμικής του Grid Computing σύμφωνα με το [32] είναι τα παρακάτω:

- Δυνατότητα για ενοποίηση πολλαπλών κατανεμημένων , ετερογενών και διαχειριστικά ανεξάρτητων πηγών δεδομένων.
- Δυνατότητα για παροχή αποδοτικών μηχανισμών μεταφοράς δεδομένων για απαιτητικούς υπολογισμούς.
- Δυνατότητα αποθήκευσης δεδομένων (data caching) με τέτοιο τρόπο ώστε να ελαττωθεί ο φόρτος του δικτύου.
- Δυνατότητα κρυπτογράφησης δεδομένων και ελέγχου ακεραιότητας τους, προκειμένου να μην υπάρξει παράνομη αλλοίωσή τους, καθώς και μηχανισμών διατήρησης αντιγράφων τους (backup).
- Δυνατότητα για ανεξάρτητη διαχείριση υπολογιστικών πόρων.
- Δυνατότητα παροχής συγκεκριμένων μηχανισμών που μπορούν με ευφυή τρόπο να επιλέγουν τους κατάλληλους υπολογιστικούς πόρους για συγκεκριμένες εργασίες των χρηστών.
- Δυνατότητα αντίληψης μελλοντικών φόρτων εργασίας στο πλέγμα, καθώς και της τρέχουσας και μελλοντικής διαθεσιμότητας των αποθηκευτικών πόρων.
- Ανίχνευση αποτυχιών και παροχή μηχανισμών ανάκαμψης.
- Παροχή των κατάλληλων μηχανισμών ασφάλειας (εμπιστευτικότητα. ακεραιότητα, διαθεσιμότητα).

1.3 ΑΝΑΓΚΗ ΓΙΑ ΕΦΑΡΜΟΓΗ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΥΠΟΛΟΓΙΣΤΙΚΗ ΠΛΕΓΜΑΤΟΣ (Grid Computing Security)

Η υπολογιστική πλέγματος ασχολείται με την διαμοίραση και την συντονισμένη χρήση ξεχωριστών κατανεμημένων πόρων ανάμεσα σε διάφορους φορείς, εταιρείες, οργανισμούς, ιδρύματα, γνωστά και σαν 'εικονικοί οργανισμοί'. Η δυναμική και πολυ-ιδρυματική φύση αυτών των περιβαλλόντων εισάγει και νέες προκλήσεις στον τομέα της ασφάλειας, που αυτές με την σειρά τους απαιτούν συγκεκριμένες λύσεις και τεχνικές [22].

Για να γίνει περισσότερο κατανοητή η ανάγκη για ασφάλεια, δίνουμε το παρακάτω παράδειγμα. Έστω μια εταιρεία που κάνει έρευνες στον χώρο της βιο-ιατρικής και βιολογίας. Το εξειδικευμένο προσωπικό της εκτελεί κάποια πειράματα πάνω σε ιατρικά δεδομένα ασθενών (π.χ DNA) και απαιτείται η εκτέλεσή τους σε κάποιους υπολογιστικούς πόρους που βρίσκονται σε κάποιο απομακρυσμένο εργαστήριο σε άλλο νομό. Γίνεται αντιληπτό ότι η μεταφορά τόσο ευαίσθητων δεδομένων πάνω από το δίκτυο απαιτεί εμπιστευτικότητα και μηχανισμούς κρυπτογράφησης . Εκτός από αυτά όμως η υπολογιστική πλέγματος πρέπει να παρέχει μηχανισμούς αυθεντικοποίησης με τους οποίους ο διαχειριστής-κάτοχος των πόρων στο απομακρυσμένο εργαστήριο πρέπει να αυθεντικοποιήσει ότι αυτός που ζητάει πρόσβαση στους πόρους του είναι πράγματι νόμιμος και εξουσιοδοτημένος χρήστης του πλέγματος.

Οι τεχνολογίες που αναπτύχθηκαν από την επιστημονική κοινότητα του Grid Computing περιλαμβάνουν λύσεις ασφάλειας που υποστηρίζουν σύμφωνα με το [25]:

- Διαχείριση πιστοποιητικών και πολιτικών ασφάλειας των διαφόρων εμπλεκόμενων φορέων.
- Πρωτόκολλα διαχείρισης πόρων
- Υπηρεσίες που υποστηρίζουν ασφαλή απομακρυσμένη πρόσβαση σε υπολογιστικούς και αποθηκευτικούς πόρους, καθώς και συνεργασία πολλαπλών πόρων.
- Πρωτόκολλα που υποβάλλουν ερωτήματα για συγκεκριμένες πληροφορίες.
- Υπηρεσίες που παρέχουν πληροφορίες διαμόρφωσης και κατάστασης συγκεκριμένων πόρων , οργανισμών (διαθεσιμότητα, υπολογιστικός φόρτος).

Σε όλα λοιπόν τα περιβάλλοντα υπολογιστικής πλέγματος γίνεται χρήση τέτοιων και άλλων παρόμοιων μηχανισμών προκείμενου να κτιστεί ένα ασφαλές υπολογιστικό πλέγμα.

1.4 ΑΝΤΙΚΕΙΜΕΝΟ ΚΑΙ ΣΤΟΧΟΙ ΤΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η ασφάλεια σε ένα υπολογιστικό πλέγμα. Πιο συγκεκριμένα, ο στόχος της διπλωματικής εργασίας είναι να ερευνήσει τις απαιτήσεις ασφάλειας των συστημάτων υπολογιστικής πλέγματος. δίνοντας ιδιαίτερη έμφαση στη πιστοποίηση οντοτήτων και στον έλεγχο πρόσβασης.

Τα θέματα που θα διαπραγματευτεί η διπλωματική είναι :

- **Καθορισμός των αντικειμένων ασφάλειας των Grid Systems:** Τι πρέπει να προστατευθεί στα συστήματα πλέγματος π.χ πόροι, δεδομένα , υπολογισμοί κτλ.
- **Διερεύνηση της χρήσης των πιστοποιητικών πληρεξουσιότητας (proxy certificates)** που επιτρέπουν στις οντότητες που συμμετέχουν στο υπολογιστικό πλέγμα να εξουσιοδοτούν άλλες οντότητες έτσι ώστε να ενεργούν εκ μέρους τους (delegation)
- **Διαδικασία καθολικής πιστοποίησης (single sign-on)** του χρήστη στο υπολογιστικό πλέγμα.
- **Γλώσσες και πολιτικές ελέγχου πρόσβασης:** Χρειάζονται εξειδικευμένες γλώσσες, οι οποίες με άλλες γνωστές γλώσσες όπως η xml, θα μπορούν να καθορίσουν πολιτικές ελέγχους πρόσβασης στους κόμβους του πλέγματος
- **Μοντέλα αρχιτεκτονικής ασφάλειας πλέγματος:** πάνω στα οποία στηρίζεται η ασφάλεια για την υπολογιστική πλέγματος (π.χ OGSA)

1.5 ΔΟΜΗ ΤΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ

Η συγκεκριμένη διπλωματική εργασία χωρίζεται σε τρία θεματικά μέρη και επτά κεφάλαια συνολικά.

Στο **εισαγωγικό μέρος** (κεφάλαιο 1) γίνεται μια εισαγωγή στο αντικείμενο της διπλωματικής εργασίας, μια μικρή αναφορά στα πλεονεκτήματα χρήσης της τεχνολογίας Grid Computing καθώς και μια αναφορά στην ανάγκη χρήσης μηχανισμών ασφάλειας σε υπολογιστικά πλέγματα. Τέλος περιγράφεται η δομή της διπλωματικής εργασίας.

Στο **πρώτο μέρος** (κεφ. 2,3), βασικό θέμα αποτελεί η ασφάλεια συστημάτων υπολογιστικής πλέγματος. Συγκεκριμένα, στο κεφάλαιο 2 αναλύονται τα βασικά χαρακτηριστικά της υπολογιστικής πλέγματος, τα δομικά στοιχεία από τα οποία αποτελείται , ενώ παράλληλα γίνεται αναφορά στην θεμελιώδη έννοια 'εικονικός οργανισμός' . Επίσης μελετώνται τα αρχιτεκτονικά μοντέλα πλέγματος με τα ιδιαίτερα χαρακτηριστικά που έχει το καθένα, δίνοντας έμφαση στην αρχιτεκτονική OGSA. Στο κεφ. 3 αναλύονται όλες οι πτυχές της ασφάλειας σε υπολογιστικό πλέγμα, μελετώνται οι απαιτήσεις ασφάλειας του πλέγματος, εξετάζεται μια ενδεικτική πολιτική ασφάλειας πλέγματος, και το αντίστοιχο μοντέλο ασφάλειας. Τέλος δίνεται έμφαση στην περιγραφή της αρχιτεκτονικής ασφάλειας OGSA

Το **δεύτερο μέρος** (κεφ. 4, 5) της διπλωματικής εργασίας ασχολείται κυρίως με πρότυπα και τεχνολογίες ασφάλειας πλέγματος (Grid Security).

Πιο συγκεκριμένα, στο κεφάλαιο 4 περιγράφεται το βασικό δομικό στοιχείο της ασφάλειας πλέγματος που είναι το GSI, τα χαρακτηριστικά του και γενικότερα η συμβολή του στο κτίσιμο ενός ασφαλούς υπολογιστικού πλέγματος.
Ακόμη γίνεται αναφορά σε μια νέα σχετικά τεχνολογία αποθήκευσης πιστοποιητικών την MyProxy.
Στο κεφάλαιο 5, αναλύεται το πακέτο Globus Toolkit. Αναπτύσσονται ιδιαίτερα τα χαρακτηριστικά και οι δυνατότητές του ενώ προς το τέλος του κεφαλαίου παρουσιάζονται υλοποιήσεις ασφάλειας σε μερικά από τα πιο γνωστά παγκοσμίως Grid projects.

Το **τρίτο μέρος** (κεφ. 6,7) της διπλωματικής διαφέρει από τον καθαρά ερευνητικό-βιβλιογραφικό χαρακτήρα των πρώτων 2 μερών. Συγκεκριμένα στο κεφάλαιο αυτό γίνεται μια πειραματική υλοποίηση της ασφάλειας σε ένα πρότυπο πλέγμα συστημάτων.
Πιο συγκεκριμένα στο 6° κεφάλαιο, περιγράφεται το περιβάλλον στο οποίο έγινε η πειραματική εφαρμογή ασφάλειας σε πλέγμα συστημάτων, το σενάριο χρήσης και η όλη διαδικασία εφαρμογής των μηχανισμών ασφάλειας που παρέχει το εργαλείο Globus Toolkit και τα πλεονεκτήματα που προήλθαν από τη χρήση του.
Στο 7° και τελευταίο κεφάλαιο, καταγράφονται τα συμπεράσματα από την έρευνα της ασφάλειας συστημάτων υπολογιστικής πλέγματος καθώς και οι μελλοντικές επεκτάσεις από τη χρήση της συγκεκριμένης τεχνολογίας.

ΜΕΡΟΣ 1: ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ (GRID SYSTEM SECURITY)

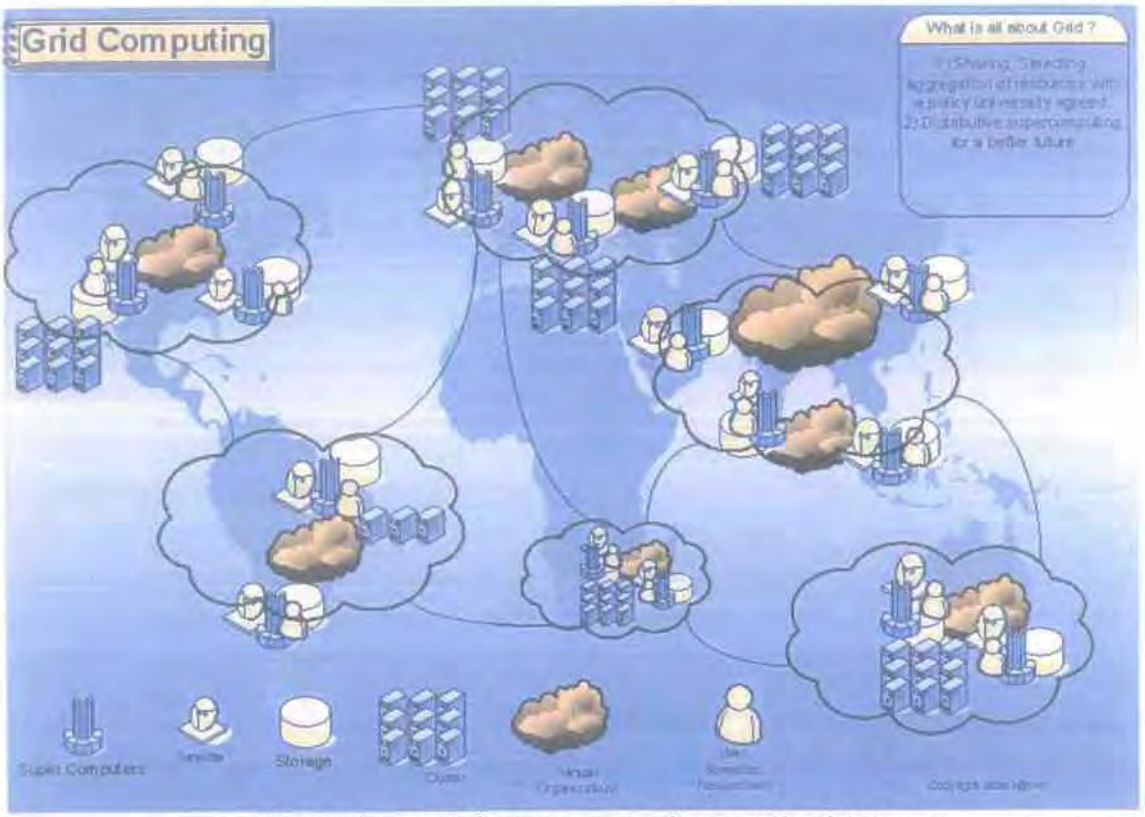
Κεφάλαιο 2: Βασικά χαρακτηριστικά υπολογιστικής πλέγματος (Grid Computing)

Κεφάλαιο 3: Ασφάλεια Πλέγματος (Grid Security)

ΚΕΦΑΛΑΙΟ 2 : ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ

Περίληψη

Στο κεφάλαιο αυτό κεντρικό θέμα μελέτης είναι τα βασικά χαρακτηριστικά των υπολογιστικών πλεγμάτων. Δίνουμε αρχικά τον ορισμό του υπολογιστικού πλέγματος, και περιγράφουμε τα βασικά συστατικά από τα οποία αποτελείται. Έπειτα αναφερόμαστε σε βασικούς τομείς της καθημερινής ζωής , και της επιστήμης, όπου βρίσκουν εφαρμογή αυτού του είδους τα πλέγματα και περιγράφουμε την έννοια 'εικονικός' οργανισμός .
Τέλος, καταγράφουμε τα βασικά αρχιτεκτονικά μοντέλα πλέγματος, την αρχιτεκτονική WSA και OGSA, δίνοντας όμως βαρύτητα στα ξεχωριστά χαρακτηριστικά του καθενός.



Γραφική αναπαράσταση της υπολογιστικής πλέγματος

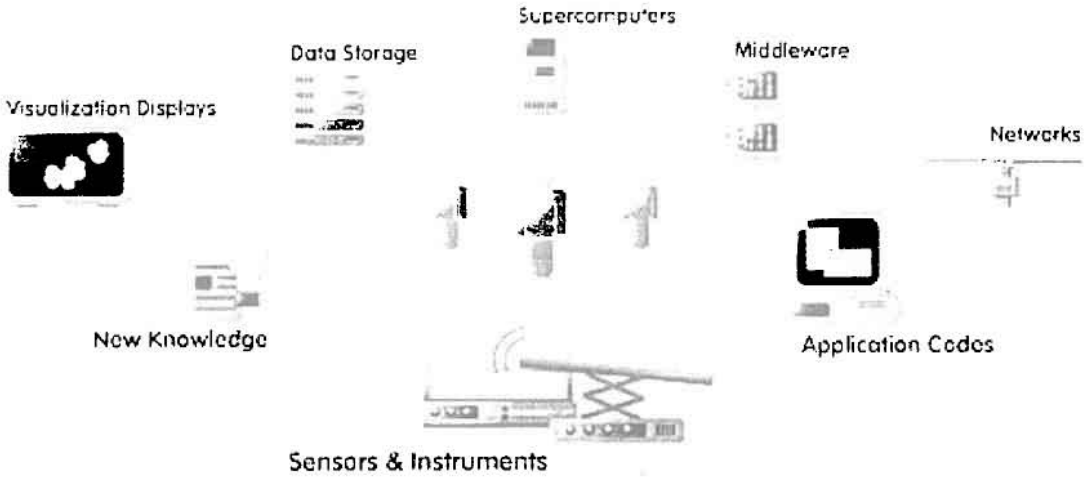
2.1 ΕΙΣΑΓΩΓΗ

Ο όρος πλέγμα (Grid) πρωτοαναφέρθηκε στα μέσα της δεκαετίας του 90 για να δώσει έμφαση στη υποδομή της κατανεμημένης υπολογιστικής (distributed computing) και στη χρήση της σε προχωρημένες εφαρμογές της επιστήμης και της μηχανικής.

Βασική φιλοσοφία του Grid **είναι η ελεγχόμενη και συντονισμένη διαμοίραση και η χρήση πόρων για την επίλυση προβλημάτων στο πλαίσιο δυναμικών πολύ-ιδρυματικών εικονικών οργανισμών (multinstitutional Virtual Organizations VOs)**. [19]
Η διαμοίραση αυτή αφορά όχι μόνο την ανταλλαγή αρχείων-δεδομένων αλλά κυρίως την άμεση πρόσβαση σε υπολογιστές, λογισμικό, υπηρεσίες, βάσεις δεδομένων και άλλους πόρους.[2]

Η υπολογιστική πλέγματος (από εδώ και πέρα θα αναφέρεται σαν Grid Computing) υπήρξε σημείο εστίασης για τους ερευνητές τόσο των πανεπιστήμιων όσο και της βιομηχανίας. Αν και η συγκεκριμένη τεχνολογία βρίσκεται στα πρώτα στάδιά της, εντούτοις γνωρίζει ραγδαία ανάπτυξη .Φαινομενικά είναι εύκολο να δώσουμε ένα τυπικό ορισμό για το Grid Computing, ωστόσο υπάρχει δυσκολία στην ακριβή περιγραφή του λόγω και των διαφόρων ειδών πλεγμάτων που υπάρχουν (data grid, health grid, computational grids,…). [8]

2.2 ΒΑΣΙΚΑ ΘΕΜΑΤΑ ΤΗΣ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ (Grid Computing)



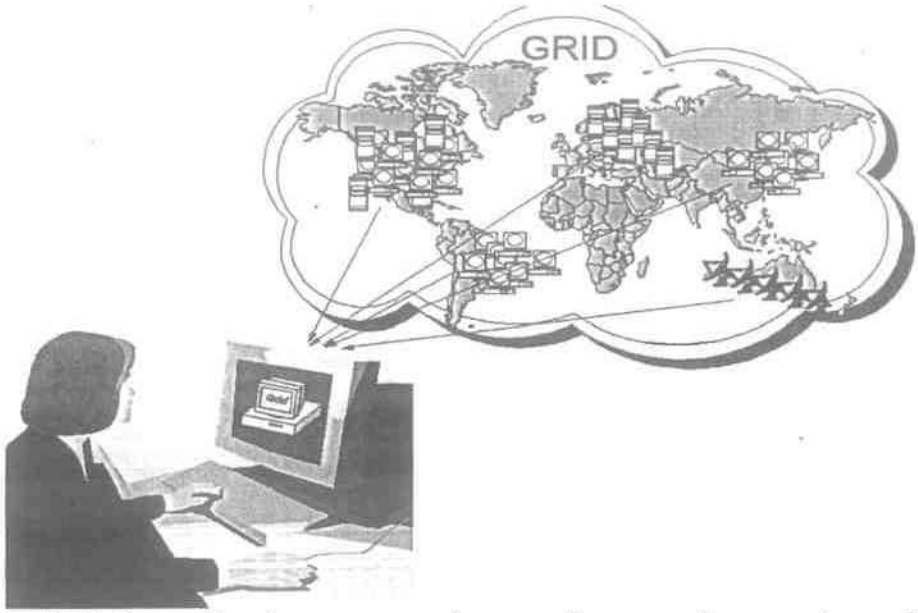
Grid Computing

Ένας κατάλληλος ορισμός σύμφωνα με το [2] είναι και ο ακόλουθος:

«***Grid Computing είναι το σύνολο της υποδομής, υλικό και λογισμικό, κατάλληλα διασυνδεδεμένης μέσω δικτύων υψηλών ταχυτήτων για τη δημιουργία ενός ενιαίου υπέρ-υπολογιστικού περιβάλλοντος***»

Η IBM στο [13] , τονίζει ότι το Grid Computing μας ***επιτρέπει να ενώνουμε ομάδες-συστοιχίες από πόρους (servers, συστήματα αποθήκευσης, δίκτυα, κτλ..) σε ένα τεράστιο σύστημα, έτσι ώστε να μπορέσουμε να εκμεταλλευτούμε την ισχύ πολλαπλών συστημάτων πόρων σε ένα και μοναδικό 'σημείο' για συγκεκριμένο σκοπό.***
Στον απλό χρήστη, το τελικό αποτέλεσμα φαντάζει σαν ένα τεράστιο εικονικό υπολογιστικό σύστημα.

Το Grid Computing έχει πολλά και σημαντικά πλεονεκτήματα, τα οποία προσπαθούν να εκμεταλλευτούν οργανισμοί, πανεπιστήμια, εταιρείες κτλ.
Οι εφαρμογές Grid , συνδέουν πολλούς πόρους που πιθανόν να είναι και γεωγραφικά διασπαρμένοι, προκειμένου να λύσουν π.χ ένα απαιτητικό επιστημονικό πρόβλημα. Γενικά όπως θα δούμε και παρακάτω, υπάρχουν πάρα πολλές πρακτικές εφαρμογές του Grid Computing.



Μέσω του Grid Computing έχουμε εικονική αντιστοίχιση των διασπαρμένων πόρων σε ένα ενιαίο υπολογιστικό σύστημα [19]

Ωστόσο αν θέλουμε να δούμε τα ***βασικά χαρακτηριστικά του Grid Computing***. τότε οι παρακάτω όροι-έννοιες θα μας δώσουν μια γενική ιδέα της υπολογιστικής πλέγματος [13]:

- **Αύξηση συνολικής επεξεργαστικής ισχύος μέσω παραλληλίας (Parallel CPU Capacity)**
- **Διαχείριση και συντονισμένος διαμοιρασμός πόρων (Coordinate resource Sharing)**
- **Δυναμική διαχείριση φόρτου εργασίας (Dynamic Workload management)**
- **Ευελιξία (flexibility)-κλιμακωσιμότητα (scalability)**
- **Ασφάλεια σε περιβάλλον Grid (Grid Security)**
- **Διεπιφάνεια Χρήστη (User Interface)**
- **Διαχείριση Δεδομένων (Data Management)**

Παρακάτω δίνεται μια σύντομη ανάλυση των παραπάνω εννοιών.

2.2.1 Αύξηση συνολικής επεξεργαστικής ισχύος μέσω παραλληλίας (Parallel CPU Capacity)

Ο πιο γνωστός πόρος προς διαμοίραση είναι η επεξεργαστική ισχύς που παρέχεται από τους επεξεργαστές των μηχανημάτων του πλέγματος. Αυτοί, μπορούν να διαφέρουν στην ταχύτητά τους, στην αρχιτεκτονική τους, την πλατφόρμα λογισμικού κτλ..
Η δυνατότητα του Grid Computing για παράλληλη επεξεργαστική ισχύ και υπολογιστική, το καθιστούν ιδιαίτερα ενδιαφέρον για πολλούς φορείς -οργανισμούς .

Εκτός των όποιων επιστημονικών αναγκών, αυτού του είδους υπολογιστική ισχύς οδηγεί σε νέα επανάσταση στον χώρο των βιομηχανιών και κυρίους σε τομείς όπως βιο-ιατρικός τομέας, μοντελοποίηση οικονομίας, ανακάλυψη κοιτασμάτων πετρελαίου, απεικόνιση εικόνων (motion animation) κτλ.

Το βασικό χαρακτηριστικό τέτοιων χρήσεων είναι ότι σχεδιάστηκαν να χρησιμοποιούν αλγορίθμους που μπορούν να καταμερίσουν τον φόρτο σε μικρότερα τμήματα τα οποία θα μπορούν να εκτελούνται παράλληλα στους κατανεμημένους κόμβους του πλέγματος. Σαφώς υπάρχουν οι κατάλληλοι μηχανισμοί (π.χ barriers) που φροντίζουν για τη σωστή ενημέρωση και επικοινωνία μεταξύ των όποιων κόμβων. [1]

Σύμφωνα με το [19] υπάρχουν 3 τρόποι εκμετάλλευσης πόρων στο πλέγμα:

1. Εκτέλεση μιας διεργασίας σε ένα κόμβο του πλέγματος που είναι διαθέσιμος.
2. Εκτέλεση μιας εφαρμογής / διεργασίας, που είναι σχεδιασμένη να 'σπάει' το φόρτο της σε μικρότερα τμήματα, ώστε καθένα από αυτά να τρέξει σε διαφορετικούς επεξεργαστές.
3. Εκτέλεση μιας εφαρμογής / διεργασίας που χρειάζεται να εκτελεστεί πολλές φορές και σε διαφορετικές μηχανές του πλέγματος.

2.2.2 Διαχείριση και συντονισμένος διαμοιρασμός πόρων (Coordinate resource Sharing)

Όπως αναφέρθηκε και πιο πάνω, πρέπει να εξασφαλιστεί ο **ελεγχόμενος και συντονισμένος διαμοιρασμός και η χρήση πόρων.** Προκειμένου να διαχειριστούν όλες οι παραπάνω διαδικασίες (όπως φόρτωμα διεργασιών με συγκεκριμένους πόρους, παρακολούθηση της κατάστασής των κτλ) , πρέπει να υπάρξει σωστή διαχείριση των πόρων.
Επίσης ο διαμοιρασμός αυτός θα πρέπει να ελέγχεται κυρίως από τους πάροχους των πόρων και τους χρήστες των πόρων, προκειμένου να καθοριστεί με σαφήνεια **τι θα πρέπει να μοιραστεί, ποιος επιτρέπεται να το διαμοιράσει και υπό ποιες συνθήκες πραγματοποιείται ο διαμοιρασμός αυτός.**

Επιπροσθέτως, οι πόροι του πλέγματος είναι γεωγραφικώς διασπαρμένοι ανήκοντας σε διάφορους τομείς-οργανισμούς. Απαιτείται λοιπόν να υπάρξει σεβασμός της αυτονομίας των κατόχων των πόρων και να υπάρξει σωστή διαχείριση .
Μεταξύ άλλων, ένα τέτοιο software μπορεί και οφείλει να μετρά τις τρέχουσες χρήσεις πόρων κάποιων κόμβων προκειμένου να παίξει το ρόλο του 'διαιτητή' και να εφαρμόσει δικαιοσύνη σε περίπτωση που ένας κόμβος δεν έχει πάρει κάποιο πόρο ενώ ο άλλος κόμβος έχει αρκετούς στη διάθεσή του.

Εκτός των άλλων, αξίζει να αναφερθεί (εκτενέστερα, πιο κάτω) η οργάνωση των χρηστών σε εικονικούς οργανισμούς. Οι χρήστες λοιπόν μπορούν να οργανωθούν δυναμικά σε ένα αριθμό 'εικονικών' ομάδων / οργανισμών (Virtual organization) , ο καθένας εκ των οποίων έχει και διαφορετική πολιτική χρήσης και διαμοίρασης των πόρων του πλέγματος και ασφάλειας όσον αφορά την πρόσβασή τους σε αυτό.

2.2.3 Δυναμική Διαχείριση φόρτου εργασίας (Dynamic Workload management)

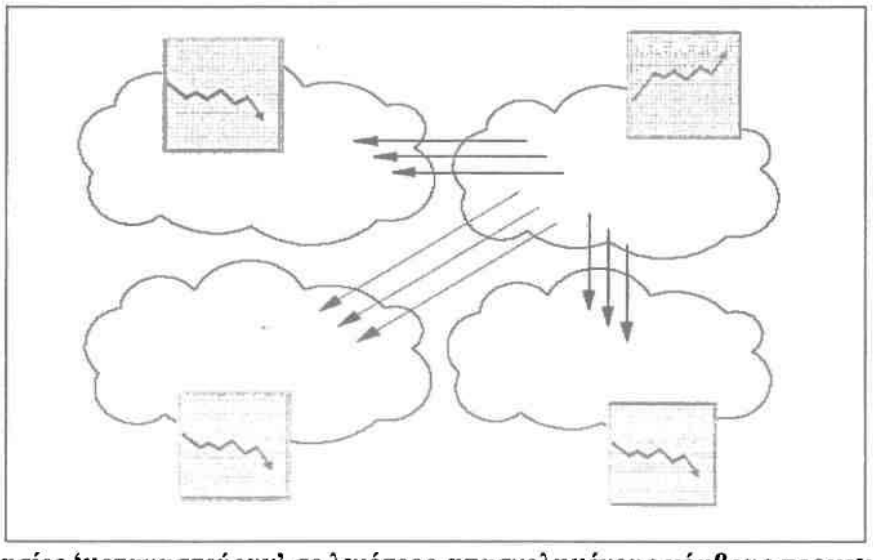
Οι εφαρμογές που θέλει να τρέξει ο χρήστης, πρέπει να 'γνωρίζουν' πόσοι πόροι είναι διαθέσιμοι στο πλέγμα ανά πάσα στιγμή. Επομένως η παροχή δυναμικής διαχείρισης φόρτου εργασίας μέσω του κατάλληλου workload manager θα χειρίζεται τη συγκεκριμένη απαίτηση των εφαρμογών.

Αυτές λοιπόν μπορούν να επικοινωνούν με το manager για να ανακαλύπτουν τους διαθέσιμους πόρους και σε ποια κατάσταση (κατοχής, αναμονής,..) βρίσκονται.

Χαρακτηριστικό παράδειγμα μπορεί να αποτελέσει η περίπτωση εκείνη κατά την οποία λόγω κάποιας αποτυχίας (είτε του δικτύου είτε του host) ο workload manager προκειμένου να μην σπαταληθεί ο πόρος, τον αναθέτει δυναμικά σε κάποια άλλη μηχανή αυτόματα.
Πιο συγκεκριμένα, στην περίπτωση που μια διεργασία, πάει να εκτελεστεί σε μια απασχολημένη μηχανή, ο manager θα ελέγξει μήπως υπάρχει μια αδρανής-έστω και στιγμιαία- μηχανή για να της αναθέσει την διεργασία, χωρίς να σπαταληθεί χρόνος.

Αξίζει μάλιστα να τονιστεί ότι σε περιβάλλοντα και εφαρμογές real-time (π.χ υπολογισμού δεδομένων πυρηνικού αντιδραστήρα) μπορούν να 'τρέχουν' πολλαπλά αντίγραφα της διεργασίας σε διαφορετικές μηχανές σε όλο το πλέγμα **αυξάνοντας σημαντικά την αξιοπιστία του όλου συστήματος (Reliability).**
Ακόμα ένα παράδειγμα είναι το εξής: στο Grid Computing έχουμε μία διεργασία χαμηλής προτεραιότητας . Ξαφνικά όμως παρουσιάζεται μια υψηλής προτεραιότητας διεργασία. Αν το πλέγμα είναι ήδη πλήρως χρησιμοποιήσιμο (δηλαδή οι πόροι του) ο workload manager καλείται να διακόψει την πρώτη και να εκτελέσει την δεύτερη.

Αυτό που επιτυγχάνεται εν ολίγοις, είναι σωστή διαχείριση των πόρων και του φόρτου τους στις διάφορες μηχανές, πράγμα που σημαίνει ότι γίνεται (και έτσι πρέπει) σωστή εκμετάλλευση των αχρησιμοποίητων πόρων (underutilized resources) [1]. Η εικόνα που ακολουθεί μας βοηθά να κατανοήσουμε καλύτερα όλα τα παραπάνω:



Οι διεργασίες 'μεταναστεύουν' σε λιγότερο απασχολημένους κόμβους προκειμένου να υπάρχει εξισορρόπηση φόρτου εργασίας και να εξαλειφθούν απρόοπτες διακυμάνσεις φόρτου.-

2.2.4 Ευελιξία (Flexibility)-κλιμακωσιμότητα (scalability)

Είναι γεγονός ότι μέσα σε ένα τέτοιο περιβάλλον Grid, είναι δυνατό να δικτυώνονται δεκάδες, εκατοντάδες χρήστες (μεμονωμένοι ή οργανισμοί). Δεδομένου του μεγάλου αριθμού, θεωρείται απίθανο, όλοι αυτοί να χρησιμοποιούν την ίδια πλατφόρμα λογισμικού.

Κρίνεται λοιπόν αναγκαία η δυνατότητα ευελιξίας και άρτιας διασύνδεσης όλων αυτών των ετερογενών πλατφόρμων κάτω από αυτό το ενιαίο υπολογιστικό περιβάλλον.
Όσο αφορά το δεύτερο χαρακτηριστικό, ένα πλέγμα μπορεί να μεγαλώσει , καλύπτοντας από μερικές δεκάδες, μέχρι εκατομμύρια χρήστες. Αυτό το χαρακτηριστικό, προκαλεί προβλήματα υποβάθμισης της απόδοσης . Για αυτό το λόγο εφαρμογές που απαιτούν ένα μεγάλο αριθμό από γεωγραφικά κατανεμημένους πόρους, πρέπει να σχεδιάζονται ώστε να έχουν ανεκτικότητα τόσο στη χρονική καθυστέρηση όσο και στο διαθέσιμο bandwidth του δικτύου.

2.2.5 Ασφάλεια σε περιβάλλον Grid (Grid Security)

Οι υπολογιστές, και κατά προέκταση οι χρήστες, μέσα στο πλέγμα είναι δικτυωμένοι και εκτελούν διάφορες εφαρμογές. Επίσης είναι πιθανό να χειρίζονται ευαίσθητες ή εξαιρετικά πολύτιμες πληροφορίες (π.χ ιατρικά-βιοτεχνολογικά δεδομένα).
Μάλιστα λόγω της ετερογενούς και κατανεμημένης φύσης του πλέγματος , αυξάνονται οι απαιτήσεις σε ασφάλεια. Η χρήση παραδοσιακών μεθόδων ασφάλειας όπως αυθεντικοποίηση μέσω password και παραδοσιακών πολιτικών ασφάλειας δεν επαρκούν.

Επομένως γίνεται χρήση διαφορετικών προτύπων και πρωτοκόλλων προκειμένου να επιτύχουν [19]:

Αυθεντικοποίηση→εξασφαλίζουμε ότι ο χρήστης είναι αυτός που λέει ότι είναι

Εξουσιοδότηση→παραχώρηση συγκεκριμένων δικαιωμάτων που εξαρτώνται από την ταυτότητά του.

Εμπιστευτικότητα→ εξασφαλίζουμε ότι τα δεδομένα θα παραμείνουν ιδιωτικά και προστατευμένα από παράνομη αποκάλυψη τους σε τρίτους μη εξουσιοδοτημένους χρήστες.

Ακόμα υπάρχει η χρήση ψηφιακών πιστοποιητικών που παρέχονται από διάφορες αρχές πιστοποίησης (Certificate Authority), η χρήση συμμετρικής κρυπτογραφίας, υποδομής δημοσίου κλειδιού αλλά και υποστήριξη παραδοσιακών συστημάτων ασφαλείας (firewall, intrusion detection systems)
Όπως γίνεται αντιληπτό, η συνιστώσα αυτή της ασφάλειας στο περιβάλλον Grid Computing είναι υψίστης σημασίας και η 'παρουσίας' της σε αυτό κρίνεται επιτακτική.

2.2.6 Διεπιφάνεια Χρήστη (User Interface)

Η πρόσβαση στη πληροφορία του Grid είναι εξίσου σημαντική, και η διεπιφάνεια χρήστη είναι αυτή που τη χειρίζεται σύμφωνα με το [13] με 2 τρόπους:

1. Ένα interface που παρέχεται από την ίδια την εφαρμογή που τρέχει ο χρήστης
2. Ένα interface που παρέχεται από τον διαχειριστή του Grid , και μοιάζει με Web Portal που παρέχει πρόσβαση σε διαθέσιμες εφαρμογές και πόρους του Grid.

2.2.7 Διαχείριση Δεδομένων (Data Management)

Η διαχείριση δεδομένων είναι επίσης πολύ σημαντική υπηρεσία του Grid καθώς είναι σημαντική η αξιόπιστη διαχείριση και μεταφορά των δεδομένων μεταξύ των διαφόρων κόμβων του πλέγματος. Μάλιστα αυτή η υπηρεσία συνεργάζεται 'στενά' και με την αντίστοιχη της ασφάλειας, προκειμένου να εξασφαλιστεί εμπιστευτικότητα, ακεραιότητα, και αυθεντικοποίηση.

Ένα ιδανικό περιβάλλον πλέγματος, θα παρέχει πρόσβαση σε διαθέσιμους πόρους έτσι ώστε να ξεπεραστούν είτε φυσικές δυσκολίες, είτε ασυμβατότητες ανάμεσα σε διαφορετικές πλατφόρμες είτε οι δυσλειτουργίες δικτυακών πρωτοκόλλων.

Σύμφωνα λοιπόν με το [12] τα βασικά χαρακτηριστικά ή καλύτερα οι απαιτήσεις για τη σωστή σχεδίαση και υλοποίηση ενός πλέγματος υπολογιστική είναι τα εξής:

- **Διοικητική ιεραρχία (administrative hierarchy):** Μια τέτοια ιεραρχία είναι ο τρόπος με τον οποίο ένα πλέγμα διασπά τον εαυτό του προκειμένου να διευκολύνει τη διαχείριση των πόρων. Στην ουσία καθορίζει πως η διαχειρίσιμη πληροφορία 'ρέει' μέσα στο πλέγμα.

- **Υπηρεσίες επικοινωνίας (Communication Services):** Οι επικοινωνιακές απαιτήσεις εφαρμογών που χρησιμοποιούν το πλέγμα ποικίλουν από αξιόπιστες (point-to-point) μέχρι αναξιόπιστες (multicast). Η υποδομή της επικοινωνίας πρέπει να υποστηρίζει πρωτόκολλα που χρησιμοποιούνται για 'ογκώδεις' μεταδόσεις δεδομένων. Επίσης οι δικτυακές υπηρεσίες παρέχουν παραμέτρους QoS (Quality of Service) που σχετίζονται με το ρυθμό μετάδοσης, την καθυστέρηση, το ρυθμό λαθών, παράμετροι που οπωσδήποτε είναι σημαντικές για το υπολογιστική πλέγματος.

- **Υπηρεσίες πληροφόρησης (Information services):** Το πλέγμα είναι ένα δυναμικό περιβάλλον όπου η τοποθεσία και ο τύπος των διαθέσιμων υπηρεσιών συνεχώς αλλάζουν. Ένας βασικός στόχος είναι να κάνουμε όλους τους πόρους προσβάσιμους από κάθε διεργασία του συστήματος. Είναι απαραίτητη η υποστήριξη μηχανισμών που θα επιτρέπουν την εύκολη μετάδοση της πληροφορίας στις αιτούσες υπηρεσίες. Αυτή την απαίτηση την αναλαμβάνουν οι υπηρεσίες πληροφόρησης, σχετικά με την δομή του πλέγματος, τους πόρους, και τις καταστάσεις τους.

- **Υπηρεσίες ονομασίας (naming services):** Στο πλέγμα, όπως άλλωστε και σε κάθε κατανεμημένο σύστημα, χρησιμοποιούνται ονομασίες για να αναφέρονται σε μια ομάδα αντικειμένων όπως υπολογιστές, υπηρεσίες. αντικείμενα δεδομένων κτλ. Αυτές λοιπόν οι υπηρεσίες παρέχουν ένα ομοιόμορφο χώρο ονομάτων σε όλο το πλέγμα. Τυπικά οι υπηρεσίες αυτές παρέχονται από το διεθνές πρότυπο ονομασίας το X.500, DNS κτλ.

- **Συστήματα κατανεμημένων αρχείων (Distributed file systems and caching):** Οι κατανεμημένες εφαρμογές, τις περισσότερες φορές, απαιτούν πρόσβαση σε αρχεία που είναι διασκορπισμένα σε διάφορους εξυπηρετητές. Για αυτό το λόγο. ένα σύστημα κατανεμημένων αρχείων είναι απαραίτητο και βασικό .Ένα τέτοιο σύστημα υποστηρίζει ένα ενιαίο πρότυπο ονομασίας, ένα αριθμό I/O πρωτοκόλλων ανάγνωσης αρχείων και στην ουσία επιτρέπει την

βελτιστοποίηση στην λειτουργία ανάγνωσης αρχείων μέσα στο περιβάλλον του πλέγματος.

- **Ασφάλεια και εξουσιοδότηση (Security and authorization):** Κάθε κατανεμημένο σύστημα προϋποθέτει εμπιστευτικότητα, ακεραιότητα, αυθεντικοποίηση και υπευθυνότητα. Γενικά το θέμα της ασφάλειας σε περιβάλλον Grid είναι αρκετά πολύπλοκο, και θα το μελετήσουμε διεξοδικά σε μια άλλη ενότητα. Πάντως το κλειδί για την επιτυχία, σε αυτόν τον τομέα είναι η ύπαρξη υποδομής ασφάλειας.

- **Σύστημα μελέτης κατάστασης / ελέγχου λαθών (System status- fault tolerance):** Προκειμένου να παρέχουμε αξιόπιστο πλέγμα, είναι σημαντικό να υπάρχουν μηχανισμοί καταγραφής και ελέγχου της κατάστασης των πόρων και των εφαρμογών .

- **Χρονοπρογραμματισμός και διαχείριση πόρων (Resource management and scheduling):** Η διαχείριση του χρόνου επεξεργασίας, της μνήμης, του δικτύου και των άλλων συστατικών στο πλέγμα, είναι πολύ σημαντική. Ο συνολικός στόχος είναι να χρονο-προγραμματίσουμε ικανά και αποδοτικά τις εφαρμογές που χρειάζονται να κάνουν χρήση των διαθέσιμων πόρων του πλέγματος.

- **Υπολογιστική οικονομία και εμπορία πόρων (Computational economy and resource trading):** Καθώς ένα πλέγμα κατασκευάζεται από ενωμένους κατανεμημένους πόρους μεταξύ διαφορετικών οργανισμών, είναι σημαντική και αναγκαία η υποστήριξη μηχανισμών και πολιτικών που θα ορίζουν τους κανόνες που θα διέπουν την χρήση και τη διαμοίραση των πόρων, κάτι που είδαμε και πιο πάνω. Πιθανή λύση μπορεί να αποτελέσει μια οικονομική προσέγγιση σχετικά με την εμπορία πόρων , κάτι που θα βοηθούσε πολλούς οργανισμούς να αυξήσουν την αξία τους και τα κέρδη.

- **Εργαλεία προγραμματισμού (Programming tools):** Οι εφαρμογές πλέγματος ενώνουν τους πόρους που δεν μπορούν να αναπαραχθούν σε ένα μόνο site ή που δεν μπορούν να γίνουν προσβάσιμοι λόγω γεωγραφικής απόστασης. Για αυτό, το πλέγμα πρέπει να περιλαμβάνει διεπαφές, APIs, εργαλεία προκειμένου να παρέχει ένα περιβάλλον ανάπτυξη εφαρμογών π.χ C,C++, Java, MPI.
  Εκτός από τα καθεαυτού εργαλεία, πρέπει να υπάρχει και γραφική διεπιφάνεια διαχείρισης GUI που θα επιτρέψει την καλύτερη διαχείριση όλων των παραπάνω εφαρμογών.

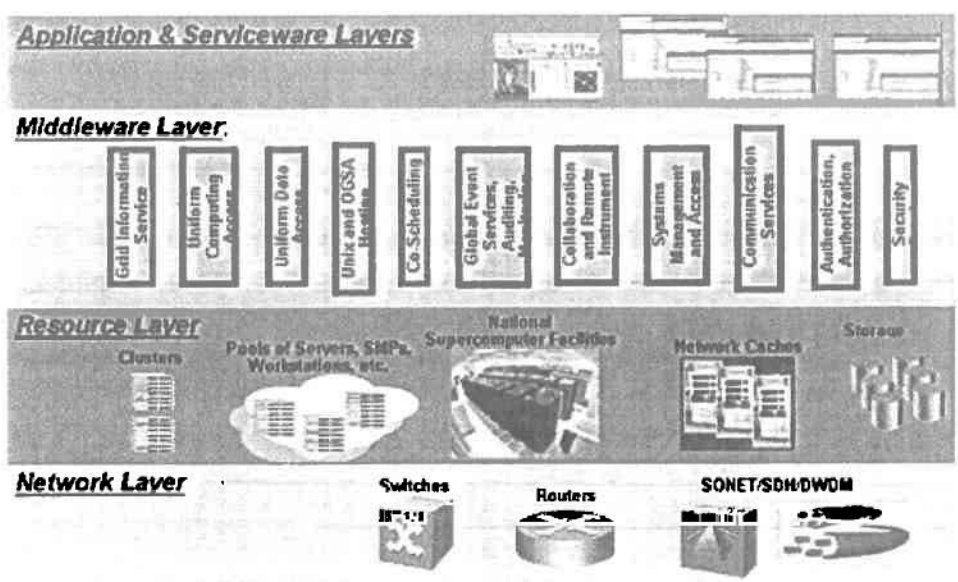
Συμπερασματικά, μελετήθηκαν κάποιες πτυχές που έχει η σχεδίαση ενός πλέγματος υπολογιστικής καθώς και οι απαιτήσεις που πρέπει να λάβει υπόψη του ο μηχανικός προκειμένου να φέρει εις πέρας το σκοπό του που δεν είναι άλλος από τη βέλτιστη εκμετάλλευση της υπολογιστικής πλέγματος.

2.3 ΠΡΟΕΠΙΣΚΟΠΗΣΗ ΤΩΝ ΣΥΣΤΑΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ (Grid Computing Components)

Η σχεδίαση ενός βιώσιμου υπολογιστικού πλέγματος (grid computing) δεν περιορίζεται μόνο στη ομαδοποίηση της επεξεργαστικής ισχύος μεμονωμένων μηχανών μέσω software. Υπάρχουν πολλαπλά επίπεδα, καθένα από τα οποία, παίζει σημαντικό ρόλο. Γενικά, τα υψηλότερα (στη ιεραρχία) επίπεδα είναι περισσότερο λογισμικο-κεντρικά (software-centric) ενώ τα χαμηλότερα είναι υλικο-κεντρικά (hardware-centric) [3].

2.3.1 Μια απλή προσέγγιση στην αρχιτεκτονική πλέγματος

Στη συγκεκριμένη ενότητα θα γίνει μια σύντομη πλην όμως κατανοητή περιγραφή των βασικών συστατικών από τα οποία αποτελείται μια αρχιτεκτονική πλέγματος.
Η παρακάτω εικόνα, σύμφωνα με το [3] παρέχει μια γραφική άποψη της αρχιτεκτονικής Grid Computing , ***κατανοητή περισσότερο στον απλό χρήστη του πλέγματος:***



Ενδεικτική αρχιτεκτονική του Grid Computing

Όπως φαίνεται και στην εικόνα, η αρχιτεκτονική πλέγματος αποτελείται από 4 επίπεδα (διατρέχοντας από κάτω προς τα πάνω):

1. **Επίπεδο δικτύου (Network Layer)**
2. **Επίπεδο πόρων (Resource Layer)**
3. **Επίπεδο ενδιάμεσου λογισμικού (Middleware layer)**
4. **Επίπεδο εφαρμογών και υπηρεσιών (Application & Serviceware Layer)**

Παρακάτω αναλύεται το κάθε ένα επίπεδο ξεχωριστά:

2.3.1.1 Επίπεδο δικτύου (Network Layer)

Το επίπεδο δικτύου είναι στην ουσία το υπόστρωμα διασυνδεσιμότητας μεταξύ των πόρων του πλέγματος. Σε αυτό περιλαμβάνονται όλες οι φυσικές διασυνδέσεις (ενσύρματες, καλώδια μισθωμένες γραμμές, οπτικές ίνες,..) και ο αντίστοιχος δικτυακός εξοπλισμός (routers, bridges, switches,...). Βέβαια για ευρείας περιοχής δίκτυα, τα γνωστά WAN (wide area network) δεν χρησιμοποιούνται απλές δικτυακές συνδέσεις, αλλά τεχνολογίες ικανές για μετάδοση και υποστήριξη υψηλού bandwidth όπως SONET / WDM (wavelength division multiplexing) γραμμές, που σε συνδυασμό με τους κατάλληλους routers θα παρέχουν άρτια σύνδεση ανάμεσα στους κόμβους του Grid, σε clusters, σε servers κτλ.

2.3.1.2 Επίπεδο πόρων (Resource Layer)

Το επίπεδο αυτό αποτελείται από όλους τους φυσικούς / υλικούς πόρους που απαρτίζουν το πλέγμα. Χαρακτηριστικά παραδείγματα τέτοιων πόρων είναι συστοιχίες υπολογιστών (clusters), servers,Hosts,σταθμοί εργασίας (workstations) , αποθηκευτικά συστήματα (storage systems) και δικτυακοί αισθητήρες (π.χ σε περιβάλλοντα πυρηνικών αντιδραστήρων).

2.3.1.3 Επίπεδο ενδιάμεσου λογισμικού (Middleware layer)

Αν γινόταν αξιολόγηση των επιπέδων του Grid Computing , θα μπορούσε να χαρακτηριστεί ίσως το πιο σημαντικό καθώς αποτελεί τον 'εγκέφαλο' του όλου συστήματος.
Πολλοί μάλιστα, ειδικοί αυτού του τομέα, το χαρακτηρίζουν σαν το κλειδί για την επιτυχία του Grid Computing , καθώς το λογισμικό (πρωτόκολλα, services) που υποστηρίζει οργανώνει και ενοποιεί εντελώς ανόμοιους πόρους του πλέγματος.
Το middleware layer παρέχει όλα εκείνα τα πρωτόκολλα και τους μηχανισμούς που επιτρέπουν στους πόρους (servers,δίκτυα,...) να συμμετέχουν στο ενοποιημένο περιβάλλον του πλέγματος.

Υπάρχουν πολλά τέτοια πρωτόκολλα και μηχανισμοί που σύμφωνα με το [15] παρέχουν υπηρεσίες :

- Ανάθεσης πόρων (resource allocation) και εξισορρόπησης φόρτου (load balancing)
- Χρονοπρογραμματισμού διεργασιών (Process Scheduling)
- Πρόσβασης πόρων
- Αυθεντικοποίησης, εξουσιοδότησης
- Παροχής Quality of Service
- Διαχείρισης πολιτικών χρήσης και ασφάλειας (policy management)

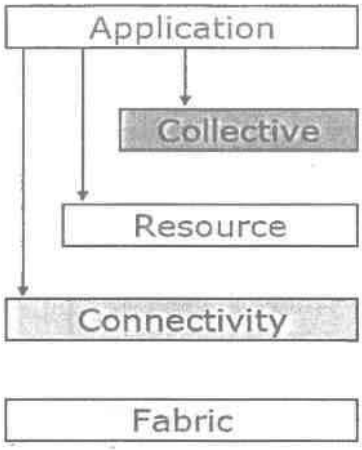
Η παροχή όλων των παραπάνω υπηρεσιών είναι αναγκαία.

2.3.1.4 Επίπεδο εφαρμογών και υπηρεσιών (Application & Serviceware Layer)

Το συγκεκριμένο επίπεδο είναι και το υψηλότερο στην ιεραρχία και όπως αναφέρθηκε πιο πάνω, σχετίζεται περισσότερο με το software παρά με το hardware. Αυτό το επίπεδο αποτελεί το πλαίσιο στο οποίο τελικά συνδέονται οι διάφορες εφαρμογές (υπολογισμοί, προσομοιώσεις,..) των διαφόρων επιστημονικών τομέων, καθώς και οι υπηρεσίες που οι χρήστες του Grid θέλουν να παρέχουν.
Εκτός των άλλων , περιλαμβάνει εργαλεία ανάπτυξης εφαρμογών για τις διάφορες εταιρείες που θέλουν να συμμετέχουν στο πλέγμα.
Όσο αφορά στο serviceware τμήμα του επιπέδου, αυτό παρέχει πολλές υπηρεσίες διαχείρισης όπως έκδοσης 'λογαριασμών', χρέωσης για συγκεκριμένους πόρους, μέτρησης της χρήσης τους, οι οποίες είναι εξίσου σημαντικές καθώς οι πόροι που 'εικονικοποιούνται' (virtualized) διαμοιράζονται ανάμεσα σε μεμονωμένους χρήστες, εταιρείες, οργανισμούς που είναι παγκόσμια διασπαρμένοι [7].

2.3.2 Μια διαφορετική προσέγγιση στην αρχιτεκτονική πλέγματος

Εκτός της παραπάνω προσέγγισης, οι ειδικοί χρησιμοποιούν μια διαφορετική προσέγγιση της ιεραρχίας των επιπέδων του πλέγματος, που φαίνεται στην εικόνα που ακολουθεί ([2],[7]):



Όπως μπορεί να παρατηρήσει κάποιος, υπάρχουν κάποιες ξεκάθαρες διαφορές οι οποίες θα γίνουν κατανοητές , αναλύοντας παρακάτω καθένα από αυτά τα επίπεδα.

2.3.2.1 Επίπεδο δομής-συγκρότησης (fabric layer)

Το συγκεκριμένο επίπεδο παρέχει όλους τους πόρους στους οποίους, τα διάφορα πρωτόκολλα του Grid, θα επιτρέψουν την πρόσβαση από τους χρήστες. Τέτοιοι πόροι είναι υπολογιστές, αποθηκευτικά συστήματα. servers, κατάλογοι αρχείων, δικτυακοί πόροι κτλ. **Σε αντιστοίχηση με την πρώτη προσέγγιση αρχιτεκτονικής, μπορούμε να πούμε ότι αποτελεί μια συνένωση των επιπέδων του δικτύου και των πόρων** .
Τα συστατικά μέρη αυτού του επιπέδου. εφαρμόζουν διάφορες λειτουργίες που έχουν να κάνουν κυρίως με την πρόσβαση και την χρήση των πόρων.

2.3.2.2 Επίπεδο σύνδεσης (connectivity layer)

Βασικός στόχος του συγκεκριμένου επιπέδου είναι η εύκολη και ασφαλής επικοινωνίας. Καθορίζει πρωτόκολλα επικοινωνίας και αυθεντικοποίησης που είναι αναγκαία για δικτυακές συναλλαγές, κυρίως μεταξύ των πόρων του επιπέδου δομής.
Τα πρωτόκολλα αυθεντικοποίησης, στηρίζονται πάνω σε υπηρεσίες επικοινωνιών και παρέχουν ασφαλής μηχανισμούς , προκειμένου να εξακριβωθεί η ταυτότητα χρηστών και πόρων.

2.3.2.3 Επίπεδο διαχείρισης πόρων (Resource layer)

Το συγκεκριμένο επίπεδο στηρίζεται πάνω στο Connectivity layer. Περιλαμβάνει και αυτό πρωτόκολλα ασφαλής επικοινωνίας, αρχικοποίησης, ελέγχου, και χρέωσης της πρόσβασης και χρήσης **μεμονωμένων πόρων**. Πως λειτουργεί όμως αυτός ο μηχανισμός;

Σύμφωνα με το [2] οι υλοποιήσεις των πρωτοκόλλων αυτού του επιπέδου, καλούν συναρτήσεις (πρωτοκόλλων) του Fabric επιπέδου προκειμένου να υπάρξει πρόσβαση και έλεγχος στους τοπικούς πόρους. Τα συγκεκριμένα πρωτόκολλα του Resource layer, **τονίζουμε ότι έχουν να κάνουν μόνο με μεμονωμένους πόρους και όχι με κατανεμημένους ή κοινά χρησιμοποιήσιμους πόρους. Αυτό αφορά το συγκεντρωτικό επίπεδο (collective layer) που αναλύεται πιο κάτω.**

Υπάρχουν 2 βασικές κατηγορίες Resource layer πρωτοκόλλων που σύμφωνα με το [2] είναι οι εξής :

- **Πρωτόκολλα πληροφορίας (information protocols)**: Χρησιμοποιούνται για να λαμβάνουν πληροφορίες σχετικά με την δομή και την κατάσταση των πόρων π.χ την διαμόρφωσή τους, τον τρέχων φόρτο εργασίας , την πολιτική χρήσης κτλ.

- **Πρωτόκολλα διαχείρισης (management protocols)**: Χρησιμοποιούνται, προκειμένου να διαπραγματευτούν την πρόσβαση σε ένα κοινά χρησιμοποιήσιμο πόρο, καθορίζοντας τις όποιες προϋποθέσεις / απαιτήσεις. Συνεπώς τα συγκεκριμένα πρωτόκολλα πρέπει να λειτουργούν ως σημεία εφαρμογής πολιτικών ασφάλειας, εξασφαλίζοντας ότι οι όποιες αιτήσεις (για πρόσβαση σε πόρους) των πρωτοκόλλων , συμβαδίζουν με την πολιτική χρήσης και ασφάλειά τους.

2.3.2.4 Επίπεδο συλλογικής διαχείρισης (Collective layer)

Ο ελληνικός όρος δεν είναι και πολύ επιτυχημένος, έτσι θα χρησιμοποιούμε τον αγγλικό. Το συγκεκριμένο λοιπόν επίπεδο, έρχεται να συμπληρώσει την λειτουργία του προηγούμενου επιπέδου, που εστίαζε στους μεμονωμένους πόρους.
Το Collective layer περιλαμβάνει και αυτό με τη σειρά του διάφορα πρωτόκολλα και υπηρεσίες, που είναι 'οικουμενικής' (global) φύσεως , ελέγχοντας τις συναλλαγές μεταξύ ομάδων-συστοιχιών πόρων. Με λίγα λόγια, ότι δεν κάνει το Resource layer.

Ακόμα, το Collective layer στηρίζεται σε πρωτόκολλα πληροφορίας (όπως και το προηγούμενο) με την βοήθεια των οποίων αποκτούν πληροφορίες για την δομή και την τρέχουσα κατάσταση των πόρων του πλέγματος.

2.3.2.5 Επίπεδο εφαρμογής (application layer)

Όπως στις περισσότερες προσεγγίσεις, έτσι και σε αυτήν το υψηλότερο επίπεδο είναι αυτό των εφαρμογών. Οι εφαρμογές βασίζονται πάνω στα κατώτερα επίπεδα προκειμένου να μπορέσουν να εκτελεστούν στο πλέγμα. Αυτές οι εφαρμογές ως επί το πλείστον εκτελούνται μέσα στο περιβάλλον των εικονικών οργανισμών (virtual organization), καλώντας υπηρεσίες και πρωτόκολλα χαμηλότερων επιπέδων ,που αυτά με τη σειρά τους επιτρέπουν (ανάλογα και με την περίπτωση) , διαχείριση, πρόσβαση πόρων κτλ.

2.4 ΠΡΟΕΠΙΣΚΟΠΗΣΗ ΤΩΝ ΕΦΑΡΜΟΓΩΝ ΤΟΥ ΠΛΕΓΜΑΤΟΣ (Grid Computing Applications)

2.4.1 Εφαρμογές υπολογιστικής πλέγματος

Αναμφισβήτητα, με την ραγδαία εξέλιξη της τεχνολογίας σε όλους σχεδόν τους τομείς (Υλικού, Λογισμικού, Δικτύων, Υπηρεσιών), αυξήθηκαν και οι απαιτήσεις πολλών επιστημονικών εφαρμογών, για υπολογιστική ισχύ, για μεγάλους αποθηκευτικούς χώρους , γρήγορες δικτυακές ταχύτητες κτλ. Παρατηρείται λοιπόν μια κατηγοριοποίηση των εφαρμογών του Grid Computing , ανάλογα και με τις ιδιαίτερες απαιτήσεις-ανάγκες των εφαρμογών.

Οι βασικές κατηγορίες, σύμφωνα με το [10] φαίνονται στον ακόλουθο πίνακα:

ΚΑΤΗΓΟΡΙΑ	ΠΑΡΑΔΕΙΓΜΑΤΑ	ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ
Κατανεμημένη υπολογιστική	**DIS,Αστροφυσικές μελέτες,**	**Προβλήματα με μεγάλες απαιτήσεις σε CPU, μνήμη**
Υψηλή απόδοση	**Σχεδιασμός κυκλωμάτων Μελέτη παραμέτρων, προβλήματα Κρυπτογράφησης**	**Συγκέντρωση πολλών αδρανών πόρων για αύξηση υπολογιστικής απόδοσης**
Κατ'απαίτηση(on demand)	**Ιατρικοί έλεγχοι συστημάτων, Πρόγνωση Καιρού**	**Απομακρυσμένη πρόσβαση σε πόρους για περιορισμένο χρονικό διάστημα**
Διεξοδικών Δεδομένων	**Παρατήρηση καιρικών φαινομένων, Δεδομένα Φυσικής**	**Σύνθεση πληροφοριών από μεγάλες αποθήκες δεδομένων**
Εφαρμογές Σύμπραξης	**Εξόρυξη-Εξερεύνηση γνώσης**	**Υποστήριξη επικοινωνίας μεταξύ πολλών επιστημόνων για συνεργασία.**

2.4.1.1 Κατανεμημένη υπερ-υπολογιστική (Distributed SuperComputing)

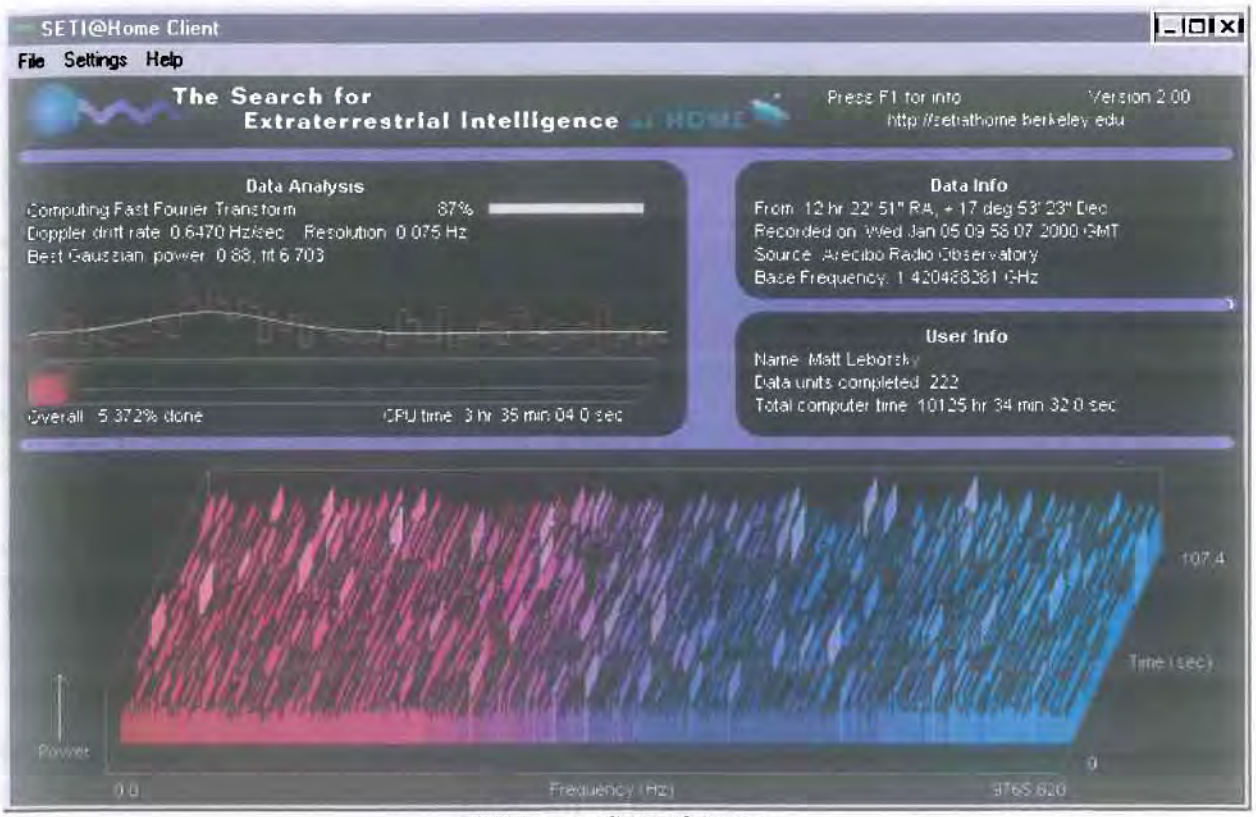
Οι εφαρμογές κατανεμημένης υπερ-υπολογιστικής, χρησιμοποιούν το πλέγμα για να συλλέξουν σημαντικούς υπολογιστικούς πόρους προκειμένου να αντιμετωπίσουν αποτελεσματικά, προβλήματα που δεν μπορούν να λυθούν σε ένα μεμονωμένο σύστημα. Ανάλογα βέβαια και με τα χαρακτηριστικά του πλέγματος, αυτοί οι πόροι μπορούν να περιλαμβάνουν την πλειοψηφία των υπερ-υπολογιστών μιας χώρας ή μιας εταιρείας.

Ορισμένα σύγχρονα παραδείγματα τέτοιων εφαρμογών είναι τα εξής [10]:

- **Κατανεμημένη διαδραστική προσομοίωση (DIS)**: είναι μια τεχνική για εκπαίδευση και για σχεδιασμό ενεργειών στον στρατό. Τα πραγματικά σενάρια που εξετάζονται, μπορεί να περιλαμβάνουν εκατοντάδες χιλιάδες οντότητες (πρόσωπα, σώματα στρατού,..) καθένα εκ των οποίων έχει περίπλοκες δομές. Ακόμα και οι σύγχρονοι υπερ-υπολογιστές μπορούν να διαχειριστούν 20000 οντότητες. Σε πρόσφατες έρευνες, ερευνητές στο πανεπιστήμιο στη Καλιφόρνια, έδειξαν πως πολλαπλοί υπερ-υπολογιστές μπορούν όταν συνδέονται, να επιτύχουν εξωπραγματικές αποδόσεις .

- **Η επακριβής προσομοίωση σύνθετων φυσικών φαινομένων** , μπορεί να απαιτεί μεγάλη αποθηκευτική και υπολογιστική ικανότητα για ακριβή αποτελέσματα. Συνδέοντας λοιπόν υπερ-υπολογιστές, μπορούν να ξεπεραστούν τα όποια προβλήματα, και να παραχθούν ικανοποιητικά επιστημονικά αποτελέσματα. Αν και μεγάλες καθυστερήσεις μπορούν να δυσχεραίνουν το έργο των επιστημόνων , οι συνδεδεμένοι υπερυπολογιστές έχουν λειτουργήσει επιτυχώς σε τομείς όπως κοσμολογία, προβλήματα χημικών αναλύσεων, μοντελοποίηση κλίματος κτλ.

- Επίσης ένα από τα πολύ γνωστά project που ανήκουν σε αυτήν την κατηγορία είναι το **SETI@home**. Πρόκειται για ένα πλέγμα **κατανεμημένης υπολογιστικής**, που χρησιμοποιεί υπολογιστές σε σπίτια σε γραφεία σε όλο τον κόσμο, και αναλύει τα σήματα ραδιοτηλεσκόπιου. Παρ'όλες τις δυσκολίες που μπορεί να έχει αυτό το εγχείρημα, υπάρχει αξιοσημείωτη υπολογιστική ισχύς. Σκοπός του όλου project είναι να ανιχνεύσει ευφυή εξωγήινη ζωή στο διάστημα. Αυτό που κάνει είναι να 'ακούει' **περιορισμένου εύρους ραδιοσήματα** που είναι σπάνια. Πολλοί μάλιστα ονομάζουν αυτό το project σαν υπολογιστική κοινών πόρων (public resource computing) ακριβώς γιατί οι κατανεμημένοι πόροι προέρχονται από τους ανθρώπους. Αξίζει να σημειωθεί η ανταπόκριση του κόσμου, που τον Ιούλιο του 2002 έφτασε σχεδόν τα 4.000.000 χρήστες .



Οθόνη του SETI@home

Οι προκλήσεις που πρέπει να αντιμετωπιστούν σε αυτού του είδους τις εφαρμογές, από αρχιτεκτονικής απόψεως, έχουν να κάνουν με την ανάγκη για καθορισμό πρωτοκόλλων, αλγορίθμων που μέσω του κατάλληλου χρονοπρογραμματισμού, θα επιτρέψει να επιτευχθούν υψηλοί ρυθμοί απόδοσης μεταξύ ετερογενών συστημάτων.[10]

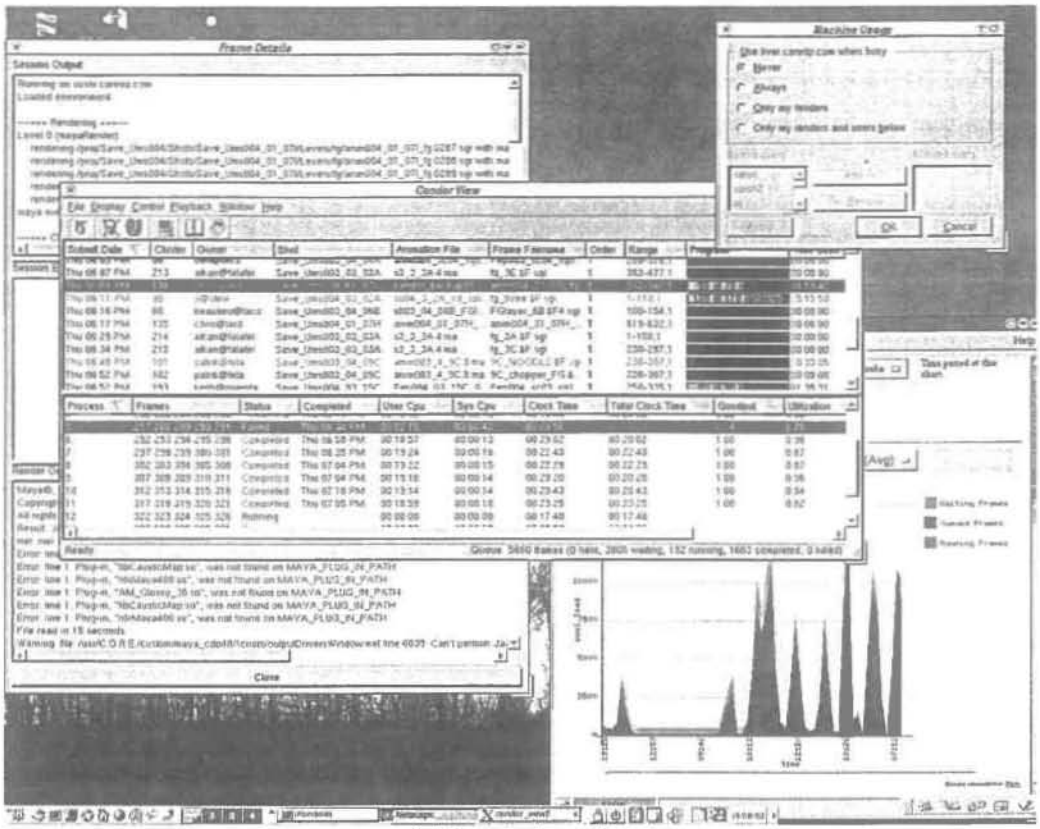
2.4.1.2 Υπολογιστική υψηλής απόδοσης (high throughput Computing)

Στη συγκεκριμένη κατηγορία υπολογιστικής, το πλέγμα χρησιμοποιείται για να προγραμματίσει ένα μεγάλο αριθμό 'χαλαρά' συνδεδεμένων ή εντελώς ανεξάρτητων εργασιών , με στόχο να εκμεταλλευτεί την χαμένη επεξεργαστική ισχύ (συνήθως από αδρανείς σταθμούς εργασίας). Το αποτέλεσμα, όπως άλλωστε και στην κατανεμημένη υπερυπολογιστική, είναι η 'εστίαση' των πόρων σε ένα συγκεκριμένο πρόβλημα,. Μερικά χαρακτηριστικά παραδείγματα είναι τα εξής [10]:

- Σχεδιασμός ψηφιακών κυκλωμάτων / επεξεργαστών: Η εταιρεία Platform Computing Corporation αναφέρει ότι η Advanced MicroDevices , που ειδικεύεται στην κατασκευή μικροεπεξεργαστών , χρησιμοποίησε συστήματα υπολογιστικής υψηλής απόδοσης για να εκμεταλλευθεί την ισχύ των επεξεργαστών K6, K7, που βρίσκονταν σε επιτραπέζιους υπολογιστές μηχανικών της AMD και γινόταν χρήση τους, μόνο όταν δεν χρησιμοποιούνταν από τους ίδιους τους μηχανικούς.

- Το σύστημα **Condor** που αναπτύχθηκε από το πανεπιστήμιο του Wisconsin , χρησιμοποιείται για την διαχείριση ομάδων εκατοντάδων σταθμών εργασίας σε πανεπιστήμια και σε εργαστήρια σε όλο τον κόσμο.

  Αυτοί οι πόροι χρησιμοποιήθηκαν για μελέτες που σχετίζονταν με μοριακές προσομοιώσεις υγρών κρυστάλλων, με μελέτες διαπεραστικών radar καθώς και με το σχεδιασμό μηχανών πετρελαίου.



Οθόνη από το Condor

- Επίσης, έχουν αναφερθεί εφαρμογές που συνέδεαν χιλιάδες υπολογιστές διασπαρμένους σε όλο τον κόσμο, προκειμένου να λύσουν σύνθετα προβλήματα κρυπτογραφίας.

2.4.1.3 Υπολογιστική κατ'απαίτηση (On demand Computing)

Οι εφαρμογές που ανήκουν στη συγκεκριμένη κατηγορία, εκμεταλλεύονται την ικανότητα του πλέγματος να ανταποκρίνεται στην απαίτηση για πόρους που δεν θα κοστίζουν πολύ. Αυτοί οι πόροι μπορεί να είναι υπολογιστικοί (επεξεργαστές), λογισμικό, αποθήκες δεδομένων, ειδικοί αισθητήρες και άλλοι.
Σε αντίθεση με την κατανεμημένη υπερ-υπολογιστική , αυτού του είδους οι εφαρμογές έχουν περισσότερο, σαν βασικό τους μέλημα τη μείωση του κόστους, παρά την επίτευξη μεγάλης υπολογιστικής απόδοσης.[10]
Π.χ

- Το NEOS και NetSolve: πρόκειται για συστήματα επίλυσης αριθμητικών προβλημάτων βασισμένα σε δίκτυο. Επιτρέπουν στους χρήστες να συνδέουν απομακρυσμένους πόρους δια μέσου κατάλληλου λογισμικού , να συνδέονται

σε απομακρυσμένους servers για να εκτελέσουν υπολογισμούς που έχουν υψηλές απαιτήσεις σε hardware ή σε λογισμικό.

- Μια υπολογιστική μηχανή MRI και ένα μικροσκόπιο σάρωσης αναπτύχθηκαν στο Εθνικό Κέντρο για εφαρμογές υπερυπολογιστικής. Και τα δύο χρησιμοποιούν υπερυπολογιστές για να επιτύχουν επεξεργασία εικόνας σε πραγματικό χρόνο. Το αποτέλεσμα, είναι μια σημαντική βελτίωση στην ικανότητα να κατανοούμε αυτό που βλέπουμε.

- Σύστημα που αναπτύχθηκε στην αεροδιαστημική βιομηχανία, για την επεξεργασία δεδομένων από μετεωρολογικούς δορυφόρους. Και αυτό , όπως και τα προηγούμενα, χρησιμοποιεί δυναμικά δεσμευμένους υπέρ-υπολογιστικούς πόρους για να παρέχει τα αποτελέσματα ενός αλγορίθμου ανίχνευσης σύννεφων σε απομακρυσμένους μετεωρολόγους σε σχεδόν πραγματικό χρόνο.

Οι προκλήσεις που πρέπει να αντιμετωπιστούν σε αυτού του είδους τις εφαρμογές προέρχονται από τη δυναμική φύση των απαιτήσεων σε πόρους, και προφανώς από τον μεγάλο αριθμό χρηστών και πόρων. Αυτές οι προκλήσεις σύμφωνα με το [10] περιλαμβάνουν ανάθεση πόρων, χρονοπρογραμματισμός, διαχείριση κώδικα, διαμόρφωση, εξέταση ανοχής σε σφάλματα, ασφάλεια και τέλος μηχανισμούς χρέωσης .

2.4.1.4 Υπολογιστική διεξοδικών δεδομένων (Data-Intensive Computing)

Το σημείο στο οποίο εστιάζουν οι εφαρμογές Data-Intensive , είναι η σύνθεση και η παραγωγή νέας πληροφορίας από δεδομένα που είναι αποθηκευμένα σε γεωγραφικά κατανεμημένες αποθήκες δεδομένων , ψηφιακές βιβλιοθήκες και βάσεις δεδομένων.
Αυτή η διαδικασία σύνθεσης είναι υπολογιστικά και επικοινωνιακά διεξοδική-αναλυτική. Χαρακτηριστικά παραδείγματα παραθέτονται από το [10] παρακάτω:

- Μελλοντικά πειράματα πάνω στη φυσική υψηλής ενέργειας, θα δημιουργούν καθημερινώς terabytes δεδομένων ή περίπου ένα petabyte κάθε χρόνο. Τα περίπλοκα ερωτήματα, που χρησιμοποιούνται για την ανίχνευση «ενδιαφερόντων» γεγονότων , ίσως να χρειάζονται πρόσβαση σε μεγάλα τμήματα των δεδομένων. Οι επιστημονικοί συνεργάτες που θα έχουν πρόσβαση σε αυτά τα δεδομένα, είναι διασπαρμένοι σε όλο τον κόσμο, και εκτός από αυτούς, διασπαρμένα είναι και τα ίδια τα συστήματα στα οποία βρίσκονται τα δεδομένα. Συνεπώς γίνεται χρήση του πλέγματος υπολογιστικής για να αντιμετωπιστούν οι όποιες δυσκολίες.

- Η ψηφιακή χαρτογράφηση του ουρανού, ανήκει και αυτή με την σειρά της στη συγκεκριμένη κατηγορία. Παράγει πολλά terabytes δεδομένων που προέρχονται από αστρονομικές φωτογραφίες, που είναι διαθέσιμες σε πολυάριθμες βάσεις δεδομένων που είναι προσβάσιμες μέσω δικτύου. Αυτός ο μηχανισμός του Grid Computing ανοίγει νέους ορίζοντες στη αστρονομική έρευνα που βασίζεται σε κατανεμημένη ανάλυση , με την προϋπόθεση ότι υπάρχουν και είναι διαθέσιμοι οι κατάλληλοι πόροι.

- Τα μοντέρνα συστήματα πρόγνωσης του καιρού, κάνουν εκτεταμένη μελέτη δεδομένων για την εκμετάλλευση των δορυφορικών παρατηρήσεων. Πιο συγκεκριμένα, η πλήρης διαδικασία απαιτεί την μετακίνηση και επεξεργασία πολλών gigabytes δεδομένων.

2.4.1.5 Υπολογιστική σύμπραξης (Collaborative Computing)

Η τελευταία λοιπόν κατηγορία, με βάση το [10] είναι η υπολογιστική σύμπραξης. Οι εφαρμογές αυτού του είδους εστιάζουν κυρίως στις ανθρώπινες αλληλεπιδράσεις. Και 'ασχολούνται' με την 'ενεργοποίηση' της δυνατότητας για κοινή χρήση υπολογιστικών πόρων (μέσω συνεργασίας) έτσι όπως συμβαίνει με τα κοινώς χρησιμοποιήσιμα αρχεία και τις προσομοιώσεις. Σε μια τέτοια περίπτωση, οι εφαρμογές παρουσιάζουν κοινά χαρακτηριστικά και με τις άλλες κατηγορίες εφαρμογών Grid που παρουσιάστηκαν πιο πάνω. Χαρακτηριστικές εφαρμογές σύμφωνα με το [10] είναι οι παρακάτω:

- Το σύστημα BoilerMaker, που αναπτύχθηκε στο Argonne National Laboratory,επιτρέπει πολλαπλούς χρήστες να συνεργάζονται για την σχεδίαση συστημάτων έκλυσης ρύπων σε βιομηχανικούς αποτεφρωτήρες. Κάθε ένας χρήστης αλληλεπιδρά με τους υπόλοιπους και με τον προσομοιωτή αποτεφρωτήρα.

- Το CAVE5D είναι σύστημα που υποστηρίζει συνεργασία για απομακρυσμένη εξερεύνηση μεγάλων συνόλων γεωφυσικών δεδομένων καθώς και των μοντέλων που τα παράγουν.

- Το NICE είναι σύστημα που αναπτύχθηκε στο πανεπιστήμιο του Ιλινόϊς στο Σικάγο, και επιτρέπει στα παιδιά να συμμετέχουν στην δημιουργία και τη συντήρηση εικονικών κόσμων, προορισμένους για διασκέδαση και εκπαίδευση.

- Στην Ευρώπη ένα από τα πολλά ευρωπαϊκά ερευνητικά προγράμματα, είναι και το έργο E-LeGI που έχει ως στόχο την σχεδίαση και ανάπτυξη προηγμένων εφαρμογών εκπαίδευσης βασισμένων στην τεχνολογία του σημασιολογικού GRID. Το έργο έχει υιοθετήσει ένα νέο μοντέλο εκπαίδευσης βασισμένο τη γνώση και σε τεχνολογίες συνεργασίας (collaborative learning).[DSMC έρευνα και ανάπτυξη].

Οι προκλήσεις, που καλούνται να αντιμετωπίσουν οι εφαρμογές σύμπραξης, σχετίζονται κυρίως με τις αντιληπτικές και αλληλεπιδραστικές ικανότητες των ανθρώπων.
Μετά την παρουσίαση των κατηγοριών των εφαρμογών Grid , υπάρχουν 3 παρατηρήσεις :

1. Παρόλη τη σχετικά σύντομη περιγραφή αυτών των κατηγοριών , παρατηρούμε μια πολύ μεγάλη ποικιλία επιτυχημένων εφαρμογών. Αυτές οι εφαρμογές αναπτύχθηκαν παρ'όλες τις σημαντικές δυσκολίες, που συνάντησαν οι προγραμματιστές.

2. Παρατηρείται ότι όλες σχεδόν οι εφαρμογές έχουν τεράστιες απαιτήσεις σε υπολογιστικούς πόρους (επεξεργαστές, μνήμη, δίσκους,κτλ), που δεν πρόκειται να υπάρξουν σε μεμονωμένα συστήματα ενός χρήστη. Αυτό από μόνο του τονίζει την σημασία των τεχνολογιών πλέγματος, όσο αφορά την διαμοίραση των πόρων και την πρόσβαση στα δεδομένα.

3. Τέλος, παρατηρείται ότι πολλές από τις εφαρμογές είναι είτε διαδραστικές είτε βασίζονται σε συγχρονισμό μεταξύ των υπολογιστικών πόρων –χρηστών.

2.4 Η ΕΝΝΟΙΑ 'ΕΙΚΟΝΙΚΟΣ ΟΡΓΑΝΙΣΜΟΣ' (VIRTUAL ORGANIZATIONS)

Μία πολύ σημαντική συνεισφορά του Grid Computing, σύμφωνα με το [1] είναι η δυνατότητα που αυτό προσφέρει για απλοποιημένη (όσο το δυνατό) συνεργασία μεταξύ ενός ευρύτερου συνόλου χρηστών. Στο παρελθόν, η κατανεμημένη υπολογιστική (distributed computing) κατάφερε ως ένα βαθμό να συμβάλλει στην ανάπτυξη της συνεργασίας. Το Grid Computing, εκμεταλλεύτηκε τις ήδη υπάρχουσες δυνατότητες, παρέχοντας καλύτερα πρότυπα, που επιτρέπουν ετερογενή συστήματα να δουλεύουν , φτιάχνοντας ένα ενιαίο εικονικό σύστημα.
Το πραγματικό πρόβλημα ,που είναι και η βασική έννοια του πλέγματος είναι ***η συντονισμένη διανομή-διαμοίραση πόρων και η επίλυση προβλημάτων σε δυναμικούς πολυ-ιδρυματικούς εικονικούς οργανισμούς***.[2]

Η διανομή των πόρων , δεν σχετίζεται τόσο πολύ με απλή ανταλλαγή αρχείων , όσο με την άμεση πρόσβαση σε υπολογιστές, λογισμικό, βάσεις δεδομένων, και σε άλλους πόρους. Καθορίζεται συνήθως από προβλήματα σε διάφορους επιστημονικούς τομείς (π.χ ιατρική, φυσική, βιοτεχνολογία κτλ) που η λύση τους απαιτεί συνεργασία. Βασικό ρόλο σε αυτή τη διαδικασία παίζουν, όπως είναι φυσικό , οι ίδιοι οι πάροχοι των πόρων , που οφείλουν να καθορίσουν σε ποιον και που επιτρέπεται η πρόσβαση.

2.5.1 Ορισμός

Από τα παραπάνω, γίνεται αντιληπτό ότι οι χρήστες ενός πλέγματος υπολογιστικής, μπορούν να οργανωθούν δυναμικά σε ένα αριθμό εικονικών οργανισμών, καθένας εκ των οποίων έχει διαφορετική πολιτική χρήσης και ασφάλειας.
Σύμφωνα λοιπόν και με τα [2,8], **εικονικός οργανισμός είναι ένα σύνολο είτε μεμονωμένων χρηστών είτε διαφόρων οργανισμών / εταιρειών ή ινστιτούτων, που μέσω του πλέγματος , συνεργάζονται για την επίλυση δύσκολων και απαιτητικών επιστημονικών προβλημάτων.**

Ένας διαφορετικός ορισμός δίνεται στο [18]:

«Εικονικός οργανισμός,˙ είναι μια αφηρημένη έννοια, που συμβάλλει στην μοντελοποίηση του κατανεμημένου διαμοιρασμού και ανάθεσης πόρων ανάμεσα σε διαφορετικούς οργανισμούς, εταιρείες κτλ.»

Επιπροσθέτως αναφέρονται κάποια παραδείγματα εικονικών οργανισμών όπως είναι οι πάροχοι εφαρμογών / υπηρεσιών, οι πάροχοι αποθηκευτικών χώρων, οι πάροχοι υπολογιστικών πόρων μέσω συστημάτων κτλ. [2]

2.5.2 Η ανάγκη για εικονικούς οργανισμούς

Παρ'όλους τους ορισμούς για την συγκεκριμένη έννοια, δεν γίνεται αμέσως αντιληπτή η σημασία των εικονικών οργανισμών. Για αυτό το λόγο παραθέτουμε παρακάτω κάποια πιθανά πρακτικά σενάρια που υποδεικνύουν τη χρησιμότητά τους :

- Μια επιχείρηση, χρειάζεται να πάρει μια απόφαση, για το που θα κτίσει το νέο της εργοστάσιο. Έτσι χρησιμοποιεί κάποια εξελιγμένα οικονομικά προγνωστικά μοντέλα, παρέχοντας ταυτόχρονα πρόσβαση σε κατάλληλα ιδιοκτησιακά ιστορικά δεδομένα, από επιχειρησιακές βάσεις δεδομένων . Κατά τη διάρκεια της συνάντησης για τη λήψη της απόφασης, 'τρέχουν' κάποια υποθετικά σενάρια, προκειμένου να καλύψουν όλες τις συμφέρουσες για την εταιρεία , περιπτώσεις. Αυτά τα σενάρια απαιτούν συνεργασία και διαδραστικότητα, παρόλο που τα συστήματα και κατά προέκταση οι χρήστες τους, βρίσκονται γεωγραφικά διασπαρμένοι.

- Μια κατασκευαστική κοινοπραξία, αποφάσισε να κάνει μια μελέτη για ένα υπερηχητικό αεροσκάφος επόμενης γενιάς. Η όλη διαδικασία, απαιτεί ακριβή ως προς τα αποτελέσματα, προσομοίωση για κάθε ένα κομμάτι του αεροσκάφους. Η προσομοίωση αυτή, ενώνει διάφορα τμήματα λογισμικού, που αναπτύχθηκαν σε διάφορους συμμετέχοντες της μελέτης π.χ τους ερευνητές του κινητήρα, της αεροδυναμικής του αεροσκάφους, της ασφάλειας κτλ.

- Μια ομάδα διαχείρισης κρίσεων, ανταποκρίνεται σε ένα περιστατικό διαρροής χημικών αερίων, κάνοντας χρήση των μοντέλων πρόγνωσης καιρού αλλά και των μοντέλων επεξεργασίας υπεδάφους, προκειμένου να υπολογίσουν πλήρως την ταχύτητα και τη διεύθυνση εξάπλωσης των ουσιών, λαμβάνοντας υπόψη και τα πληθυσμιακά στατιστικά της περιοχής. Για να δημιουργήσουν ένα πλάνο αντιμετώπισης του περιστατικού, χρειάζεται συντονισμένος διαμοιρασμός στοιχείων, δεδομένων και πόρων (π.χ χημικοί αισθητήρες.)

- Χιλιάδες επιστήμονες της φυσικής, εργαζόμενοι σε εκατοντάδες εργαστήρια σε όλο τον κόσμο, συνεργάζονται για να φέρουν εις πέρας διάφορες επιστημονικές μελέτες όπως συμβαίνει π.χ στο CERN,. Κατά τη διάρκεια της ανάλυσης δεδομένων, ομαδοποιούν τους πόρους δημιουργώντας ένα τεράστιο δίκτυο δεδομένων.

Όπως δείχνουν τα παραπάνω παραδείγματα, οι εικονικοί οργανισμοί ποικίλουν σημαντικά ως προς τον σκοπό τους, το μέγεθός τους , και γενικά την δομή τους.

2.5.3 Δυνατότητες εικονικών οργανισμών

Όπως αναφέρεται και στο [8] τα μέλη ενός εικονικού οργανισμού έχουν τη δυνατότητα:

- Να δημοσιεύσουν νέα δεδομένα που θα προέρχονται από τις πιο πρόσφατες μελέτες τους.
- Να εντοπίζουν δεδομένα με βάση κάποια ιδιαίτερα κριτήρια
- Να ανακτούν συγκεκριμένα δεδομένα που τους ενδιαφέρουν
- Να εντοπίζουν κατάλληλους υπολογιστικούς πόρους, προκειμένου να 'τρέξουν' κάποια προσομοίωση.
- Να ενημερώνονται τακτικά για νέα δεδομένα. π.χ στο project GriPhyn αν ένας χρήστης κάνει υπολογισμούς και παράγει δεδομένα, οφείλει να τα δημοσιεύσει, αποθηκεύοντάς τα σε πόρους, ώστε και χρήστες από άλλους εικονικούς οργανισμούς, να μπορούν να τα χρησιμοποιούν χωρίς να σπαταλούν χρόνο και κόπο σε ανώφελους υπολογισμούς.

Εν κατακλείδι , το βασικό χαρακτηριστικό των εικονικών οργανισμών είναι , και πρέπει να είναι η συνεργασία .

2.6 ΑΡΧΙΤΕΚΤΟΝΙΚΑ ΜΟΝΤΕΛΑ ΠΛΕΓΜΑΤΟΣ (Grid Architecture models)

Η τεχνολογία της υπολογιστικής πλέγματος, 'βρίσκεται εν τω μέσω' διαφορετικών ερευνητικών κοινοτήτων, όπου βασικό ρόλο παίζει η απάντηση στο ερώτημα 'Τι είναι πλέγμα'. Σε αυτές τις κοινότητες, περιλαμβάνονται υπολογιστο-κεντρικές (computer centric), peer-to-peer, ερευνητικές ομάδες με πολλές διαφορές στην φιλοσοφία τους. Καθεμιά από αυτές μπορεί να χρησιμοποιεί διαφορετικό μοντέλο για την τεχνολογία πλέγματος.
Η έννοια της υπολογιστικής πλέγματος, είναι σχετικά νέα στην βιομηχανία. Η επιλογή του πλέγματος από μια εταιρεία, εξαρτάται από την ικανότητα της τεχνολογίας να αυξάνει την επιχειρηματική της αξίας. [16]
Σε αυτήν την ενότητα θα εστιάσουμε την προσοχή μας σε διάφορα αρχιτεκτονικά μοντέλα, και θα περιγράψουμε τα κύρια χαρακτηριστικά τους καθώς και τα πρότυπα τα οποία ακολουθούν .

2.6.1 Επιλογή αρχιτεκτονικού μοντέλου (Grid model adoption)

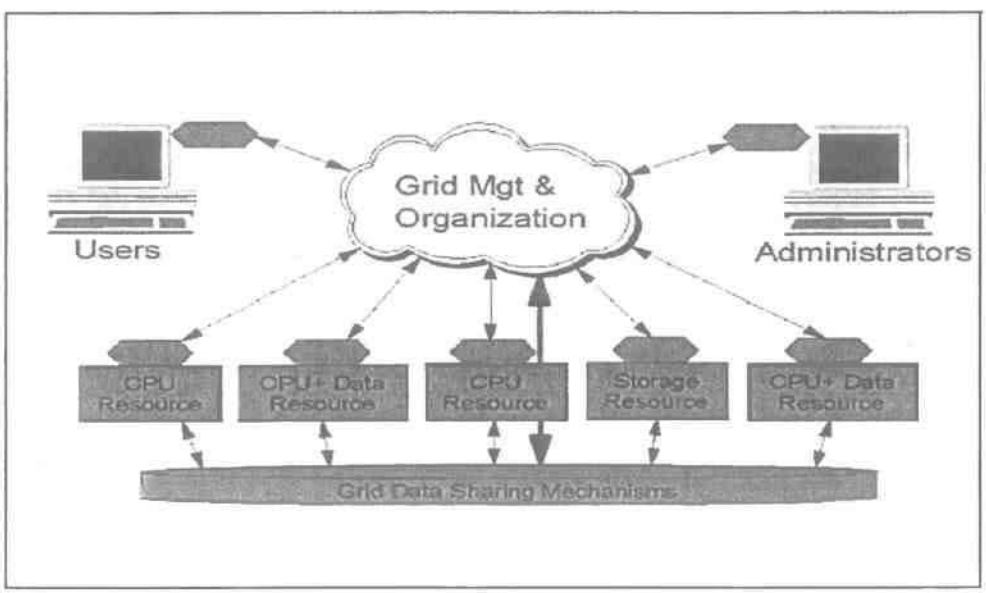
Σύμφωνα με το [16] , τα επιχειρησιακά ζητήματα, που σχετίζονται με την υιοθέτηση ενός Grid μοντέλου, περιλαμβάνουν ορισμένους παράγοντες αποφασιστικής σημασίας όπως:

1. Κατοχή και εκμετάλλευση ήδη υπαρχόντων πόρων και επενδύσεων
2. Μείωση λειτουργικών εξόδων
3. Δημιουργία ευέλικτης και επεκτάσιμης υποδομής
4. Επιτάχυνση χρόνου ανάπτυξης έργων
5. Αύξηση της παραγωγικότητας της εταιρείας
6. και φυσικά η αυξανόμενη ικανοποίηση του πελάτη

Ένας οργανισμός, είναι πιθανό να συνεργάζεται με άλλους οργανισμούς μέσα στην εταιρεία ή με εξωτερικούς οργανισμούς- εταιρείες. Συνεπώς , το πλέγμα μπορεί να ενώνει τόσο εσωτερικούς όσο και εξωτερικούς συνεργάτες. Η πολυπλοκότητα των απαιτήσεων μιας επιχείρησης, εξαρτάται από μηχανισμούς εικονικοποίησης, από τον αντίκτυπο της επιχείρησης, από σχέσεις εμπιστοσύνης, θέματα ασφάλειας, παγκοσμιοποίησης κτλ.

Με βάση το **επίπεδο πολυπλοκότητας**, τα μοντέλα αρχιτεκτονικής πλέγματος κατηγοριοποιούνται σύμφωνα με το [16] ως εξής :

- **Infra-Grid:** Αυτό το μοντέλο αρχιτεκτονικής επιτρέπει τη βελτιστοποίηση του διαμοιρασμού των πόρων μέσα σε ένα τμήμα μιας επιχείρησης. Πρόκειται για ένα πολύ καλά ελεγχόμενο περιβάλλον με καλά ορισμένες επιχειρησιακές πολιτικές καθώς και απαιτήσεις ασφάλειας. Επειδή τα ζητήματα διαχείρισης σχετίζονται μόνο με ένα **domain** (καθώς υπάρχει μια επιχείρηση), ο κύριος στόχος μπορεί να είναι το κέρδος σε τεχνική εμπειρία. Και αυτό γιατί οι συναλλαγές που λαμβάνουν χώρα είναι, μέσα στο ίδιο τμήμα της επιχείρησης. Αυτού του είδους τα πλέγματα ονομάζονται και πλέγματα συστάδων ή αλλιώς "**cluster grids**". Η μορφή του, μοιάζει με αυτήν της εικόνας που ακολουθεί, η οποία ωστόσο ανταποκρίνεται περισσότερο στην επόμενη κατηγορία που ακολουθεί.

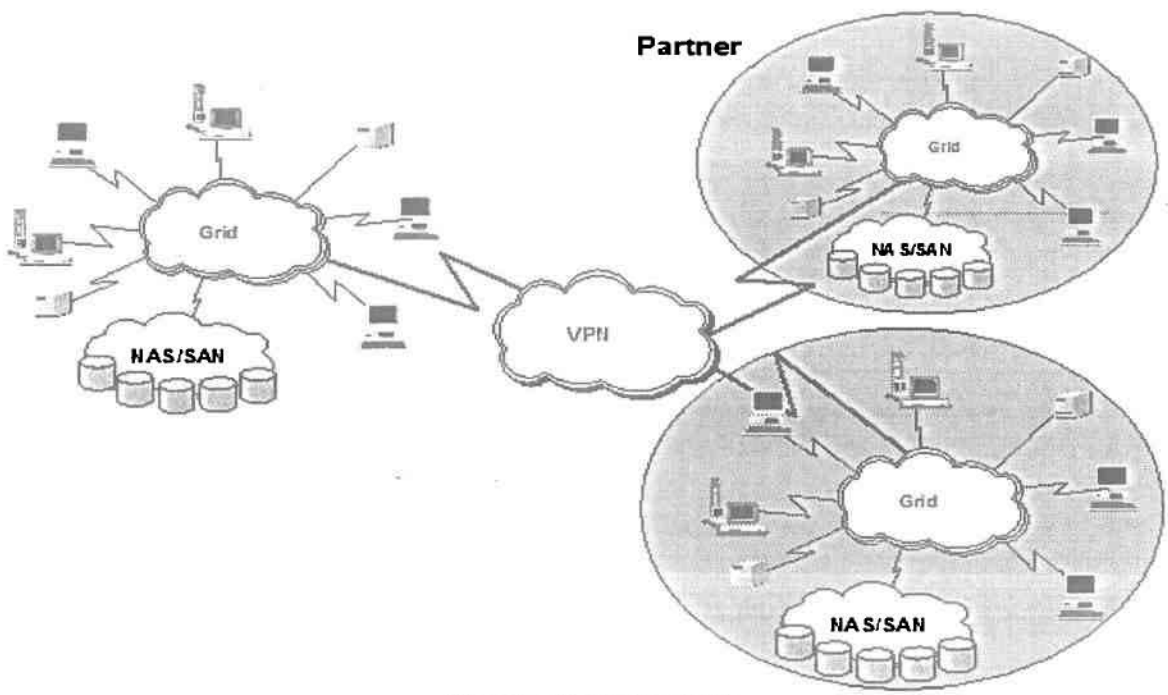


Τοπολογία Intra-Grid

- **Intra-grid:** Πρόκειται για μια πιο σύνθετη υλοποίηση πλέγματος, και καλύπτει τις απαιτήσεις οργανισμών για διαμοίραση πόρων π.χ υπολογιστικών. αποθηκευτικών, βάσεων δεδομένων κτλ. Η ειδοποιός διαφορά με το προηγούμενο μοντέλο είναι ότι η διανομή αυτών των πόρων γίνεται **μεταξύ διαφορετικών τμημάτων της ίδιας εταιρείας** / οργανισμού. Αυτού του είδους τα πλέγματα χρειάζονται καλά ορισμένες πολιτικές για την διαμοίραση των πόρων μέσα στην επιχείρηση.Επιπροσθέτως, λόγω της αυξημένης πολυπλοκότητας των ζητημάτων ασφάλειας, διαμοίρασης δεδομένων-πόρων. μπορεί να αυξηθεί το κέρδος της επιχείρησης και σε επίπεδο τεχνικών εμπειριών

Επειδή όμως οι πόροι βρίσκονται **μέσα σε μία μόνο επιχείρηση**, πρωταρχικός στόχος είναι ο καθορισμός των πολιτικών ασφαλείας και η υλοποίησή τους.
Αυτά τα πλέγματα καλούνται και 'επιχειρησιακά πλέγματα' ή αλλιώς 'πανεπιστημιακά πλέγματα' (**campus grids**).
Όπως παρατηρούμε στην παραπάνω εικόνα, αρκούν λίγοι υπολογιστικοί - αποθηκευτικοί πόροι, οι χρήστες και οι διαχειριστές. Τα υπόλοιπα είναι δουλειά των πρωτοκόλλων και των διάφορων μηχανισμών διαμοίρασης και διαχείρισης πόρων

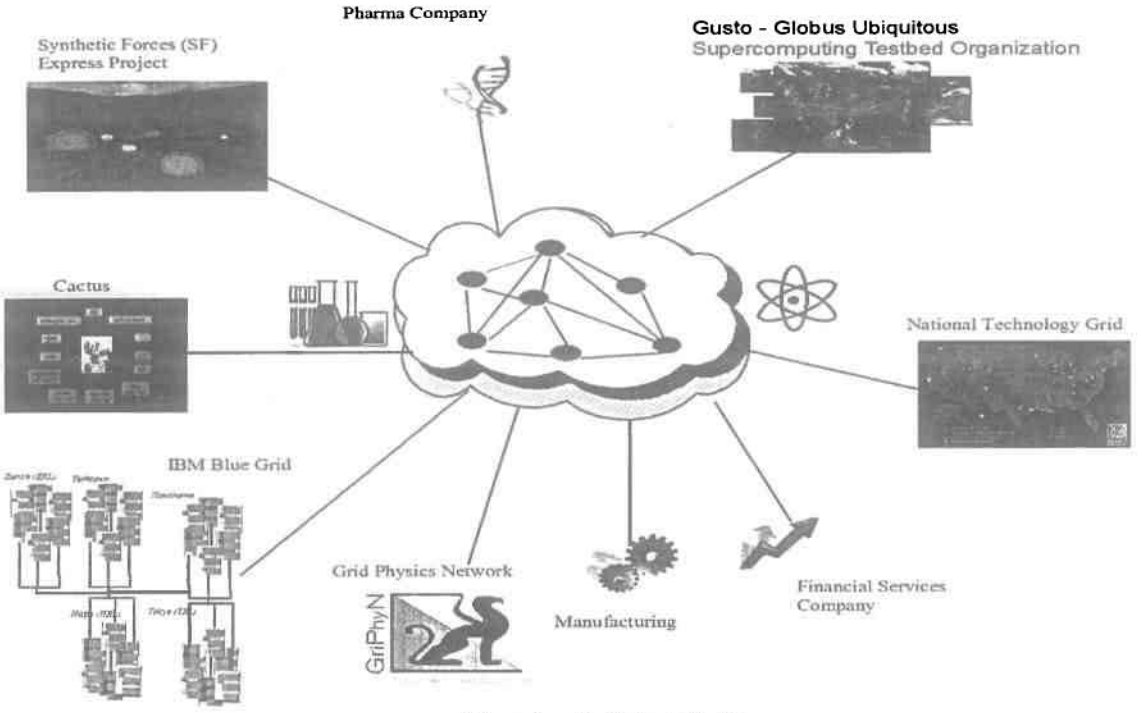
- **Extra-Grid:** Το συγκεκριμένο μοντέλο αρχιτεκτονικής, αντιμετωπίζει τα θέματα της διαμοίρασης δεδομένων, **ανάμεσα σε τμήματα όχι μόνο μιας** επιχείρησης, αλλά και των τμημάτων αυτής **με εξωτερικούς** έμπιστους συνεργάτες, με τους οποίους η εν λόγω εταιρεία έχει αναπτύξει μια επιχειρησιακή σχέση. Αυτά τα πλέγματα είναι γνωστά και σαν 'συνεταιρικά πλέγματα' (**partner grids**). Επειδή αυτού του είδους τα πλέγματα , επεκτείνουν προς τα έξω το διαχειρίσιμο τομέα (management domain) μιας επιχείρησης, απαιτούνται αμοιβαίες συνεταιρικές συμφωνίες, καθώς και υπηρεσίες που θα καθορίζουν την χρήση των πόρων. Υλοποιώντας αυτές τις συμφωνίες, οι επιχειρήσεις κερδίζουν σημαντικές εμπειρίες στην διαχείριση και διατήρηση της πρόσβασης ανάλογα βέβαια και με το τι περιλαμβάνουν αυτές. Μια ενδεικτική τοπολογία που υλοποιεί αυτό το αρχιτεκτονικό μοντέλο είναι και η παρακάτω:



Τοπολογία Extra-Grid

Από την εικόνα, παρατηρούμε ότι μια επιχείρηση, δημιουργεί ένα 'τοπικό' πλέγμα, ένα Intra-Grid, προκειμένου να μπορούν τα τμήματά της να μοιράζονται τους πόρους. Επιπροσθέτως το Intra-Grid θα συνδέεται μέσω ασφαλών συνδέσεων π.χ Virtual Private Networks με συνεργάτες της, και κατά προέκταση με τα πλέγματά τους.

- **Inter-Grid:** Πρόκειται για μοντέλα αρχιτεκτονικής πλέγματος που επιτρέπουν την διανομή-'μοίρασμα' των υπολογιστικών, αποθηκευτικών πόρων, κατά **μήκος του Web** σε συνεργασία φυσικά και με άλλες επιχειρήσεις. Πρόκειται στην ουσία για την πιο πολύπλοκη μορφή αρχιτεκτονικής πλέγματος, καθώς σε κάθε τομέα είναι τουλάχιστον ένα επίπεδο πολυπλοκότητας πιο πάνω από τα υπόλοιπα. Τόσο στον τομέα των service-level συμφωνιών , όσο και στην ασφαλή διαχείριση και διανομή πόρων οι απαιτήσεις είναι πραγματικά πολύπλοκες και μεγάλες.
  Και σε αυτό το μοντέλο αρχιτεκτονικής, μια επιχείρηση μπορεί να συνδεθεί στο πλέγμα εταιρικών της συνεργατών κτλ, υποστηρίζοντας έτσι αμφίδρομες επικοινωνίες και αλληλεπιδράσεις.



Τοπολογία Inter-Grid

Όλα τα παραπάνω, τονίζουν ιδιαίτερα την πολυπλοκότητα και τις δυσκολίες του εγχειρήματος που ακούει στο όνομα '*Ενσωμάτωση τεχνολογίας Grid στις επιχειρήσεις*'. Σημαντικό ρόλο για την αποδοχή ενός εκ των παραπάνω μοντέλων αρχιτεκτονικής είναι και η πληροφοριακή υποδομή που απαιτείται από μια επιχείρηση προκειμένου υλοποιήσει ένα πλέγμα.

2.7 SERVICE ORIENTED ARCHITECTURE (SOA)

Η αρχιτεκτονική πλέγματος την οποία μελετήσαμε πιο πάνω, προτείνεται σαν μια λύση σε τέτοια προβλήματα, καθώς είναι σχεδιασμένη για ελεγχόμενη διαμοίραση πόρων με βελτιωμένη διαλειτουργικότητα μεταξύ των συμμετεχόντων στο πλέγμα. Αντίθετα, οι παρακάτω προτυποποιημένες αρχιτεκτονικές , βοηθούν την αρχιτεκτονική που μόλις αναφέραμε , να προσαρμοστεί σε μια περιοχή ευρύτερης (και στρατηγικά σημαντικής) τεχνολογίας.

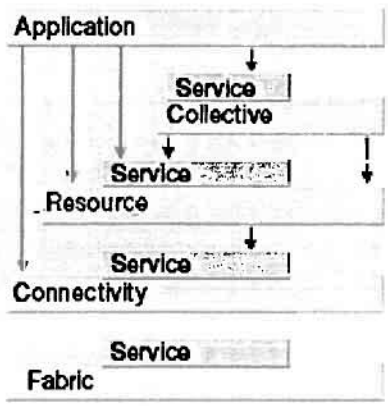
2.7.1 Μοντέλο αρχιτεκτονικής SOA (Service Oriented Architecture)

Μια τέτοια αρχιτεκτονική, βασίζεται σε υπηρεσίες, και αποτελεί ένα συγκεκριμένο πλαίσιο (framework) κατανεμημένων συστημάτων, στο οποίο υπάρχουν agents που δρουν σαν υπηρεσίες λογισμικού , εκτελώντας καλά ορισμένες λειτουργίες. Σύμφωνα με το [16] μπορούμε να καθορίσουμε την αρχιτεκτονική SOA , σαν μια αρχιτεκτονική αρκετά αφαιρετική ως προς κάποια συστατικά του πλέγματος , αρκετά δυσνόητη για τους πελάτες, αλλά με εύκολη πρόσβαση πέρα από το δίκτυο μέσω καλά ορισμένων πολιτικών όπως υπαγορεύονται από τα ίδια τα συστατικά του πλέγματος.

Επιπλέον, μια υπηρεσία ενεργεί κατά κάποιο τρόπο σαν τμήμα λογισμικού ,που έρχεται 'αντιμέτωπη' συχνά με τον ίδιο το χρήστη και σχετίζεται με εφαρμογή ή ακόμα και πόρο του πλέγματος. Αυτού του είδους η λειτουργικότητα, επιτρέπει στους χρήστες της εφαρμογής ή των πόρων, να ασχολούνται μόνο με τη λειτουργική περιγραφή της υπηρεσίας. [16]

Επίσης, η αρχιτεκτονική SOA **τονίζει ότι όλες οι υπηρεσίες έχουν δικτυακά προσβάσιμη διεπαφή (interface) , και επικοινωνούν μέσω πρότυπων πρωτοκόλλων και συγκεκριμένων μορφών δεδομένων-μηνυμάτων.** Με τον όρο δικτυακά προσβάσιμη διεπαφή, εννοούμε ότι μέσω κατάλληλων μηχανισμών λογισμικού, ο χρήστης χρησιμοποιώντας το δίκτυο θα μπορεί να έχει απομακρυσμένη πρόσβαση σε υπηρεσίες πλέγματος.

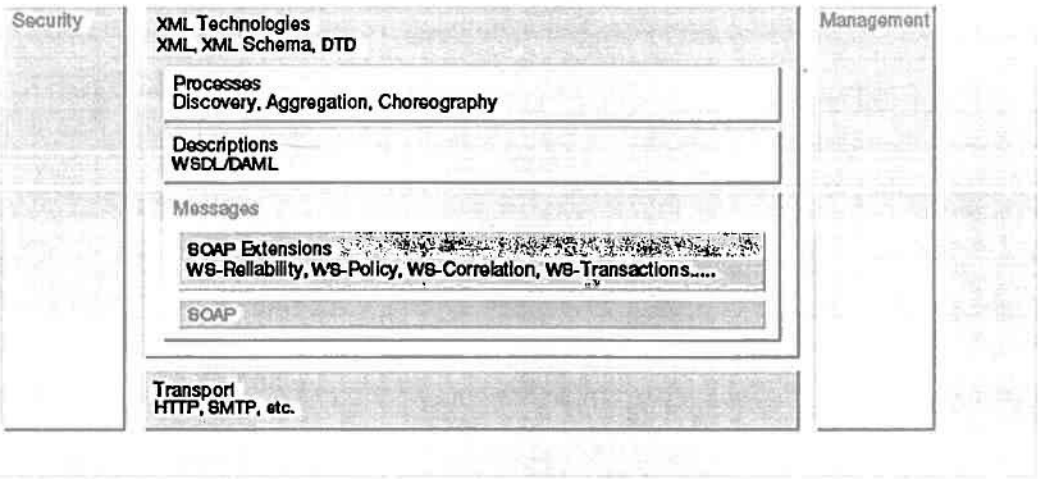
Μια ενδεικτική αρχιτεκτονική SOA σύμφωνα με Pearson technology Group, είναι η ακόλουθη:



Service oriented Αρχιτεκτονική Grid

2.8 WEB SERVICES ΑΡΧΙΤΕΚΤΟΝΙΚΗ (WSA)

Η ανάπτυξη και η προτυποποίηση των Web υπηρεσιών, ήρθε να συμβάλλει στην ανάπτυξη μιας νέας αρχιτεκτονικής την Web Services Architecture ή πιο σύντομα WSA. Αυτή η αρχιτεκτονική εμπλουτίζει την SOA καθώς επιτρέπει στις διάφορες υπηρεσίες να αλληλεπιδρούν ανταλλάσσοντας XML μηνύματα, κάτι που φαίνεται και στην ακόλουθη εικόνα [16] .



Αρχιτεκτονική Web Services(WSA) σύμφωνα και με την Pearson Technology Group.

Σύμφωνα με το [16] τα σημαντικότερα χαρακτηριστικά της WSA είναι τα εξής :

- Βασίζεται σε τεχνολογίες XML, XML σχήματα
- Είναι ανεξάρτητη των πρωτοκόλλων μεταφοράς του υποστρώματος, όπως είναι π.χ το HTTP,SMTP
- Χρησιμοποιεί XML για την ανταλλαγή μηνυμάτων ανάμεσα σε υπηρεσίες, ενώ παράλληλα παρέχει επεκτασιμότητα πάνω στο μοντέλο ανταλλαγής μηνυμάτων προκειμένου να υπάρξει καλύτερη προσαρμογή στις όποιες απαιτήσεις σε ασφάλεια, αξιοπιστία, και εμπιστευτικότητα. Αυτά τα διαλειτουργικά μηνύματα μπορούν να δημιουργηθούν μέσω του πρωτοκόλλου SOAP και των επεκτάσεών του.
- Χρησιμοποιεί μηχανισμούς ανακάλυψης υπηρεσιών , ελέγχου ροής εργασίας, και διαχείρισης κατάστασης των συναλλαγών που βασίζονται στις ιδιότητες της XML.

Η ανάδειξη της αρχιτεκτονικής SOA, βοηθά τους πόρους του πλέγματος να 'διαφημίσουν' τις δυνατότητές τους μέσω πρότυπων διεπαφών. Επίσης, οι λειτουργίες του κάθε επιπέδου της αρχικής αρχιτεκτονικής Grid, μπορούν να απλοποιηθούν, καθιστώντας έτσι ευκολότερη την συνένωση πόρων –χρηστών σε ένα ενιαίο πλέγμα.

2.9 ΒΑΣΙΚΑ ΘΕΜΑΤΑ ΤΗΣ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ OGSA

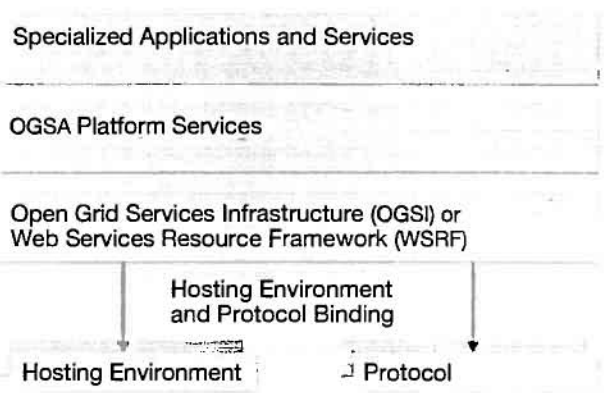
Είναι γεγονός ότι στον χώρο του e-business, είναι συχνά αναγκαία η **ενσωμάτωση υπηρεσιών** μεταξύ κατανεμημένων , ετερογενών , δυναμικών 'εικονικών' οργανισμών. Τον τελευταίο καιρό , έχουν αναπτυχθεί πολλές εφαρμογές middleware χωρίς να έχουν καταφέρει να λύσουν τα προβλήματα του πλέγματος, και αυτό γιατί οι λύσεις αυτές δεν ήταν διαλειτουργικές (interoperable) .Έτσι παρέμεναν και τα προβλήματα μεταξύ των χρηστών του πλέγματος που χρησιμοποιούσαν διαφορετικές πλατφόρμες [16].
Η ενσωμάτωση αυτή , είναι σύμφωνα με το [9] , μια τεχνολογική πρόκληση, εξαιτίας της ανάγκης για επίτευξης, ποιότητας υπηρεσιών (QoS), ανάμεσα στις διάφορες πλατφόρμες λογισμικού. Στα πλαίσια αυτών των αναγκών, παρουσιάζεται μια νέα αρχιτεκτονική η OGSA (Open Grid Service Architecture) , η οποία επιλαμβάνεται αυτών των προκλήσεων.

Βασιζόμενη σε έννοιες και τεχνολογίες από τον χώρο του πλέγματος (Grid) και των διαδικτυακών υπηρεσιών (Web Services), η OGSA καθορίζει κάποιους συγκεκριμένους μηχανισμούς για την δημιουργία, την ονομασία, και την ανακάλυψη προσωρινών υπηρεσιών πλέγματος (**Grid Service Instances**). Μπορούμε να πούμε ότι αυτή η αρχιτεκτονική συνδυάζει τα καλύτερα χαρακτηριστικά τόσο της υπολογιστικής πλέγματος όσο και των τεχνολογιών των Web Services.

2.9.1 Ορισμός Αρχιτεκτονικής OGSA

Με βάση το [16] η αρχιτεκτονική OGSA είναι μια αρχιτεκτονική χωρισμένη σε επίπεδα όπως φαίνεται και στην παρακάτω εικόνα.

Figure 4 OGSA platform architecture



Αρχιτεκτονική OGSA

Μπορούμε να παρατηρήσουμε ότι τα βασικά αρχιτεκτονικά επίπεδα είναι το OGSI (Open Grid Service Infrastructure) και το OGSA platform services, που περιλαμβάνει διαχείριση πολιτικής, πρόσβασης και διαχείριση υπηρεσιών .

Ένας άλλος, ορισμός, είναι ο παρακάτω [9]:

«Η OGSA είναι μια αρχιτεκτονική, που συνδυάζει τεχνολογίες Grid με Web Services προκειμένου να εκμεταλλευθεί χρήσιμες ιδιότητες των τελευταίων.»

Στη συγκεκριμένη αρχιτεκτονική, το ενδιαφέρον εστιάζεται στις υπηρεσίες καθώς όλοι οι πόροι (υπολογιστικοί, αποθηκευτικοί, δικτυακοί, βάσεις δεδομένων κτλ) αναπαρίστανται σαν υπηρεσίες.
Με τον προαναφερθέντα όρο 'χρήσιμες ιδιότητες' εννοούμε:

- Περιγραφή και ανακάλυψη υπηρεσιών
- Αυτόματη παραγωγή κώδικα στην πλευρά του πελάτη και του εξυπηρετητή , με τη βοήθεια υπηρεσιών περιγραφής
- Συμβατότητα ανάμεσα σε διάφορα standards.

Μελετώντας τα ακρωνύμια, ο όρος **architecture** αναφέρεται σε ένα καλά καθορισμένο σύνολο βασικών διεπαφών, ενώ ο όρος **open** χρησιμοποιείται για να δηλώσει την δυνατότητα επεκτάσιμης επικοινωνίας, και την ανεξαρτησία πλατφόρμας καθώς δεν υπάρχουν δεσμεύσεις για τους χρήστες [9].

2.9.2 Χαρακτηριστικά της αρχιτεκτονικής OGSA

Η αρχιτεκτονική την οποία μελετάμε, χρησιμοποιεί μια γλώσσα περιγραφής Web υπηρεσιών την WSDL, προκειμένου να προσδώσει στις υπηρεσίες κάποιες χρήσιμες δυνατότητες όπως αυτό-περιγραφή, ευκολία ανακάλυψης , συμβατότητα λογισμικών και διαχείρισης.
Ας δούμε όμως πιο αναλυτικά τα χαρακτηριστικά της :

1. **ΤΕΧΝΟΛΟΓΙΚΟ ΥΠΟΒΑΘΡΟ ([9])→**Η OGSA βασίζεται σε δύο τεχνολογίες το Globus Toolkit και την τεχνολογία των Web υπηρεσιών. Το Globus Toolkit, είναι ένα ανοικτό αρχιτεκτονικά σύστημα που περιλαμβάνει υπηρεσίες και βιβλιοθήκες που υποστηρίζουν με τη σειρά τους το πλέγμα και τις εφαρμογές του. Κάποια μέρη αυτού του συστήματος, που σχετίζονται ιδιαίτερα με την OGSA είναι το GRAM, MDS-2,GSI, τα οποία θα μελετήσουμε αναλυτικά παρακάτω. Όσο αφορά την δεύτερη τεχνολογία, των Web services , πρόκειται στην ουσία για τεχνική περιγραφής συστατικών λογισμικού προς πρόσβαση, μέθοδοι για πρόσβαση σε πόρους και ανακάλυψη μεθόδων που σχετίζονται με διάφορους πάροχους υπηρεσιών. Σε αυτήν την κατηγορία μπορούμε να αναφέρουμε κάποια standard που αναπτύχθηκαν όπως το WSDL, SOAP κτλ. Η συγκεκριμένη τεχνολογία παρουσιάζει δύο πλεονεκτήματα. Πρώτο, η WSDL καλύπτει την ανάγκη μας για υποστήριξη δυναμικής ανακάλυψης και σύνθεσης υπηρεσιών σε ετερογενή περιβάλλοντα, καθώς παρέχει μηχανισμούς για εγγραφή υπηρεσιών και πλήρη περιγραφή τους.
   Και το δεύτερο, είναι ότι οι τεχνολογίες Web Services τυγχάνουν ευρείας αποδοχής, επομένως θα μπορούσαν να αποτελέσουν το πλαίσιο εργασίας μέσα στο οποίο θα μπορούν να αναπτυχθούν ποικίλα εργαλεία και υπηρεσίες, π.χ επεξεργαστές WSDL κτλ.

2. **ΕΙΚΟΝΙΚΟΠΟΙΗΣΗ ΥΠΗΡΕΣΙΩΝ (Service Virtualization)→** Στην συγκεκριμένη αρχιτεκτονική, εστιάζουμε στις υπηρεσίες. Γενικά, μια κρίσιμης σημασίας απαίτηση σε κατανεμημένα περιβάλλοντα πλέγματος, είναι η διαλειτουργικότητα. Μια αρχιτεκτονική που βασίζεται σε υπηρεσίες (service oriented) , απλοποιεί την εικονικοποίηση (virtualization) , η οποία με την σειρά της επιτρέπει την πρόσβαση και επικοινωνία μεταξύ ετερογενών συστημάτων . Επίσης επιτρέπει την αντιστοίχηση πολλαπλών 'λογικών' πόρων στον ίδιο φυσικό πόρο , ενώ ταυτόχρονα δίνει την δυνατότητα στον εκάστοτε εικονικό οργανισμό για διαχείριση αυτών των πόρων –υπηρεσιών.

3. **ΥΠΗΡΕΣΙΑ ΠΛΕΓΜΑΤΟΣ (Grid Service)→** Η δυνατότητα να εικονικοποιούμε και να συνθέτουμε υπηρεσίες, δεν βασίζεται μόνο σε ορισμούς standard διεπαφών. Απαιτείται να θεσπιστούν κάποιες πρότυπες έννοιες για τις αλληλεπιδράσεις των υπηρεσιών π.χ σε περιπτώσεις σφαλμάτων. Η αρχιτεκτονική OGSA καθορίζει την **υπηρεσία πλέγματος**. Πρόκειται για Web Service που παρέχει ένα καλά ορισμένο σύνολο διεπαφών που ακολουθεί ορισμένους κανόνες -συμβάσεις. Σε αυτό το σύνολο περιλαμβάνονται διεπαφές για ανακάλυψη διευθύνσεων , για δυναμική δημιουργία υπηρεσιών, διαχείρισης διάρκειας υπηρεσιών (lifetime management) κτλ. Οι διεπαφές και οι συμβάσεις, που αναφέραμε προηγουμένως, σχετίζονται κυρίως με την διαχείριση *προσωρινών μη στατικών υπηρεσιών (transient service instances)*. Π.χ σε ένα σύστημα βιντεο-διάσκεψης, η εγκατάσταση μιας διεργασίας βιντεοδιάσκεψης μπορεί να περιλαμβάνει την δημιουργία πολλών τέτοιων προσωρινών υπηρεσιών που εξυπηρετούν την από άκρου σε άκρο, ροή της πληροφορίας, εξασφαλίζοντας QoS. Να σημειωθεί ακόμη ότι η υπηρεσία πλέγματος παρέχει και δυνατότητες αξιόπιστης μεταφοράς δεδομένων, καθώς και αυθεντικοποίησης.

4. **ΠΡΟΤΥΠΕΣ ΔΙΕΠΑΦΕΣ (Standard Interfaces)→** Στον πίνακα που ακολουθεί[9] δίνονται κάποιες διεπαφές (στην ορολογία WSDL αναφέρονται σαν portTypes) που καθορίζει η υπηρεσία πλέγματος. Αυτές έχουν μια συγκεκριμένη λειτουργία και παρέχουν δυνατότητες →

   - ***Ανακάλυψης (Discovery)***:Οι εφαρμογές πλέγματος απαιτούν μηχανισμούς ανακάλυψης διαθέσιμων υπηρεσιών και καθορισμού των χαρακτηριστικών τους. Πως επιτυγχάνεται αυτό; Με μια αναπαράσταση service data που στην ουσία είναι πληροφορία για την υπηρεσία πλέγματος, μέσω XML elements που ονομάζονται service data elements, με μια λειτουργία FindServiceData για την ανάκληση υπηρεσιών καθώς και με το HandleMap που είναι υπεύθυνο για το registering των υπηρεσιών.

   - ***Δυναμική δημιουργία υπηρεσιών***: Η δυνατότητα για δυναμική δημιουργία και διαχείριση 'αντικειμένων' υπηρεσιών (service instance) έχει μεγάλη σημασία (σύμφωνα με το [9]) , για την αρχιτεκτονική OGSA. Αυτή καθορίζει μια πρότυπη διεπαφή (Factory) που πρέπει να παρέχει κάθε μια υπηρεσία.

PortType	Λειτουργία	Περιγραφή
GridService	FindServiceData	Υποβάλλει ερώτημα για πληροφορίες σχετικά με την υπηρεσία πλέγματος
	SetTerminationTime	Καθορίζει τον χρόνο τερματισμού του στιγμιότυπου Grid Service
	Destroy	Τερματίζει το Grid Service
Notification-Source	SubscribeTo NotificationTopic	Εγγραφή και προειδοποίηση γεγονότων μέσω κατάλληλων μηνυμάτων
Notification-Sink	DeliverNotification	Ασύγχρονη Μεταφορά μηνυμάτων ειδοποίησης
Registry	Register Service	Διαχείριση της διαδικασίας εγγραφής των Grid Service
	Unregister Service	Ακύρωση εγγραφής
Factory	Create Service	Δημιουργία στιγμιότυπου Grid Service
HandleMap	FindbyHandle	Επιστρέφει αναφορά σε Grid Service

Web Services σε περιβάλλον πλέγματος

- ***Διαχείριση διάρκειας ζωής***: Κάθε κατανεμημένο σύστημα πρέπει να είναι ικανό να αντιμετωπίζει τα αναπόφευκτα σφάλματα. Σε ένα σύστημα λοιπόν που υποστηρίζει μη στατικές transient υπηρεσίες, πρέπει να παρέχονται μηχανισμοί διαχείρισης υπηρεσιών που σχετίζονται με εσφαλμένες υπηρεσίες προκειμένου να τερματιστούν . Αυτή η απαίτηση καλύπτεται από δύο λειτουργίες Destroy SetTerminationTime όπως φαίνεται και στον πίνακα.

- ***Ειδοποίηση***: Οι δυναμικές κατανεμημένες υπηρεσίες πρέπει να μπορούν να ειδοποιήσουν η μία την άλλη ασύγχρονα , σχετικά με σημαντικές αλλαγές στην κατάστασή τους. Η αρχιτεκτονική OGSA καθορίζει διεπαφές υπηρεσιών (NotificationSource, NotificationSink) για επεξεργασία τέτοιων ειδοποιήσεων , ώστε να υπάρξει σωστή αλληλεπίδραση ακόμα και σε περιπτώσεις σφαλμάτων.

5. **Περιβάλλον εκτέλεσης (Hosting Environment)→** Πρακτικά, οι υπηρεσίες πλέγματος, αρχικοποιούνται μέσα σε ένα συγκεκριμένο περιβάλλον εκτέλεσης ή αλλιώς hosting environment. Ένα τέτοιο περιβάλλον , δεν καθορίζει μόνο το μοντέλο προγραμματισμού, γλώσσας, εργαλεία ανάπτυξης και αποσφαλμάτωσης αλλά και πως μια υλοποίηση μιας υπηρεσίας πλέγματος, ικανοποιεί τους όποιους σημασιολογικούς περιορισμούς.

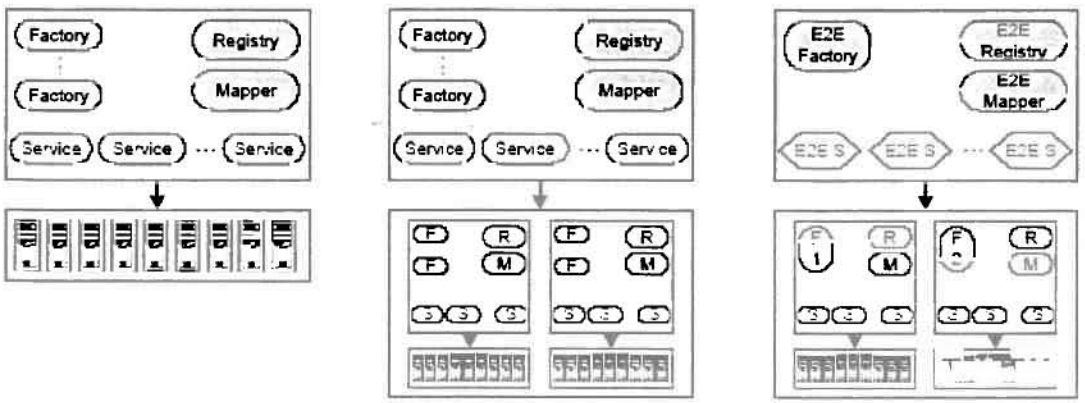
2.9.3 Χρήση μηχανισμών της OGSA για δομές VO

Στην ενότητα αυτή θα μελετήσουμε πως χρησιμοποιούνται πρακτικά όλα τα παραπάνω, προκειμένου να δημιουργηθούν κάποιες δομές υπηρεσιών VO (Virtual Organization).
Εξετάζουμε λοιπόν τις διάφορες περιπτώσεις ανάλογα με την δομή του περιβάλλοντος εκτέλεσης:

- **Single Hosting Environment:** Πρόκειται για σύνολο πόρων που είναι συγκεντρωμένοι μέσα σε ένα συγκεκριμένο domain που υποστηρίζει διαχείριση υπηρεσιών (π.χ J2EE Server, .NET system). Με βάση την αρχιτεκτονική OGSA, η διεπαφή χρήστη σε ένα τέτοιο περιβάλλον θα αποτελείται (δομικά) από registry , μια ή περισσότερες εταιρείες (οντότητες τους) και μια υπηρεσία handleMap. Κάθε εταιρεία είναι εγγεγραμμένη στην registry, ώστε να μπορούν οι πελάτες να ανακαλύψουν τις διαθέσιμες εταιρείες και άρα τις υπηρεσίες τους. Όταν η εταιρεία λαμβάνει ένα αίτημα πελάτη για δημιουργία υπηρεσίας πλέγματος, η εταιρεία, προβαίνει στις ανάλογες ενέργειες υπηρεσιών προκειμένου αν γίνεται να ικανοποιήσει τον πελάτη.

- **Virtual hosting environment:** Σε πιο περίπλοκα περιβάλλοντα, οι πόροι που σχετίζονται με ένα VO μπορούν να καλύπτουν ετερογενή, και γεωγραφικώς διασπαρμένα περιβάλλοντα εκτέλεσης. Ένα παράδειγμα, τέτοιας δομής μπορεί να φανεί παρακάτω στον πίνακα που δείχνει την δομή και των τριών περιβαλλόντων εκτέλεσης.

- **Collective operations:** Μπορούμε να κατασκευάσουμε ένα πιο πολύπλοκο περιβάλλον παρέχοντας 'συλλογικές' υπηρεσίες. Σε αυτή την περίπτωση η registry κρατά αντίγραφα από τις εταιρείες που παρέχουν υψηλού επιπέδου υπηρεσίες.



Τρεις διαφορετικές VO δομές. Από αριστερά στα δεξιά:simple hosting, virtual hosting και collective services [9]

Τα παραπάνω παραδείγματα , διευκρινίζουν πως οι μηχανισμοί υπηρεσιών πλέγματος μπορούν να ενώσουν τους κατανεμημένους πόρους μεταξύ διαφόρων οργανισμών. Σημαντική ρόλο παίζουν όπως είδαμε. οι υπηρεσίες πλέγματος , με τις κατάλληλες δυνατότητες εξεύρεσης, παρέχοντας κατάλληλη διαχείριση και κατά προέκταση QoS.

Μελετήσαμε λοιπόν την αρχιτεκτονική Open Grid Services Architecture (OGSA) που υποστηρίζει , μέσω κατάλληλων διεπαφών , την δημιουργία, τον τερματισμό, την διαχείριση προσωρινών μη στατικών υπηρεσιών . Το βασικό χαρακτηριστικό σε αυτήν την αρχιτεκτονική είναι ***ότι τα πάντα, αναπαρίστανται σαν υπηρεσίες πλέγματος.*** Ουσιαστικά, έχοντας ένα *service oriented model* όπου όλα τα συστατικά του περιβάλλοντος εικονικοποιούνται ,αυτό από μόνο του διευκολύνει την διαχείριση των υπηρεσιών και την πρόσβαση σε διάφορους πόρους του πλέγματος.

2.10 ΠΡΟΤΥΠΟΠΟΙΗΣΗ ΥΠΗΡΕΣΙΩΝ ΠΛΕΓΜΑΤΟΣ (Grid Services standardization)

Στην συγκεκριμένη ενότητα θα εξετάσουμε ένα ακόμη σημαντικό θέμα αυτό της προτυποποίησης των Grid υπηρεσιών. Σύμφωνα με το [16] μια υπηρεσία Grid είναι πρακτικά μια Web υπηρεσία που προσαρμόζεται σε ένα συγκεκριμένο σύνολο πρακτικών κωδικοποίησης δηλαδή ένα σύνολο XML κανόνων σε μορφή προτύπων. Π.χ οι υπηρεσίες πλέγματος μπορούν να καθοριστούν με όρους της γλώσσας WSDL που με την σειρά της περιγράφει υπηρεσίες ,και ως γνωστό βασίζεται στην XML.

Αυτές οι υπηρεσίες πλέγματος, μπορούν να επωφεληθούν από τις Web υπηρεσίες, χρησιμοποιώντας κάποιες τεχνολογίες όπως SOAP, WSReliableMessaging ,WS transaction,κτλ.
Από την οπτική γωνία του προγραμματιστή, οι Grid υπηρεσίες μοιάζουν πολύ με τις Web υπηρεσίες. Όπως αναφέρθηκε πιο πάνω, **όλοι οι πόροι στην OGSA μοντελοποιούνται σαν υπηρεσίες.** Αυτές οι υπηρεσίες κτίζονται πάνω στην κορυφή της αρχιτεκτονικής SOA και πιο συγκεκριμένα στην WSA. Αυτό επιτρέπει στην υπηρεσία πλέγματος να χρησιμοποιήσει τις δυνατότητες του μοντέλου μηνυμάτων (XML) , των περιγραφών των υπηρεσιών και φυσικά την λειτουργία εξεύρεσής τους μέσα στο πλέγμα.
Πρωταγωνιστικό ρόλο παίζουν και τα πρότυπα Web υπηρεσιών που έχουν αναπτυχθεί γιατί επιτρέπουν σε υπηρεσίες Grid να κάνουν πιο ασφαλείς και αξιόπιστες της συναλλαγές τους.

2.10.1 Εξέλιξη προτύπων Web υπηρεσιών

Τα πρότυπα είναι πολύ σημαντικά για την διαλειτουργικότητα ενός κατανεμημένου υπολογιστικού συστήματος , και ιδιαίτερα σε προχωρημένα συστήματα που παρέχουν υπηρεσίες και αυτό γιατί επιτρέπουν σε υπηρεσίες συστημάτων να απλοποιήσουν την διαδικασία ενοποίησης του επιπέδου middleware και της υπάρχουσας υποδομής. Ακόμα, επιτρέπουν να μειωθεί η πολυπλοκότητα της συναλλαγής μεταξύ ετερογενών συστημάτων.
Βασιζόμενοι στο [16] μπορούμε να πούμε ότι μερικά σημαντικά χαρακτηριστικά των προτύπων Web υπηρεσιών είναι τα ακόλουθα:

- **Το μοντέλο δεδομένων XML**: Όπως καθορίζει ο οργανισμός προτύπων W3C αυτό το μοντέλο δεδομένων, καθορίζει όλες τις προδιαγραφές XML συμπεριλαμβανομένου του SOAP και του WSDL.

- **Διαμορφωσιμότητα (modularity):** Το πρωτόκολλο SOAP παρέχει ένα μηχανισμό επεξεργασίας XML μηνυμάτων που πρόκειται να ανταλλαχθούν . Επίσης παρέχει ένα είδος δεδομένων για την μεταφορά αυτών των μηνυμάτων , όπως καθορίζουν οι εκάστοτε SOAP προδιαγραφές.

- **Αποκεντροποίηση (Decentralization):** Μία περιοριστική συμφωνία είναι μια ρυθμιστική συμφωνία ανάμεσα σε ένα Web service-πελάτη και τον πάροχο αυτών των υπηρεσιών πάνω στην μορφή των δεδομένων που θα ανταλλαχθούν. Και οι δύο πλευρές συμφωνούν πάνω στη σύνταξη και στη σημασιολογία των μηνυμάτων , παρ'όλες τις διαφωνίες τους σε θέματα επιλογής και χρήσης λογισμικού, βάσεων δεδομένων, λειτουργικού συστήματος κτλ. Αυτό από μόνο του είναι κέρδος, καθώς κανείς από τους συμμετέχοντες, δεν εξαναγκάζεται να ακολουθήσει κάποιο πρότυπο , πλατφόρμα ή λογισμικό. Συνεπώς έχουν την δυνατότητα να κινηθούν όπως οι ίδιοι θέλουν σε τομείς επεξεργασίας μηνυμάτων, ασφάλειας, διαχείρισης πολιτικών χρήσης κτλ.

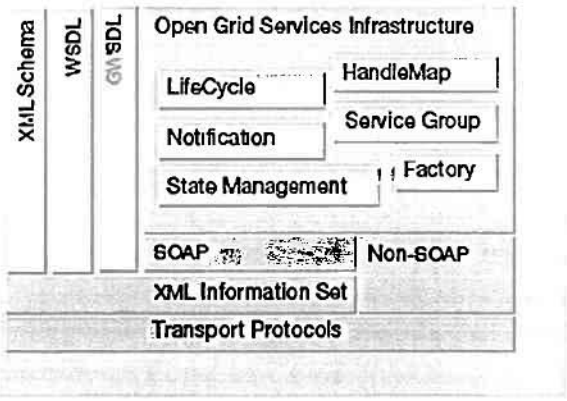
- **Ουδετερότητα εφαρμογών και μετάδοσης (Application and transport neutrality):** Πρόκειται για μια δεσμευτικού χαρακτήρα, απόφαση μεταξύ της υπηρεσία και του αιτούντος για αυτήν. Αυτή η συμφωνία είναι ανεξάρτητη του μηνύματος που πρόκειται να μετακινηθεί. Η ουδετερότητα εφαρμογών προέρχεται από το γεγονός ότι οι δύο πλευρές δεν καθορίζουν κάποιο συγκεκριμένο πρωτόκολλο ανταλλαγής μηνυμάτων αλλά αντιθέτως καθορίζουν προτυποποιημένα XML μηνύματα που πρέπει να ανταλλαχθούν.

- **Ανοικτά πρότυπα (Open standards):** Οι περισσότερες από τις προδιαγραφές πρότυπων πρωτοκόλλων που αναφέρονται στη μελέτη μας υπάγονται σε διάφορες αρχές προτυποποίησης όπως π.χ OASIS,W3C.

Υπάρχουν λοιπόν 2 βασικά πρότυπα που είναι διαθέσιμα για την προτυποποίηση του πλέγματος. Αυτά είναι το OGSI, το οποίο και θα μελετήσουμε , και το WSRF.

2.11 ΤΟ ΠΡΟΤΥΠΟ OGSI

Το βασικό συστατικό της αρχιτεκτονικής OGSA είναι το OGSI (Open Grid Service Infrastructure). Πρόκειται για πρότυπο υποδομής λογισμικού πλέγματος βασιζόμενο στα νέο-αναπτυχθέντα πρότυπα Web υπηρεσιών. Ο στόχος του OGSI είναι να παρέχει την μέγιστη διαλειτουργικότητα μεταξύ των OGSA συστατικών λογισμικού.
Σύμφωνα με το [16], ένα αντικείμενο grid υπηρεσίας, είναι μια web υπηρεσία, που συμμορφώνεται σε ένα σύνολο κανόνων που με τη σειρά τους εκφράζονται μέσω WSDL.
Η παρακάτω εικόνα, δείχνει την δομή σε επίπεδα των συστατικών OGSI σε μια Web υπηρεσία.



Αρχιτεκτονική OGSI

Το πιο αξιοπρόσεκτο σημείο είναι η επέκταση του WSDL προκειμένου να παρέχει επιπρόσθετους μηχανισμούς περιγραφής κατάστασης των υπηρεσιών. Ένα βασικό χαρακτηριστικό αυτού του προτύπου είναι η διαλειτουργικότητα σε επίπεδο μηνυμάτων, και αυτό επιτυγχάνεται με τη χρήση της XML .

Η XML αποτελεί στην ουσία τον σκελετό της μορφής του μηνύματος. Μία από τις απαιτήσεις των υπηρεσιών, που καθορίζεται από το OGSI είναι η δυνατότητα περιγραφής εννοιών που σχετίζονται με την κατάσταση των δεδομένων, και με τον κύκλο ζωής των ιδιοτήτων των υπηρεσιών. Για αυτό το λόγο αναπτύχθηκε και μια γλώσσα, όπως φαίνεται και από την εικόνα, η GWSDL , η οποία είναι ένας συνδυασμός της WSDL και των μηχανισμών του OGSI.
Το άλλο πρότυπο είναι το WSRF το οποίο στην ουσία είναι μια συλλογή προδιαγραφών για την υποστήριξη υπηρεσιών Grid ή άλλων στατικών πόρων και είναι συγκρίσιμο με το OGSI.

2.12 ΣΥΜΠΕΡΑΣΜΑΤΑ

Αναμφισβήτητα, η πληθώρα των χαρακτηριστικών των υπολογιστικών πλεγμάτων τα καθιστούν ενδιαφέροντα για μελέτη. Στο κεφάλαιο αυτό καταγράψαμε τον ορισμό αλλά και τα θεμελιώδη συστατικά του πλέγματος προκειμένου ο χρήστης να κατανοήσει καλύτερα περί τίνος πρόκειται.
Επίσης καταγράψαμε τις εφαρμογές των υπολογιστικών πλεγμάτων με συγκεκριμένα γνωστά παραδείγματα.
Τέλος περιγράψαμε τα αρχιτεκτονικά μοντέλα καταγράφοντας τα χαρακτηριστικά τους, δίνοντας όμως ιδιαίτερη βαρύτητα στην αρχιτεκτονική πλέγματος OGSA.

Η αρχιτεκτονική του πλέγματος παίζει σημαντικό ρόλο στην ενσωμάτωση της τεχνολογίας Grid στον εμπορικό κόσμο. Παρ'όλες τις δυσκολίες που υπάρχουν, βλέπουμε γύρω μας να έχει ενσωματωθεί σε πολλές εταιρείες η τεχνολογία Grid Computing (π.χ οικονομία, εκπαίδευση, επιστήμες, τηλεπικοινωνίες) και μάλιστα με πολύ θετικά αποτελέσματα Η εκάστοτε επιχείρηση , αυτό που καλείται να κάνει είναι να μελετήσει προσεκτικά κάθε μοντέλο αρχιτεκτονική πλέγματος, να εξετάσει ποιο είναι το καταλληλότερο, και έπειτα με τις κατάλληλες επενδύσεις, να επωφεληθεί από αυτήν την τεχνολογία.

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ ΠΛΕΓΜΑΤΟΣ (Grid Security)

Περίληψη

Στο κεφάλαιο μελετούμε την ασφάλεια πλέγματος. Καταγράφουμε τις προκλήσεις της ασφάλειας στα συστήματα Grid, καθώς και τις γενικότερες απαιτήσεις.
Επίσης μελετούμε την μορφή που μπορεί να έχει μια πολιτική ασφάλειας πλέγματος, καθώς και την αρχιτεκτονική ασφάλειας, και τις αντίστοιχες υπηρεσίες.
Εκτός των παραπάνω, επικεντρώνουμε την προσοχή μας στην αρχιτεκτονική OGSA και τα ιδιαίτερα χαρακτηριστικά της, ενώ κλείνουμε το κεφάλαιο με την μελέτη των εικονικών οργανισμών , τα θέματα της ασφάλειάς τους και τα θέματα που αφορούν την πολιτική ασφάλειάς τους.

3.1 ΕΙΣΑΓΩΓΗ

Η υπολογιστική πλέγματος σχετίζεται με την διαμοίραση και την συντονισμένη χρήση ποικίλων πόρων σε κατανεμημένους «εικονικούς οργανισμούς ». Η δυναμική φύση αυτών των περιβαλλόντων , εισάγει κάποιες προκλήσεις στο τομέα της ασφάλειας, οι οποίες απαιτούν νέες τεχνολογικά προσεγγίσεις.[22].
Σύμφωνα με το [20], τα συστήματα πλέγματος αναπτύχθηκαν αρχικά για την υποστήριξη επιστημονικών υπολογισμών. Σήμερα οι εταιρείες, οι χρήστες και οι ερευνητές, ψάχνουν τρόπους για τη χρήση του πλέγματος σε πολλούς καθημερινούς τομείς. Παρόλο που δεν έχουν γίνει εκτεταμένες μελέτες πάνω στην ασφάλεια τέτοιων συστημάτων, αυτή παραμένει βασική προϋπόθεση για την αποδοτική χρήση των συστημάτων σε διάφορες κοινωνικές εφαρμογές.
Κάποιες ερωτήσεις σχετικά με την ασφάλεια στο πλέγμα τις οποίες πρέπει να καλύψουν οι ερευνητές είναι και οι ακόλουθες [20]:

- **Μέσα στο πλέγμα, τι χρειάζεται προστασία** (υπολογιστές, πόροι, δεδομένα, routers) ;

- **Γλώσσες ελέγχου πρόσβασης πολιτικές πρόσβασης:** Χρειαζόμαστε ειδικές γλώσσες για τον καθορισμό πολιτικών ελέγχου πρόσβασης για τους κόμβους του πλέγματος; Και αν ναι ποια πρέπει να είναι τα χαρακτηριστικά τους;

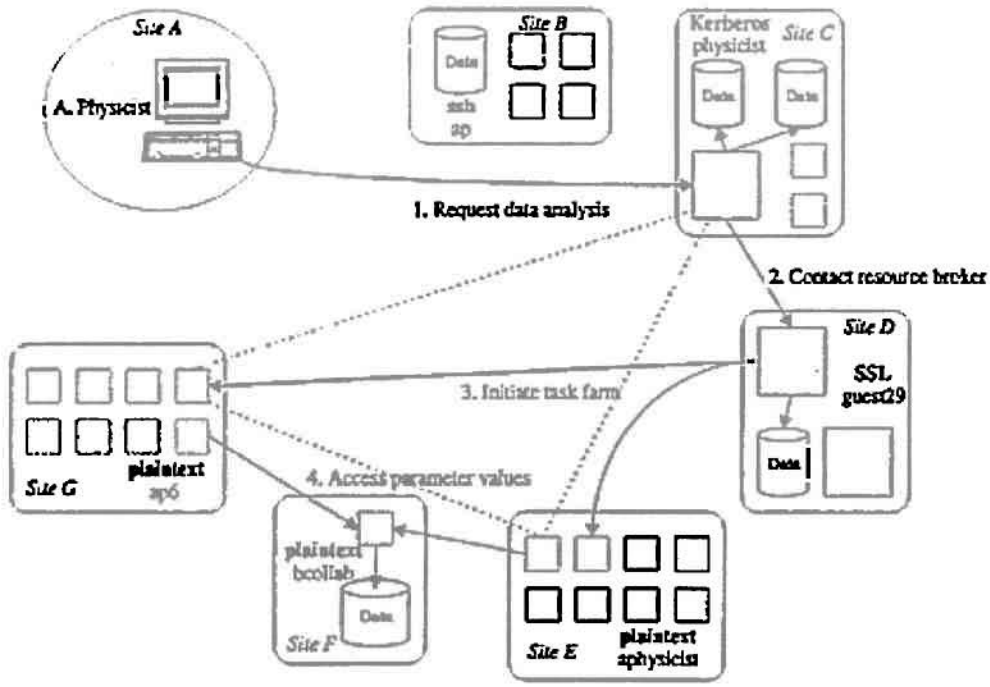
- **Απαιτήσεις χρηστών:**Διαφορετικοί διακομιστές πλέγματος μπορούν να παρέχουν διαφορετικά επίπεδα ασφάλειας. Πως μπορεί ένας χρήστης να καθορίσει τις δικές του απαιτήσεις ασφάλειας κατά τους υπολογισμούς;

- **Κλιμακωσιμότητα και εξέλιξη:** Συστήματα υπολογιστικής πλέγματος, μπορούν να περιλαμβάνουν ένα τεράστιο αριθμό κόμβων . Επίσης η φύση ενός πλέγματος είναι δυναμική εξαιτίας της δυναμικής ένταξης και εγκατάλειψης των πελατών-χρηστών. Πως μπορούμε να σχεδιάσουμε δυναμικά επεκτάσιμα συστήματα πρόσβασης;

Πολύ γενικά μπορούμε να πούμε ότι η ενσωμάτωση ασφάλειας σε συστήματα πλέγματος μπορεί να χωριστεί στους εξής τομείς [23]:

- Διαχείριση οντοτήτων και αυθεντικοποίηση χρηστών
- Ασφαλής επικοινωνία μεταξύ αυθεντικοποιημένων χρηστών
- Πολιτική εξουσιοδότησης και εφαρμογή πολιτικής πρόσβασης στους πόρους
- Ιδιωτικότητα των πληροφοριών του χρήστη
- Έλεγχος και παρακολούθηση της χρήσης των πόρων.

Προκειμένου να γίνει πιο κατανοητή η αναγκαία παρουσία της ασφάλειας στο Grid παραθέτουμε το ακόλουθο παράδειγμα [21]:



Παράδειγμα κατανεμημένων υπολογισμών

Υποθέτουμε ότι ένας επιστήμονας, που ανήκει σε μια ερευνητική ομάδα με επιστήμονες από όλο τον κόσμο, λαμβάνει ένα email από ένα συνάδελφό του που του στέλνει ένα καινούργιο σύνολο δεδομένων. Τότε ξεκινά ένα πρόγραμμα ανάλυσής δεδομένων, αφού πρώτα εκτελέσει απομακρυσμένα τον κώδικά του στο site C. Μόλις ξεκινήσει, καταλαβαίνει ότι πρέπει να γίνει μια προσομοίωση προκειμένου να συγκρίνει τα πειραματικά του αποτελέσματα. Έτσι οι υπόλοιποι υπολογισμοί πρέπει να γίνουν συντονισμένα, στα άλλα sites. Με το συγκεκριμένο παράδειγμα γίνεται κατανοητή η δυναμική φύση του πλέγματος υπολογιστικής καθώς:

- Το πλήθος των χρηστών είναι μεγάλο και δυναμικό. Οι συμμετέχοντες σε τέτοιους εικονικούς οργανισμούς, όπως αυτή η επιστημονική συνεργασία, θα περιλαμβάνει μέλη από πολλά εργαστήρια και θα αλλάζει συχνά. Δυναμικό επίσης είναι και το 'απόθεμα' των πόρων λόγω της απαίτησης των χρηστών για πρόσβαση σε αυτά.
- Οι πόροι μπορούν να απαιτούν διαφορετικού είδους αυθεντικοποίηση και εξουσιοδότηση μέσω κάποιων μηχανισμών και πολιτικών ασφάλειας. Στην εικόνα πιο πάνω φαίνονται τεχνολογίες ασφάλειας και πολιτικών ασφάλειας όπως Kerberos, passwords, SSL,SSH.

Γίνεται κατανοητό πλέον ότι το πρόβλημα που καλούνται να αντιμετωπίσουν οι ερευνητές είναι η παροχή λύσεων ασφάλειας που θα επιτρέπουν τους υπολογισμούς και που θα συντονίζουν ποικίλες πολιτικές ασφάλειας ανάμεσα σε ετερογενή περιβάλλοντα.

Επιπροσθέτως, απαιτούνται μηχανισμοί αυθεντικοποίησης έτσι ώστε οι οντότητες των χρηστών ή των υπηρεσιών να μπορούν να αλληλεπιδρούν με ασφάλεια, ενώ οι πάροχοι υπηρεσιών από την μεριά τους πρέπει να αναπτύξουν μηχανισμούς εξουσιοδότησης προκειμένου να εφαρμόσουν συγκεκριμένες πολιτικές πάνω στις υπηρεσίες και στους πόρους τους.[25]

3.2 ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΠΛΕΓΜΑΤΟΣ

Οι απαιτήσεις ασφάλειας μέσα σ'ένα περιβάλλον πλέγματος σχετίζονται με πρότυπες λειτουργίες ασφάλειας όπως π.χ η αυθεντικοποίηση, ο έλεγχος πρόσβασης, η ακεραιότητα, η ιδιωτικότητα και η μη απάρνηση.

3.2.1 Γενικές απαιτήσεις ασφάλειας πλέγματος

Σύμφωνα με το [21] οι προκλήσεις και οι απαιτήσεις που πρέπει να ικανοποιηθούν στην ασφάλεια πλέγματος είναι οι εξής:

- **Καθολική πιστοποίηση (Single sign-on)**: Ένας χρήστης πρέπει να έχει τη δυνατότητα να αυθεντικοποιείται μια φορά (π.χ στην έναρξη υπολογισμών) και να αρχικοποιεί νέους υπολογισμούς οι οποίοι με τη σειρά τους θα χρησιμοποιούν και θα ελευθερώνουν πόρους επικοινωνώντας εσωτερικά, χωρίς ο χρήστης να χρειάζεται να αυθεντικοποιείται κάθε φορά.

- **Προστασία πιστοποιητικών (Protection of credentials)**: Τα πιστοποιητικά χρηστών (password, ιδιωτικά κλειδιά) πρέπει να προστατεύονται .

- **Διαλειτουργικότητα με τοπικές λύσεις ασφάλειας (Interoperability with local security solutions)**: Καθώς οι λύσεις ασφάλειας παρέχουν μηχανισμούς ανάμεσα σε domains- τμήματα του πλέγματος, η πρόσβαση σε τοπικούς πόρους τυπικά θα καθορίζεται από μια τοπική πολιτική ασφάλειας που θα εφαρμόζεται από έναν τέτοιο μηχανισμό.

- **Εξαγωγιμότητα (Exportability):** Υπάρχει απαίτηση ο κώδικας να είναι εξαγώγιμος και εκτελέσιμος σε απομακρυσμένα μηχανήματα, πόρους κτλ.

- **Υποδομή πιστοποίησης-ομοιόμορφα πιστοποιητικά (certification infrastructure):**Η διατμηματική πρόσβαση απαιτεί τουλάχιστον, ένα κοινό τρόπο έκφρασης της οντότητας σε σχέση με θέματα ασφάλειας. Επίσης είναι επιτακτική ανάγκη να αναπτυχθούν κάποια πρότυπα (π.χ X.509v3) για την κωδικοποίηση πιστοποιητικών .

- **Υποστήριξη για ασφαλή επικοινωνία:** Ένας υπολογισμός μπορεί να συνδυάζει ένα αριθμό διεργασιών που θα απαιτούν συνεργασία των ενεργειών τους σαν ένα ενιαίο σύνολο group.Η σύνθεση ενός τέτοιου συνόλου διεργασιών θα αλλάζει κατά την πάροδο του χρόνου εκτέλεσης του υπολογισμού. Επίσης απαιτείται υποστήριξη για ασφαλή –αυθεντικοποιημένη επικοινωνία για δυναμικά σύνολα. Προς το παρόν καμία λύση ασφάλειας δεν υποστηρίζει τέτοια χαρακτηριστικά.

- **Υποστήριξη για πολλαπλές εφαρμογές :**Η πολιτική ασφάλειας δεν πρέπει να υποδεικνύει μια συγκεκριμένη και μόνο τεχνολογία. Αντιθέτως, θα πρέπει να υπάρχει η δυνατότητα εφαρμογής της με τη χρήση πληθώρας τεχνολογιών ασφάλειας, που θα στηρίζονται σε κρυπτογραφία δημοσίου και ιδιωτικού κλειδιού.

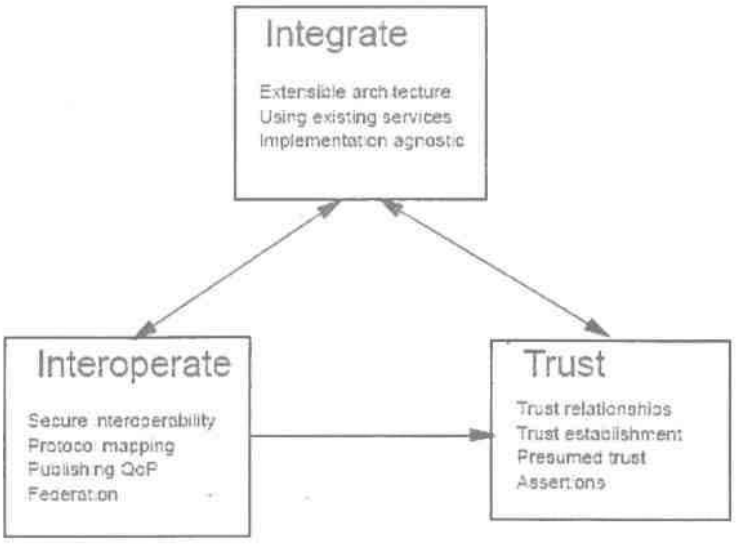
Μια διαφορετική προσέγγιση , για την κατηγοριοποίηση των παραπάνω προκλήσεων ασφάλειας, συναντούμε στο [25] σύμφωνα με το οποίο οι προκλήσεις ασφάλειας που καλείται να αντιμετωπίσει ένα υπολογιστικό πλέγμα χωρίζονται στις παρακάτω κατηγορίες:

- **Προκλήσεις ολοκλήρωσης (Integration)** όπου χρησιμοποιούνται ήδη υπάρχουσες υπηρεσίες και τεχνολογίες προκειμένου να παρέχουν μια επεκτάσιμη αρχιτεκτονική.

- **Προκλήσεις διαλειτουργικότητας (interoperability)** έτσι ώστε υπηρεσίες που παρέχονται σε διαφορετικούς εικονικούς οργανισμούς (και έχουν διαφορετικούς μηχανισμούς ασφάλειας), να μπορούν να επικοινωνούν μεταξύ τους χωρίς προβλήματα.

- **Προκλήσεις για τη διαχείριση και εφαρμογή πολιτικών ασφάλειας μέσα σε δυναμικό περιβάλλον πλέγματος.**

Οι προκλήσεις και των τριών κατηγοριών, αλληλεξαρτώνται όπως δείχνει και η παρακάτω εικόνα:



Κατηγορίες προκλήσεων ασφάλειας σε περιβάλλον πλέγματος

Σε ένα περιβάλλον πλέγματος, όπου οι οντότητες είναι οργανωμένες σε εικονικούς οργανισμούς (VOs) που υπερβαίνουν τα όρια των φυσιολογικών οργανισμών, οι απειλές της ασφάλειας, δεν είναι εύκολα διαχωρίσιμες. Και αυτό γιατί οι οντότητες την μια φορά μπορούν να δρουν ως μέλη ενός VO και την άλλη στιγμή σαν μέλη ενός διαφορετικού VO, ανάλογα με το είδος της εργασίας που πρέπει να επιτελέσουν.
Επίσης, ένα πρόσθετο ρίσκο είναι όταν πολλαπλοί VO μοιράζονται ένα εικονικοποιημένο (virtualized) πόρο (π.χ server, σύστημα αποθήκευσης) όπου ο κάθε συμμετέχων VO μπορεί να μην εμπιστεύεται κάποιον άλλο συμμετέχων στο πλέγμα. μην μπορώντας έτσι να ελέγχει την χρήση και την ακεραιότητα του διαμοιραζόμενου πόρου.

3.2.2 Η πρόκληση ολοκλήρωσης (Integration Challenge)

Είναι παράλογο τόσο για τεχνικούς όσο και για ρεαλιστικούς λόγους, να περιμένουμε από μια μόνο τεχνολογία ασφάλειας να καλύψει όλες τις ανάγκες και απαιτήσεις που έχει η υπολογιστική πλέγματος στον τομέα της ασφάλειας. Οι υπάρχουσες υποδομές ασφάλειας είναι αδύνατο να αντικατασταθούν σε μια νύκτα. Π.χ κάθε τομέας-domain σε ένα περιβάλλον πλέγματος, μπορεί να κατέχει αρχείο τήρησης μητρώων χρηστών – registries) όπου θα αποθηκεύονται τα στοιχεία του χρήστη (LDAP κατάλογοι). Αυτά τα μητρώα είναι απίθανο να διαμοιράζονται μεταξύ πολλών οργανισμών.

Παρόμοιο παράδειγμα είναι και αυτό των μηχανισμών αυθεντικοποίησης και εξουσιοδότησης όπου κάθε domain έχει και τυπικά τη δική του υποδομή εξουσιοδότησης. Έτσι είναι λίγο έως πολύ δύσκολη η αντικατάσταση τέτοιων συστημάτων ασφάλειας , από ένα κοινά αποδεκτό μοντέλο ασφάλειας.

Συνεπώς , για να είναι πετυχημένη μια αρχιτεκτονική ασφάλειας πλέγματος, πρέπει να αντιμετωπίσει την πρόκληση της ενοποίησης και εκμετάλλευσης των ήδη υπαρχόντων αρχιτεκτονικών ασφάλειας των συστημάτων, και να μπορεί να επεκταθεί μέσω νέων τεχνολογιών που θα συνεργαστούν με τις 'παλιές'.

3.2.3 Η πρόκληση διαλειτουργικότητας (Interoperability Challenge)

Οι υπηρεσίες που 'διασχίζουν' πολλά domains πρέπει να μπορούν να αλληλεπιδρούν μεταξύ τους, καθιστώντας την διαλειτουργικότητα βασικό χαρακτηριστικό των μηχανισμών ασφάλειας σε πολλαπλά επίπεδα:

- Στο **επίπεδο πρωτοκόλλου (protocol layer)** , απαιτούνται μηχανισμοί που θα επιτρέπουν την ανταλλαγή μηνυμάτων ανάμεσα σε διαφορετικά domain , και αυτό μπορεί να γίνει μέσω SOAP/HTTP.

- Στο **επίπεδο πολιτικής ασφάλειας (policy level)**, η ασφαλής διαλειτουργικότητα απαιτεί από τον κάθε συμμετέχων , να μπορεί να καθορίζει όποια πολιτική χρειάζεται προκειμένου να εξασφαλιστεί ασφαλής επικοινωνία, και να καθορίζεται με τέτοιο τρόπο ώστε οι πολιτικές ασφάλειας όλων των εμπλεκομένων να μπορούν να γίνονται κατανοητές από όλους. Μόνο τότε οι οντότητες του πλέγματος θα μπορέσουν να επικοινωνήσουν με ασφάλεια, εγκαθιδρύοντας ένα ασφαλές κανάλι που θα βασίζεται στην αμοιβαία αυθεντικοποίηση, στις σχέσεις εμπιστοσύνης και στην πιστή τήρηση της πολιτικής ασφάλειας των άλλων οντοτήτων.

- Στο **επίπεδο ταυτότητας (identity level)** απαιτούνται μηχανισμοί που θα εξακριβώνουν τον χρήστη από το ένα domain στο άλλο. Αυτή η απαίτηση δεν έχει να κάνει μόνο-με την εγκαθίδρυση σχέσεων εμπιστοσύνης και συνεργασίας μηχανισμών ασφαλείας (π.χ Kerberos, X.509), αλλά και με την χρήση πιστοποιητικών πληρεξουσιότητας (proxy certificates) που θα βοηθούν στην αυθεντικοποίηση του χρήστη μεταξύ διαφόρων domains, και θα λειτουργούν σαν τρίτες έμπιστες πηγές.

3.2.4 Η πρόκληση έμπιστων σχέσεων

Οι υπηρεσίες πλέγματος, μπορούν να εκτείνονται πάνω από πολλά domains. Οι έμπιστες λοιπόν σχέσεις μεταξύ αυτών των domains παίζουν πολύ σημαντικό ρόλο .
Μια υπηρεσία πρέπει να γνωστοποιεί τις απαιτήσεις πρόσβασης σε όλους τους ενδιαφερομένους πελάτες, ώστε να γνωρίζουν και αυτοί με τη σειρά τους πώς να έχουν ασφαλή πρόσβαση σε αυτό. Σε ένα περιβάλλον πλέγματος, δεν υπάρχει κάποια προκαθορισμένη-αναμενόμενη εμπιστοσύνη, λόγω της δυναμικής φύσης του πλέγματος αλλά και της κατανομής των εικονικών οργανισμών. Για τον ίδιο λόγο, κάποιες φορές είναι αδύνατη η εγκαθίδρυση σχέσεων εμπιστοσύνης μεταξύ sites πριν από την εκτέλεση της εφαρμογής.
Αν μάλιστα λάβουμε υπόψη ότι οι συμμετέχοντες μπορούν να έχουν διαφορετικές υποδομές ασφάλειας (Kerberos,PKI) τότε γίνεται αντιληπτό ότι *η απαιτούμενη εμπιστοσύνη στις σχέσεις των VO σχετίζεται στενά με την 'συνεργασία' όλων των μηχανισμών ασφαλείας των συμμετεχόντων στο πλέγμα.*

Το πρόβλημα όμως των σχέσεων εμπιστοσύνης γίνεται ακόμα πιο δύσκολο σε ένα περιβάλλον πλέγματος, εξαιτίας της ανάγκης για υποστήριξη δυναμικών 'προσωρινών' (transient) υπηρεσιών που αναπτύσσει ο τελικός χρήστης. Αυτές οι υπηρεσίες πραγματοποιούν συγκεκριμένες εργασίες που σχετίζονται με τα αιτήματα των χρηστών, που μπορεί να περιλαμβάνουν και εκτέλεση κώδικα.

Π.χ σε ένα σενάριο κατανεμημένης εξόρυξης δεδομένων, οι προσωρινές υπηρεσίες μπορούν να δημιουργούνται σε πολλές τοποθεσίες του συστήματος, και να εξάγουν πληροφορίες από απομακρυσμένες βάσεις δεδομένων συνθέτοντας νέα πληροφορία. Οι προκλήσεις ασφάλειας που σχετίζονται με αυτές τις υπηρεσίες είναι σύμφωνα με το [25] οι εξής:

- **Ταυτότητα και εξουσιοδότηση:** Πρέπει να είναι εφικτός ο έλεγχος της εξουσιοδότησης υπό την οποία εκτελούνται οι προσωρινές υπηρεσίες.

- **Εφαρμογή πολιτικής ασφάλειας:** Οι χρήστες μπορούν να δημιουργούν πολιτικές για συγκεκριμένες υπηρεσίες, προκειμένου να ελέγχουν ποιος έχει πρόσβαση σε αυτές και τι ενέργειες μπορεί να κάνει. Σε μια τέτοια περίπτωση όμως, αυτές οι πολιτικές του χρήστη, πρέπει οπωσδήποτε να περιορίζονται από τις πολιτικές του πάροχου των υπηρεσιών , του VO με άλλα λόγια που θα 'φιλοξενεί' την υπηρεσία του χρήστη.

- **Διαπίστωση επιπέδου ασφάλειας (assurance level discovery):** Ο χρήστης λαμβάνει υπόψη του το επίπεδο ασφάλειας που έχει ο πάροχος υπηρεσίας, προκειμένου να αποφασίσει σε ποιον θα εμπιστευτεί την υπηρεσία του. Αυτή λοιπόν η πληροφορία πρέπει να είναι ανακαλύψιμη, καθώς αυτό που νοιάζει τον τελικό χρήστη είναι η παροχή ή όχι εμπιστευτικότητας, προστασίας από ιούς, χρήσης firewall, VPN κτλ. Ένας τρόπος για να γίνει γνωστή αυτή η πληροφορία είναι η χρήση ενός μηχανισμού διαπίστευσης μέσα στον οποίο μια τρίτη διαπιστευμένη 'πλευρά' θα αποδεικνύει πιο πραγματικά είναι το επίπεδο ασφάλειας που παρέχεται από τον υποψήφιο host της υπηρεσίας του χρήστη.

- **Σύνταξη πολιτικής ασφάλειας (Policy composition):** Η πολιτική ασφάλειας σαν υπηρεσία, μπορεί να παραχθεί δυναμικά από πολλές πηγές. Όχι μόνο από τους κατόχους των πόρων αλλά και από την οντότητα της οποίας το αίτημα δημιούργησε την υπηρεσία, και φυσικά από τον εικονικό οργανισμό VO του οποίου μέλος αποτελεί η παραπάνω οντότητα.

- **Ανάθεση για αντιπροσώπευση (delegation):** Οι προσωρινές υπηρεσίες κάποιες φορές χρειάζεται να δρουν εκ μέρους του χρήστη χωρίς την άμεση επέμβαση. Π.χ μια διεργασία υπολογισμού που τρέχει όλη τη νύκτα, μπορεί να χρειαστεί πρόσβαση σε δεδομένα που είναι αποθηκευμένα σε διαφορετικό πόρο. Από τη στιγμή μάλιστα, που δεν υπάρχει άμεση σχέση εμπιστοσύνης μεταξύ του VO της διεργασίας και του VO του πόρου στον οποίο απευθύνεται , η υπηρεσία, είναι ανάγκη να δράσει εκπροσωπώντας τον χρήστη μέσω της ανάθεσης των δικαιωμάτων. Εκτός από αυτό, υπεισέρχονται και άλλα ζητήματα χρήσης και διαχείρισης διαπιστευτηρίων όπως το ' τι συμβαίνει αν τα διαπιστευτήρια που ανατέθηκαν στην υπηρεσία, λήξουν προτού αυτή τελειώσει την εργασία της'.

3.2.5 Βασικές απαιτήσεις ασφάλειας πλέγματος

Στην παρούσα ενότητα, θα μελετήσουμε τις βασικές απαιτήσεις ασφάλειας σε ένα περιβάλλον πλέγματος υπολογιστικής. Ο στόχος των τεχνολογιών Grid είναι η υποστήριξη και η συντονισμένη χρήση ποικίλων πόρων σε δυναμικούς, κατανεμημένους εικονικούς οργανισμούς VOs [10]. Με άλλα λόγια, η δυνατότητα δημιουργίας εικονικών υπολογιστικών συστημάτων από κατανεμημένα συστατικά. Η ασφάλεια, σε ένα σύστημα αρχιτεκτονικής OGSA, είναι ένα από τα σημαντικότερα χαρακτηριστικά του. Οι βασικές απαιτήσεις ενός μοντέλου ασφάλειας OGSA σχετίζονται με την ικανότητα των μηχανισμών ασφάλειας να είναι ανακαλύψιμοι και εύκολα προσαρμόσιμοι (pluggable) ανάλογα και με το αίτημα της υπηρεσίας.
Αυτή η λειτουργικότητα, επιτρέπει στον πάροχο υπηρεσιών να διαλέξει ανάμεσα σε πολλές κατανεμημένες αρχιτεκτονικές ασφάλειας που υποστηρίζονται από διάφορους κατασκευαστές και να προσαρμόσει την κατάλληλη στην υποδομή που ο ίδιος έχει , προκειμένου να παρέχει με ασφάλεια τις υπηρεσίες του.

Σύμφωνα λοιπόν και με το [21] οι βασικές απαιτήσεις ασφάλειας πλέγματος είναι η εξής:

- **Αυθεντικοποίηση:** Πρόκειται για τη παροχή σημείων προσαρμογής (plug points) για πολλαπλούς μηχανισμούς αυθεντικοποίησης καθώς και των μέσων για την διαβίβαση του συγκεκριμένου μηχανισμού ασφάλειας. Ο μηχανισμός μπορεί να είναι ένας τυπικός γνωστός μηχανισμός αυθεντικοποίησης ή κάποια πρότυπη τεχνολογία . Το σημείο προσαρμογής αυθεντικοποίησης πρέπει όμως να είναι ανεξάρτητο από κάποια συγκεκριμένη τεχνολογία αυθεντικοποίησης ώστε να υπάρχει ακόμα καλύτερη διαλειτουργικότητα.

- **Ανάθεση (delegation):** Απαίτηση για παροχή διευκολύνσεων για την ανάθεση δικαιωμάτων πρόσβασης από τους αιτούντες στις υπηρεσίες. Όταν λοιπόν πρόκειται για κάποιο είδος εξουσιοδότησης από μια οντότητα σε μια άλλη, πρέπει με προσοχή να γίνεται η ανάθεση δικαιωμάτων ώστε να πραγματοποιηθεί σωστά η εργασία που πρέπει να γίνει , μέσα σε μικρό χρονικό διάστημα. προκειμένου να ελαττωθεί η πιθανότητα κατάχρησης ή ακόμα και παράνομης χρήσης της αναθετημένης εξουσίας.

- **Καθολική πιστοποίηση (single logon):** Πρόκειται για μια πολύ σημαντική απαίτηση, καθώς με την καθολική πιστοποίηση, απαλλάσσεται μια οντότητα, που έχει αυθεντικοποιηθεί μια φορά επιτυχώς, από το να περνά την ίδια διαδικασία αυθεντικοποίησης (ξανά και ξανά), για ένα εύλογο χρονικό διάστημα. Πρέπει να λαμβάνεται υπόψη ότι μια αίτηση μπορεί να 'εκτείνεται' ανάμεσα σε πολλά domains ασφάλειας και έτσι πρέπει να υπάρχει συνεργασία ανάμεσα στους εκάστοτε μηχανισμούς ασφάλειας. Αυτό από μόνο του είναι πολύ σημαντικό γιατί

  1. Καθιστά αναγκαία την ανάθεση των δικαιωμάτων μιας οντότητας με βάση την πολιτική ασφάλειας
  2. Σε περίπτωση που τα διαπιστευτήρια ανατεθούν σε ενδιαμέσους συμμετέχοντες, μπορεί να έχει μεγάλη σημασία η ένδειξη της ταυτότητας καθενός από αυτούς, με βάση και την πολιτική ασφάλειας.

- **Διάρκεια ζωής και ανανέωση διαπιστευτηρίου (credential's lifetime):** Σε πολλά σενάρια χρήσης του πλέγματος, μια διεργασία που αρχικοποιήθηκε από το χρήστη, μπορεί να διαρκέσει περισσότερο από ότι διαρκεί το πιστοποιητικού του χρήστη. Σε τέτοιες περιπτώσεις ο χρήστης πρέπει είτε να ειδοποιείται πριν τη λήξη των πιστοποιητικών του, είτε να έχει τη δυνατότητα να τα ανανεώνει έτσι ώστε η διεργασία του να ολοκληρωθεί ομαλώς.

- **Εξουσιοδότηση:** Απαίτηση λήψης μέτρων για τον έλεγχο πρόσβασης σε υπηρεσίες OGSA , που θα βασίζεται σε πολιτικές εξουσιοδότησης (π.χ ποιος μπορεί να έχει πρόσβαση στην υπηρεσία, και υπό ποιες συνθήκες) που θα επισυνάπτονται σε κάθε υπηρεσία. Η εξουσιοδότηση , γενικά πρέπει να 'καλύπτει', να προσαρμόζει και να εφαρμόζει πολλά μοντέλα ελέγχου πρόσβασης και όχι μόνο κάποιο συγκεκριμένο.

- **Ιδιωτικότητα (Privacy):** Απαίτηση να επιτρέπεται τόσο στους αιτούντες όσο και στους πάροχους υπηρεσίας, να καθορίζουν και να επιβάλλουν πολιτικές ιδιωτικότητας, λαμβάνοντας υπόψη θέματα που άπτονται προσωπικών δεδομένων. Μάλιστα αυτές οι πολιτικές ιδιωτικότητας, μπορούν να αντιμετωπίζονται σαν μέρος της πολιτικής εξουσιοδότησης.

- **Εμπιστευτικότητα (Confidentiality):** Απαίτηση για προστασία της εμπιστευτικότητας του μηχανισμού επικοινωνίας , και της εμπιστευτικότητας των μηνυμάτων ή των εγγράφων που διακινούνται στην υποδομή OGSA.

- **Ακεραιότητα μηνύματος (Message Integrity):** Απαίτηση για διασφάλιση, ότι μη εξουσιοδοτημένες αλλαγές στα μηνύματα ή στα έγγραφα, θα ανιχνεύονται από τον παραλήπτη. Η χρήση ελέγχου ακεραιότητας των εγγράφων , καθορίζεται από την πολιτική, η οποία συνδέεται στενά με την παρεχόμενη ποιότητα υπηρεσίας (QoS).

- **Ανταλλαγή πολιτικών :** Απαίτηση να επιτρέπεται στους αιτούντες και παρέχοντες την υπηρεσία, να ανταλλάσσουν δυναμικά πολιτικές ασφάλειας προκειμένου να εγκαθιδρύσουν ένα ασφαλές πλαίσιο επικοινωνίας. Αυτές οι πληροφορίες περιλαμβάνουν απαιτήσεις ασφάλειας, υποστηριζόμενη λειτουργικότητα, περιορισμοί και κανόνες ιδιωτικότητας.

- **Ασφαλής πρόσβαση (Secure logging):** Απαίτηση για παροχή όλων των υπηρεσιών, (συμπεριλαμβανομένου και αυτών της ασφάλειας) με ικανότητες ασφαλής πρόσβασης στο δίκτυο του πλέγματος, καθώς αυτή είναι η θεμελίωση των απαιτήσεων για ασφάλεια μη απάρνησης, και έλεγχο χρήσης (auditing).

- **Εγγύηση (assurance):** Παροχή των μέσων για τροποποίηση του επιπέδου ασφάλειας ώστε να 'ταιριάξει' με τις απαιτήσεις του εκάστοτε περιβάλλοντος Αυτό μπορεί να χρησιμοποιηθεί για την περιγραφή των χαρακτηριστικών προστασίας που παρέχονται όπως προστασία από ιούς, χρήση firewall, VPN. Τέτοιου είδους πληροφορία μπορεί να λαμβάνεται υπόψη κατά την επιλογή περιβάλλοντος στο οποίο θα αναπτύξει ο χρήστης την υπηρεσία του.

- **Ευκολία διαχείρισης (manageability):** Πολλή σημαντική η απαίτηση για ευκολία στη διαχείριση των λειτουργιών ασφάλειας στο μοντέλο OGSA, όπως είναι η διαχείριση οντοτήτων, πολιτικών ασφάλειας κτλ. Η ανάγκη για ασφαλή διαχειρίσιμη περιλαμβάνει ακόμα υψηλού επιπέδου απαιτήσεις για προστασία από ιούς, ανίχνευση εισβολέων.

- **Διάσχιση Firewall :** Ένας περιοριστικός παράγοντας στα πολυτμηματικά (multi-institutional) πλέγματα υπολογιστικής είναι η ύπαρξη των firewalls. Είναι απίθανο η τεχνολογία των firewall στο επόμενο διάστημα να εξαφανιστεί. Έτσι το μοντέλο ασφάλειας OGSA πρέπει να λαμβάνει υπόψη την παρουσία των firewall και να παρέχει μηχανισμούς συνεργασίας με τις πολιτικές ασφάλειάς των.

- **Διασφαλίζοντας την υποδομή OGSA:** Η υποδομή OGSI προϋποθέτει την ύπαρξη ενός συνόλου υπηρεσιών υποδομής, όπως handleMap, registry και βιομηχανικές υπηρεσίες. Το μοντέλο ασφάλειας OGSA, πρέπει να αντιμετωπίσει όλα αυτά τα θέματα, διασφαλίζοντας το επίπεδο ασφάλειας των συμμετεχόντων

3.3 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΕΓΜΑΤΟΣ (Grid Security Policy)

Είναι σημαντικό να προσδιορίσουμε ακριβώς τα αντικείμενα της ασφάλειας, και τις συμμετέχουσες οντότητες του πλέγματος. Με λίγα λόγια πρέπει να καθορίσουμε μια πολιτική ασφάλειας, *δηλαδή ένα σύνολο κανόνων που θα καθορίζουν τα αντικείμενα ασφάλειας και τις σχέσεις μεταξύ τους.* [21]

Με βάση αυτή τη προσέγγιση, αναλύονται κάποιοι **βασικοί όροι της πολιτικής ασφάλειας** όπως:

- **Το υποκείμενο (subject)** είναι ένας συμμετέχων σε μια λειτουργία ασφάλειας. Γενικά σε συστήματα πλέγματος, το υποκείμενο είναι είτε χρήστης, είτε μια διαδικασία που δρα εκ μέρους ενός χρήστη, είτε ακόμα και ένας πόρος (υπολογιστής ή αρχείο).

- **Το διαπιστευτήριο (credential)** είναι ένα κομμάτι πληροφορίας που χρησιμοποιείται για να αποδείξει την ταυτότητα ενός υποκειμένου. Παραδείγματα τέτοιων διαπιστευτηρίων είναι οι κωδικοί πρόσβασης (passwords) και τα πιστοποιητικά (certificates).

- **Η αυθεντικοποίηση (authentication)** είναι η διαδικασία μέσω της οποίας ένα υποκείμενο αποδεικνύει τυπικά την ταυτότητά του στον αιτούντα (requestor) μέσω της χρήστης των διαπιστευτηρίων. Μάλιστα υπεισέρχεται και ένας νέος όρος αυτός της «αμοιβαίας αυθεντικοποίησης» (mutual authentication), κατά την οποία και οι δύο συναλλασσόμενες πλευρές αυθεντικοποιούνται ο ένας στον άλλο ταυτόχρονα.

- **Το αντικείμενο (object)** είναι ένας πόρος ο οποίος προστατεύεται από την πολιτική ασφάλειας.

- **Η εξουσιοδότηση (authorization)** είναι η διαδικασία μέσω της οποίας καθορίζουμε κατά πόσο ένα υποκείμενο επιτρέπεται να έχει πρόσβαση ή να χρησιμοποιήσει κάποιο αντικείμενο.

- **Ένας τομέας εμπιστοσύνης (trust domain)** είναι μια λογική διαχειρίσιμη δομή μέσα στην οποία, εφαρμόζεται μια συγκεκριμένη πολιτική ασφάλειας. Με άλλα λόγια, ο τομέας αυτός είναι μια συλλογή από υποκείμενα και αντικείμενα που ελέγχονται από μια μόνο πολιτική ασφάλειας.

Μπορούμε να καθορίσουμε σύμφωνα με το [21] μια **πολιτική ασφάλειας** όπως η ακόλουθη:

1. **Το περιβάλλον του πλέγματος αποτελείται από πολλούς τομείς εμπιστοσύνης:** Αυτό σημαίνει ότι η πολιτική ασφάλειας πλέγματος πρέπει να ενσωματώνει μια συλλογή τοπικά διαχειρίσιμων χρηστών και πόρων. Γενικά το πλέγμα έχει περιορισμένη επιρροή πάνω στην τοπική πολιτική ασφάλειας.

2. **Οι λειτουργίες που περιορίζονται σε ένα μόνο τομέα εμπιστοσύνης είναι αντικείμενα ελέγχου την τοπικής και μόνο πολιτικής ασφάλειας:** Η τοπική πολιτική ασφάλειας μπορεί να εφαρμοστεί με ένα σύνολο μεθόδων και τεχνολογιών όπως είναι τα firewalls, Kerberos, SSH

3. **Μπορούν να συνυπάρχουν τόσο τα 'παγκόσμια' (global) όσο και τα τοπικά αντικείμενα.** Για κάθε τομέα εμπιστοσύνης, υπάρχει μια μερική αντιστοίχηση-απεικόνιση (mapping) από παγκόσμια σε τοπικά αντικείμενα μέσω του κατάλληλου μηχανισμού. Στην ουσία , κάθε χρήστης ενός πόρου έχει δύο ονόματα ένα με το οποίο θα είναι αναγνωρίσιμος σε όλο το πλέγμα (global) και ένα τοπικού χαρακτήρα (local). Η διαδικασία της απεικόνισης εξαρτάται και από την 'τοποθεσία' (σε σχέση με το domain στο οποίο ανήκει ο κόμβος).
   Επιπροσθέτως, η ύπαρξη παγκόσμιων υποκειμένων, δίνει τη δυνατότητα στην πολιτική ασφάλειας πλέγματος να παρέχει καθολική πιστοποίηση (single sign-on).

4. **Οι λειτουργίες μεταξύ οντοτήτων που βρίσκονται σε διαφορετικούς τομείς εμπιστοσύνης, απαιτούν αμοιβαία αυθεντικοποίηση.**

5. **Ένα αυθεντικοποιημένο παγκόσμιο (global) υποκείμενο που απεικονίζεται σε ένα τοπικό, θεωρείται ότι είναι ισοδύναμο με ένα τοπικά αυθεντικοποιημένο υποκείμενο.**

6. **Όλες οι αποφάσεις ελέγχου πρόσβασης, λαμβάνονται τοπικά έχοντας ως βάση το ίδιο το τοπικό υποκείμενο.** Αυτό σημαίνει ότι οι αποφάσεις ελέγχου πρόσβασης παραμένουν υπό την εποπτεία τον διαχειριστών τοπικών συστημάτων.

7. **Ένα πρόγραμμα ή μια διεργασία επιτρέπεται να δρα εκ μέρους του χρήστη εκπροσωπώντας έτσι και ένα μέρος των δικαιωμάτων που αυτός έχει (ενδεχομένως δικαιώματα χρήσης, πρόσβασης κτλ).** Αυτό από μόνο του παρέχει υποστήριξη στις μεγάλης διάρκειας διεργασίες , οι οποίες κατά την εκτέλεσή τους μπορεί να απαιτήσουν δυναμικά νέους πόρους, χωρίς βέβαια να είναι απαραίτητη η ανθρώπινη παρουσία. Επίσης είναι πολύ σημαντικό, για τη δημιουργία διεργασιών από άλλες διεργασίες.

8. **Οι διεργασίες που δρουν εκ μέρους του ίδιου υποκειμένου , μέσα στο ίδιο τομέα εμπιστοσύνης, μπορούν να μοιράζονται το ίδιο σύνολο διαπιστευτηρίων.** Οι υπολογισμοί πλέγματος μπορούν να περιλαμβάνουν εκατοντάδες διεργασίες πάνω σε ένα πόρο.
   Αυτός ο κανόνας πολιτικής καθιστά δυνατή τη κλιμακωσιμότητα της αρχιτεκτονικής πλέγματος σε μεγάλης κλίμακας εφαρμογές, αποφεύγοντας τη δημιουργία διαπιστευτηρίων για κάθε μια διεργασία ξεχωριστά.

Το σημαντικό στοιχείο σε μια τέτοιου είδους πολιτική ασφάλειας πλέγματος, είναι η δυνατότητα της ένταξης διαφορετικών τοπικών πολιτικών ασφαλείας σε ένα περιβάλλον υπολογιστικής πλέγματος.
Όσο αφορά γενικά το **μοντέλο ασφάλειας πλέγματος**, υπάρχουν τρεις πολύ βασικές λειτουργίες , με βάση το [22]:

1. **Πολλαπλοί μηχανισμοί ασφάλειας :** Οι οργανισμοί που συμμετέχουν σε ένα VO επενδύουν σε υπάρχουσες τεχνολογίες ασφάλειας και υποδομής. Επομένως το μοντέλο ασφάλειας πλέγματος πρέπει να συνεργάζεται μαζί με αυτούς τους μηχανισμούς και όχι να τους αντικαθιστά.

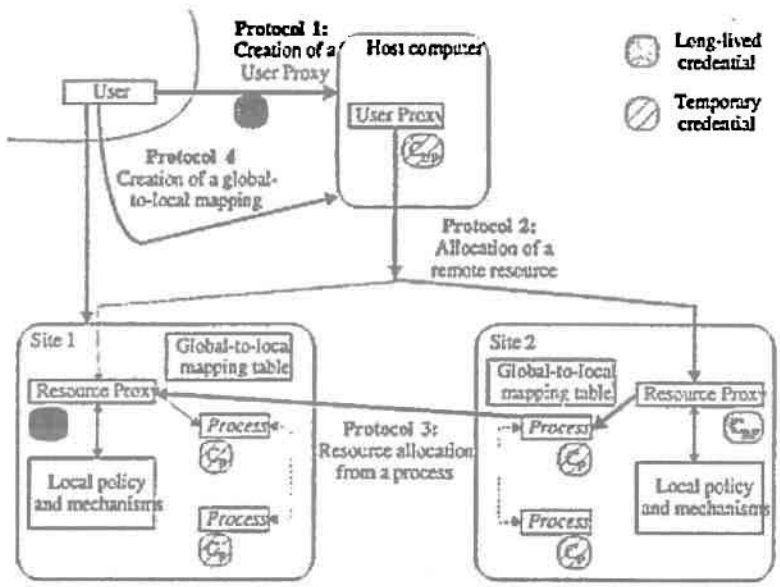
2. **Δυναμική δημιουργία υπηρεσιών:** Οι χρήστες πρέπει να μπορούν να δημιουργούν νέες υπηρεσίες με δυναμικό τρόπο χωρίς την παρέμβαση του διαχειριστή. Αυτές οι υπηρεσίες πρέπει να συνεργάζονται και να αλληλεπιδρούν με ασφαλή τρόπο με άλλες υπηρεσίες.
   Επιπλέον είναι αναγκαίο να μπορούμε να ονομάσουμε αυτές τις υπηρεσίες (με δυναμική ταυτότητα) και να παραχωρούμε δικαιώματα χρήσης σε μια οντότητα χωρίς να υπάρξει σύγκρουση με την επικρατούσα τοπική πολιτική ασφάλειας.

3. **Δυναμική εγκαθίδρυση τομέων εμπιστοσύνης (trust domain):** Προκειμένου να συνεργαστούν οι πόροι, οι εικονικοί οργανισμοί πρέπει να εγκαθιδρύσουν -σχέση εμπιστοσύνης μεταξύ όχι μόνο των χρηστών και πόρων στο VO αλλά μεταξύ των πόρων του ίδιου VO έτσι ώστε να υπάρξει αρμονική συνεργασία. Αυτά τα domains εμπιστοσύνης μπορούν να καλύπτουν πολλούς οργανισμούς και πρέπει να προσαρμόζονται δυναμικά καθώς οι συμμετέχοντες θα 'μπαίνουν' ή θα 'βγαίνουν' από το πλέγμα.

3.4 ΜΟΝΤΕΛΟ ΑΣΦΑΛΕΙΑΣ ΠΛΕΓΜΑΤΟΣ

3.4.1 Αρχιτεκτονική ασφάλεια πλέγματος (Grid Security Architecture)

Η πολιτική ασφάλειας που είδαμε πιο πάνω παρέχει ένα πλαίσιο μέσα στο οποίο μπορούμε να κτίσουμε μια συγκεκριμένη αρχιτεκτονική ασφάλειας. Στο [21] καθορίζονται τα υποκείμενα και τα αντικείμενα, τα οποία θα βρίσκονται κάτω από τον έλεγχο την πολιτικής ασφάλειας, καθώς και τα πρωτόκολλα τα οποία καθορίζουν τις αλληλεπιδράσεις μεταξύ υποκειμένων και αντικειμένων. Η αρχιτεκτονική που προτείνεται , έχει την δομή που φαίνεται στην παρακάτω εικόνα:



Αρχιτεκτονική ασφάλειας υπολογιστικής πλέγματος

Οι πιο έντονες γραμμές απεικονίζουν τα πρωτόκολλα, ενώ η κυρτή γραμμή, που χωρίζει τον χρήστη από το υπόλοιπο κομμάτι υποδεικνύει ότι ο χρήστης κάποια στιγμή μπορεί να αποσυνδέσει τον διαμεσολαβητή χρήστη (user proxy) που δημιούργησε ο ίδιος.
Πρέπει να τονιστεί ότι ένας υπολογισμός αποτελείται από πολλές διεργασίες, καθεμιά εκ των οποίων δρα εκ μέρους κάποιου χρήστη. Τα αντικείμενα σε αυτήν την αρχιτεκτονική, περιλαμβάνουν διαθέσιμους πόρους του πλέγματος όπως υπολογιστές, αποθήκες δεδομένων, δίκτυα, συσκευές απεικονίσεις κτλ. [21].

Οι υπολογισμοί πλέγματος μπορούν να επεκτείνονται ή να συρρικνώνονται δυναμικά, απαιτώντας όταν χρειάζεται πόρους, προκειμένου να λύσουν ένα πρόβλημα, και ελευθερώνοντάς τους όταν πλέον δεν τους χρειάζονται. Κάθε φορά λοιπόν που μια διεργασία αποκτά ένα πόρο, το κάνει εκ μέρους κάποιου χρήστη.

Ωστόσο είναι άσκοπο να εξαναγκάζεται ο χρήστης , να αυθεντικοποιείται , κάθε φορά που αλληλεπιδρά με ένα πόρο. Και αυτό γιατί ο αριθμός των πόρων είναι πολύ μεγάλος. καθιστώντας αναγκαία την ύπαρξη ενός μηχανισμού που δεν θα απαιτεί τη συνεχή παρουσία του χρήστη. Έτσι στη συγκεκριμένη αρχιτεκτονική που εξετάζουμε, εισάγεται η έννοια του διαμεσολαβητή χρήστη (ή καλύτερα user proxy), που δρα εκ μέρους του χρήστης, χωρίς να απαιτείται η επέμβαση του χρήστη.

Ένας καλός ορισμός είναι ο εξής:

«Διαμεσολαβητής χρήστη (user proxy) είναι ένας διαχειριστής διεργασιών που έχει το δικαίωμα να δρα εκ μέρους του χρήστη για περιορισμένο χρονικό διάστημα» [21].

Ο user proxy λειτουργεί σαν προσωρινός αντικαταστάτης του χρήστη. Έχει τα δικά του διαπιστευτήρια, εξαλείφοντας έτσι την ανάγκη να είναι ο χρήστης συνεχώς απασχολημένος με τον υπολογισμό και με την ανάγκη παροχής των διαπιστευτηρίων του χρήστη σε κάθε διαδικασία αυθεντικοποίησης.

Επιπροσθέτως αξίζει να τονιστεί ότι ο χρόνος ζωής του user proxy είναι περιορισμένος και καθορίζεται από τον ίδιο τον χρήστη. Επομένως σε περίπτωση έκθεσης ή κλοπής των διαπιστευτηρίων του proxy, οι επιπτώσεις είναι λιγότερο αρνητικές από ότι θα ήταν η κλοπή των διαπιστευτηρίων του ίδιο του χρήστη.

Στη συγκεκριμένη αρχιτεκτονική, καθορίζεται μια οντότητα που αναπαριστά ένα πόρο, που ουσιαστικά είναι η διεπαφή μεταξύ της αρχιτεκτονικής ασφάλειας πλέγματος και της τοπικής αρχιτεκτονικής πλέγματος.
Αυτή η οντότητα ορίζεται ως εξής:

«Το πληρεξούσιο πόρου (resource proxy) είναι ένας πράκτορας που χρησιμοποιείται για τη συνεργασία μεταξύ διατμηματικών (inter-domain) λειτουργιών ασφαλείας και τοπικών εσωτμηματικών (intra-domain) μηχανισμών». [21].

Για τον καθορισμό των πρωτοκόλλων , χρησιμοποιούνται κάποια γράμματα όπως είναι τα U, R , P που αναφέρονται στον χρήστη, στους πόρους και στις διεργασίες ενώ τα UP, RP αναφέρονται στο user και στο resource proxy αντιστοίχως.
Οι αλληλεπιδράσεις που μπορούν να συμβούν μεταξύ οντοτήτων στην υπολογιστική πλέγματος, καθορίζονται κυρίως από την λειτουργικότητα και τη φύση του. Ωστόσο υπάρχουν κάποιες βασικές λειτουργίες όπως είναι οι παρακάτω:

1. Ανάθεση πόρου από ένα χρήστη
2. Ανάθεση πόρου από μια διεργασία
3. Επικοινωνία μεταξύ διεργασιών που βρίσκονται σε διαφορετικά domains.

Με τον όρο 'ανάθεση' εννοούμε τις λειτουργίες που απαιτούνται για την παροχή σε χρήστη, πρόσβασης σε πόρο. Συνεπώς πρέπει να καθοριστούν πρωτόκολλα που διαχειρίζονται αλληλεπιδράσεις UP-RP, P-RP, P-P . Επιπροσθέτως η εισαγωγή του όρου 'user proxy' καθιστά αναγκαίο τον καθορισμό της αλληλεπίδρασης χρήστη διαμεσολαβητή. Μέσα στην συγκεκριμένη αρχιτεκτονική που μελετάμε, η τελευταία απαίτηση ικανοποιείται , επιτρέποντας στο χρήστη να μπει στο πλέγμα, μέσω ενός διαμεσολαβητή χρήστη χρησιμοποιώντας το πρωτόκολλο 1.
Έπειτα ο user proxy μπορεί να αναθέσει πόρους κάνοντας χρήση του πρωτοκόλλου 2, ενώ μέσω του πρωτοκόλλου 3, μια διεργασία μπορεί να αναθέσει και άλλους πόρους άμεσα. Ακόμη το πρωτόκολλο 4 χρησιμεύει για την απεικόνιση ενός παγκόσμιου αντικειμένου σε τοπικό.
Παρακάτω περιγράφουμε αναλυτικά καθένα από αυτά τονίζοντας ότι βασίζονται στην αυθεντικοποίηση και σε τεχνικές υπογραφής, και όχι κρυπτογράφησης.

- **Πρωτόκολλο δημιουργίας πληρεξούσιου χρήστη (User Proxy Creation Protocol)** : Υπενθυμίζεται ότι το user proxy είναι μια οντότητα μέσα στην συγκεκριμένη αρχιτεκτονική που δρα εκ μέρους του χρήστη. Στην ουσία, πρόκειται για μια ειδική διεργασία , την οποία ξεκινά ο χρήστης. Το βασικό θέμα σε αυτό το πρωτόκολλο είναι η φύση των πιστοποιητικών που δίνονται στο proxy και πως αυτό τα αποκτά. Ο χρήστης θα μπορούσε να επιτρέψει στο user proxy να δράσει εκ μέρους του δίνοντάς του τα κατάλληλα πιστοποιητικά.
  Έπειτα το user proxy θα μπορούσε άμεσα να τα χρησιμοποιήσει όπου θα απαιτούνταν αυθεντικοποίηση. Ωστόσο σε μια τέτοια περίπτωση υπάρχουν δύο σημαντικά μειονεκτήματα.
  Το πρώτο είναι ότι υπάρχει αυξημένος κίνδυνος να κλαπούν τα πιστοποιητικά και το δεύτερο είναι ότι δεν επιτρέπεται στο χρήστη να επέμβει στο χρόνο κατά τον οποίο το user proxy θα δρα εκ μέρους του. Αντί αυτού δημιουργείται ένα προσωρινό πιστοποιητικό Cup .
  Ο χρήστης το υπογράφει με ένα προσωπικό του κλειδί. Εκτός από την υπογραφή του χρήστη, στο Cup υπάρχουν και άλλες πληροφορίες όπως που θα εκτελεστεί ο κώδικας, σε ποιον host κτλ. Η έννοια του user proxy δεν είναι καινούργια. Για παράδειγμα, στο σύστημα Kerberos, παράγεται ένα περιορισμένου χρόνου ticket για την αναπαράσταση του χρήστη.
  Πολλά άλλα συστήματα δημοσίου κλειδιού, χρησιμοποιούν τέτοια τεχνική, κατά την οποία προσωρινά πιστοποιητικά χρησιμοποιούνται για να παράγουν ένα είδος πιστοποιητικού το οποίο έπειτα υπογράφεται από τον χρήστη. Αυτό που διαφέρει στην περίπτωση που εξετάζουμε είναι ο τρόπος που το user proxy αλληλεπιδρά με το resource proxy για να επιτευχθεί καθολική πιστοποίηση και ανάθεση δικαιωμάτων πρόσβασης.

- **Πρωτόκολλο ανάθεσης πόρων (resource allocation protocol by user proxy):** Μελετώντας το συγκεκριμένο πρωτόκολλο, μπορούμε να διακρίνουμε δύο υποπεριπτώσεις αυτή *της ανάθεσης πόρων από το user proxy* και *της ανάθεσης πόρων από διεργασία*. Η τελευταία είναι μια γενίκευση της πρώτης, την οποία μελετούμε πρώτη. Υπενθυμίζεται ότι οι πόροι του πλέγματος ελέγχονται από μια οντότητα που ονομάζεται **πληρεξούσιο πόρου** ή πιο απλά **resource proxy**, το οποίο είναι υπεύθυνο για την ελεγχόμενη πρόσβαση σε πόρους και στην ανάθεση κάποιου υπολογισμού σε αυτόν τον πόρο [21]. Το resource proxy λειτουργεί ως εξής: Το user proxy που απαιτεί πρόσβαση σε ένα πόρο , αρχικά εξακριβώνει την ταυτότητα του resource proxy για αυτό τον πόρο. Αν το αίτημα είναι επιτυχημένο, ο πόρος ανατίθεται και μια διεργασία δημιουργείται σε αυτόν. Βέβαια το αίτημα μπορεί να αποτύχει είτε λόγω μη διαθεσιμότητας του πόρου, είτε γιατί ο χρήστης δεν μπορεί να αυθεντικοποιηθεί, είτε γιατί δεν έχει το δικαίωμα πρόσβασης στον πόρο. Όπως αναφέρθηκε πιο πάνω, το resource proxy μπορεί να επιβάλλει και να εφαρμόσει τοπική πολιτικής ασφάλειας.
  Εξαρτώμενος από την φύση του πόρου και την τοπική πολιτική ασφάλειας, ο έλεγχος εξουσιοδότησης μπορεί να γίνει κατά την ανάθεση πόρου ή κατά τη στιγμή δημιουργίας της διεργασίας. Κατά την φάση της πιστοποίησης, μπορεί να απαιτηθεί η αντιστοίχηση των πιστοποιητικών του χρήστη σε κάποιο τοπικό user id ή σε κάποιο τοπικό λογαριασμό. Το συγκεκριμένο πρωτόκολλο δημιουργεί ένα προσωρινό πιστοποιητικό για τις νέες διεργασίες. Αυτό το πιστοποιητικό Cp . δίνει τη δυνατότητα στη διεργασία να αυθεντικοποιεί τον εαυτό της και την πιστοποίηση του χρήστη εκ μέρους του οποίου δρα. Η ύπαρξη πιστοποιητικών διεργασιών, μας επιτρέπει να αναπτύξουμε πρόσθετα πρωτόκολλα που επιτρέπουν μια διεργασία να ελέγχει την πρόσβαση κατά την επικοινωνία με τον πόρο.

- **Πρωτόκολλο ανάθεσης πόρων από διεργασία (resource allocation protocol by process):** Αν και η ανάθεση πόρων από user proxy είναι αναγκαία για την έναρξη των υπολογισμών, η πιο συνηθισμένη περίπτωση είναι ότι η ανάθεση πόρων γίνεται δυναμικά από μια διεργασία που δημιουργήθηκε από το προηγούμενο αίτημα ανάθεσης πόρων.
  Με λίγα λόγια συμβαίνουν τα εξής: Η διεργασία και το user proxy αυθεντικοποιούνται ο ένας στον άλλο μέσω των Cp, Cup.
  Η διεργασία εκδίδει ένα υπογεγραμμένο αίτημα στο user proxy της με παραμέτρους που σχετίζονται με την ανάθεση πόρων. Αν το user proxy κάνει δεκτό το αίτημα, στέλνει αίτημα ανάθεσης πόρων στο κατάλληλο resource proxy και επιστρέφεται η διεργασία που έχει κάνει τους τελικούς υπολογισμούς.
  Ομολογουμένως , αυτή η τεχνική στερείται κλιμακωσιμότητας, λόγω της εμπιστοσύνης που δίνεται σε ένα και μόνο user proxy , για να μεταδώσει το αίτημά του στο resource proxy. Ωστόσο το πρωτόκολλο αυτό έχει το πλεονέκτημα της απλότητας και ταυτόχρονα του λεπτομερούς ελέγχου (fine-grain control), ο οποίος απαιτεί πολλά στάδια επεξεργασίας.

  Ας αναλογιστούμε μια ακριβώς αντίθετη περίπτωση όπου επιτρέπεται σε μια διεργασία να αναθέτει παραπάνω (από το επιτρεπόμενο όριο) πόρους και να δημιουργεί μονομερώς νέες διεργασίες. Σε αυτή λοιπόν την περίπτωση έχουμε δύο περιορισμούς:

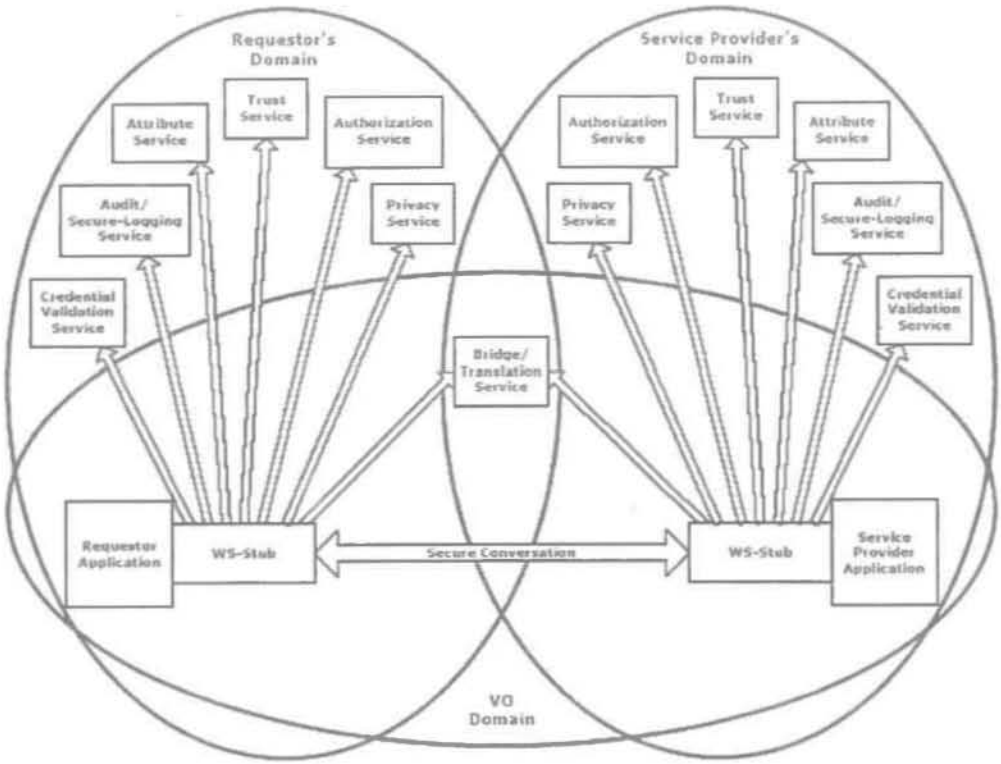
  1. Ο χρήστης πρέπει να μπορεί να κωδικοποιεί και να εισάγει σε κάθε διεργασία μια πολιτική ώστε να ικανοποιούνται κάποια ξεχωριστά κριτήρια για την ανάθεση πόρων.

  2. Μια παραβίαση στην ασφάλεια σε ένα απομακρυσμένο site μπορεί να καταλήξει σε κακόβουλες αναθέσεις πόρων οι οποίες θα γίνονται εν αγνοία του χρήστη.

  Η δημιουργία συγκεκριμένων πιστοποιητικών για τη διεργασία, καταλήγουν στην εκχώρηση δικαιωμάτων (delegation) από το χρήστη στη διεργασία. Αυτό που κάνει την αρχιτεκτονική αυτή να διαφέρει από άλλες delegation –based είναι ο ρόλος που παίζει το πληρεξούσιο πόρων-resource proxy. Στην αρχιτεκτονική μας λοιπόν η αυθεντικοποίηση γίνεται **πάντα** μεταξύ user και resource proxy.
  Συνεπώς το πρωτόκολλο καθολικής πιστοποίησης ενισχύει την σχέση εμπιστοσύνης που είχε εγκαθιδρυθεί μεταξύ του χρήστη και του πόρου, όταν για πρώτη φορά ο χρήστης είχε αποκτήσει πρόσβαση σε αυτόν τον πόρο.

- **Πρωτόκολλο εγγραφής αντιστοιχήσεων (Mapping Registration Protocol):** Ένα ακόμα βασικό συστατικό της πολιτικής ασφάλειας που είδαμε πιο πάνω, είναι η ύπαρξη ενός μηχανισμού αντιστοίχησης μεταξύ ενός παγκόσμιου αντικειμένου και ενός ισοδύναμου τοπικού αντικειμένου. Αυτή η μετατροπή από παγκόσμια ονομασία (ετικέτα ή πιστοποιητικό) σε τοπικό όνομα (login όνομα. ή user ID) σύμφωνα και με το[21] επιτυγχάνεται μέσω ενός πίνακα αντιστοίχησης (mapping table) που κρατείται στο resource proxy. Στην ίδια βιβλιογραφία, αναφέρεται μια τεχνική που επιτρέπει στον ίδιο χρήστη να προσθέτει πίνακα mapping.Η βασική ιδέα πίσω από αυτή τη τεχνική είναι να διευκολυνθεί ο χρήστης για να αποδείξει ότι είναι κάτοχος των πιστοποιητικών του παγκόσμιου και τοπικού αντικειμένου. Αυτό επιτυγχάνεται κάνοντας άμεση αυθεντικοποίηση στο πόρο μέσω τοπικής μεθόδου αυθεντικοποίησης.

3.4.2 Υπηρεσίες ασφάλειας πλέγματος (Grid Security Services)



Υπηρεσίες ασφάλειας πλέγματος

Η κλήση υπηρεσιών πλέγματος, αναδεικνύει την ανάγκη για ένα μοντέλο ασφάλειας που θα καθορίζει επακριβώς τα αντικείμενα ασφάλειας με βάση και τις απαιτήσεις ασφάλειας του πλέγματος
Σύμφωνα με το [25] η αρχιτεκτονική ασφάλειας πλέγματος πρέπει να διασφαλίζει ότι οι υπηρεσίες πλέγματος όταν καλούνται από κάποιο χρήστη, θα πρέπει να εφαρμόζονται κανόνες-πολιτικές ασφάλειας που θα καθορίζονται από το συγκεκριμένο περιβάλλον. Αυτές οι πολιτικές μπορούν να περιλαμβάνουν συγκεκριμένο τύπο πιστοποιητικών , απαιτήσεις εμπιστευτικότητας κτλ.
Η ίδια η υπηρεσία , από την άλλη μεριά , θα πρέπει να έχει όλα εκείνα τα χαρακτηριστικά ασφάλειας (πιστοποιητικά, εμπιστευτικότητα κτλ) ώστε ο αιτών να μπορεί με ασφάλεια να συναλλαχθεί μαζί της.

Όπως οποιαδήποτε υπηρεσία, έτσι και οι υπηρεσίες ασφάλειας πλέγματος πρέπει να εκτίθενται ως web υπηρεσίες (WSDL). Οι υπηρεσίες πρέπει να διασφαλίζονται κάνοντας χρήστη των μηχανισμών του μοντέλου ασφάλειας πλέγματος.

Με βάση την ίδια βιβλιογραφία, ένα ενδεικτικό σύνολο από υπηρεσίες ασφάλειας πλέγματος είναι και το παρακάτω:

- **Υπηρεσία αυθεντικοποίησης (authentication service):** Μια τέτοια υπηρεσία ασχολείται κυρίως με την εξακρίβωση της ταυτότητας ενός αντικειμένου (χρήστη, user proxy). Ένα χαρακτηριστικό παράδειγμα είναι η αξιολόγηση του συνδυασμού User Id -password ενός χρήστη που κάνει κάποιο αίτημα για πόρο ή υπηρεσία.

- **Υπηρεσία αντιστοίχησης ταυτότητας (Identity Mapping Service):** Η συγκεκριμένη υπηρεσία παρέχει τη δυνατότητα μετασχηματισμού της ταυτότητας ενός χρήστη σε ένα domain, σε μια άλλη ταυτότητα, που θα αντιστοιχεί σε διαφορετικό τοπικό domain .

- **Υπηρεσία εξουσιοδότησης (authorization service):** Η συγκεκριμένη υπηρεσία ασχολείται με την λήψη απόφασης σχετικά με την πρόσβαση με βάση κάποια πολιτική. Η υπηρεσία, εκμεταλλεύεται πλήρως το πιστοποιητικό του αιτούντα για κάποιο πόρο-υπηρεσία , χρήστη, που έχει ήδη αυθεντικοποιηθεί, και με βάση τη πολιτική πρόσβασης αποφασίζεται αν θα επιτραπεί στο χρήστη η πρόσβαση στην υπηρεσία που ζητά.

- **Υπηρεσία πολιτική ασφάλειας εικονικών οργανισμών (VO policy service):** Η υπηρεσία αυτή, ασχολείται με τη διαχείριση των πολιτικών ασφάλειας. Η συσσωμάτωση των πολιτικών ασφάλειας που διαχειρίζονται από αυτήν συνθέτουν ένα ενιαίο σύνολο πολιτικών VO.

- **Υπηρεσία μετατροπής πιστοποιητικών (Credential Conversion service):** Η υπηρεσία αυτή παρέχει τη δυνατότητα μετατροπής μεταξύ ενός τύπου πιστοποιητικού σε ένα άλλο τύπο. Αυτό προϋποθέτει την διευθέτηση ζητημάτων σχετικά με την ιδιότητα μέλους ενός group καθώς και την αποδοχή γνωρισμάτων και προνομιών που πηγάζουν από αυτή.Π.χ, η υπηρεσία μετατροπής πιστοποιητικών μπορεί να αλλάξει ένα πιστοποιητικό Kerberos σε ένα διαφορετικού τύπου πιστοποιητικό το οποίο απαιτεί η υπηρεσία εξουσιοδότησης. Επιπροσθέτως, τονίζεται ότι η συγκεκριμένη υπηρεσία συνεργάζεται και με την υπηρεσία αντιστοίχησης ταυτότητας.

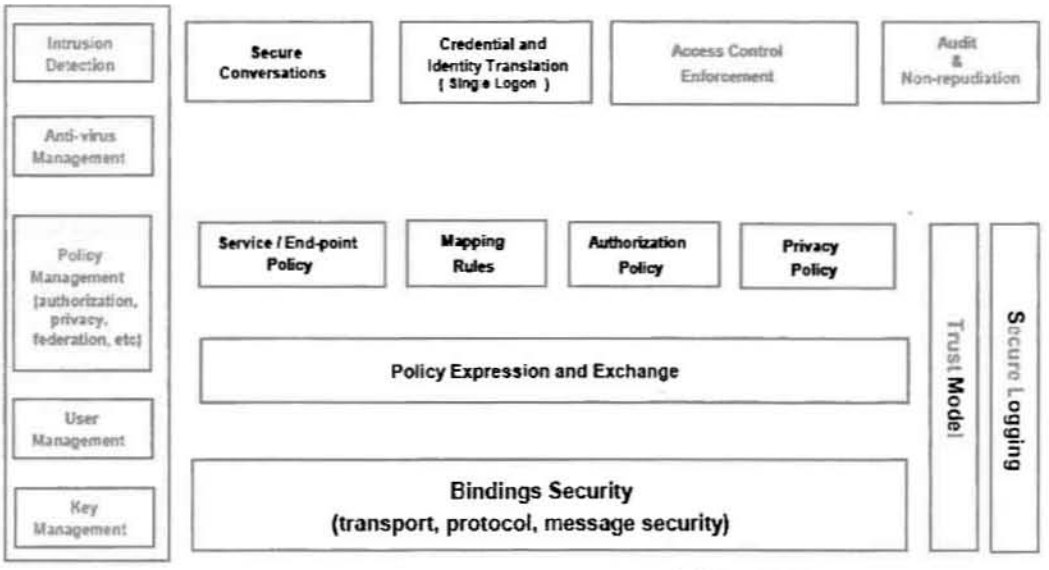
- **Υπηρεσία ελέγχου (audit Service):** Αυτή η υπηρεσία, όπως και αυτή της αντιστοίχησης ταυτότητας αλλά και της εξουσιοδότησης, είναι ελεγχόμενες από πολιτικές ασφάλειας.. Είναι υπεύθυνη για την παραγωγή εγγραφών που καταγράφουν γεγονότα που σχετίζονται με θέματα ασφάλειας (πρόσβασης και χρήσης υπηρεσιών, πόρων, αυθεντικοποίηση κτλ.).
  Οι παραγόμενες εγγραφές εξετάζονται λεπτομερώς προκειμένου να διαπιστωθεί αν εφαρμόζεται η επιθυμητή πολιτική ασφάλειας. Η συγκεκριμένη διαδικασία γίνεται από τους διαχειριστές των εκάστοτε VO προκειμένου να ελέγξουν αν υπάρχει απαρέγκλιτη τήρηση των πολιτικών πρόσβασης και αυθεντικοποίησης.

- **Υπηρεσία προφίλ (Profile service):** Η υπηρεσία προφίλ ασχολείται με τη διαχείριση των προτιμήσεων του χρήστη που κάνει αίτηση για υπηρεσία. Μπορεί να πρόκειται για συγκεκριμένα εξατομικευμένα δεδομένα, που μπορούν να χρησιμοποιηθούν για να κτίσουν π.χ ένα προφίλ εμπειρίας για το συγκεκριμένο χρήστη.

- **Υπηρεσία ιδιωτικότητας (Privacy Service):** Στόχος της υπηρεσίας αυτής είναι η κατηγοριοποίηση προσωπικών εξακριβωμένων πληροφοριών. κατηγοριοποίηση - που βασίζεται σε πολιτικές ασφάλειας. Αυτήν την υπηρεσία. τη χρησιμοποιούν κυρίως πάροχοι υπηρεσιών.

3.5 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΣΦΑΛΕΙΑΣ OGSA

Στη συγκεκριμένη ενότητα , θα μελετήσουμε την αρχιτεκτονική ασφάλειας OGSA, και θα δούμε κάποιες βασικές υπηρεσίες της. Η αρχιτεκτονική ασφάλειας OGSA σχηματικά, φαίνεται στην παρακάτω εικόνα :



Αρχιτεκτονική ασφάλειας OGSA [26]

Στη συγκεκριμένη πολυ-επίπεδη αρχιτεκτονική, τα συστατικά των εφαρμογών όπως «ασφαλής επικοινωνία», «Μετατροπή πιστοποιητικών», «Εφαρμογή ελέγχου πρόσβασης» κτλ, εξαρτώνται από πολιτικές και κανόνες που σχετίζονται με εξουσιοδότηση, ιδιωτικότητα
Παρακάτω, θα μελετήσουμε, τις σημαντικότερες και πιο βασικές σύμφωνα και με το [26] προδιαγραφές και χαρακτηριστικά της ασφάλειας στην αρχιτεκτονική OGSA.

3.5.1 Προσδιορισμός ονομασίας (Naming)

Η ασφάλεια στην αρχιτεκτονική OGSA καθορίζει ένα σύνολο απαιτήσεων όσο αφορά στην ανάθεση ονομάτων σε χρήστες, υπηρεσίες, γνωρίσματα και μεθόδους. Συγκεκριμένα έχουμε:

- **Εφαρμογή εξουσιοδότησης:** Απαιτείται στις αξιολογήσεις των πολιτικών ασφάλειας, να παρέχονται ονομασίες έγκυρες σε χρήστες, πάροχους υπηρεσιών κτλ. Μάλιστα πρέπει να υπάρξει προτυποποίηση των ονομάτων αυτών, ώστε να υπάρχουν μοναδικές ονομασίες ανάμεσα σε διαφορετικές περιοχές.

- **Αντιστοίχηση γνωρισμάτων:** Γνωρίσματα και ιδιότητες, συχνά αντιστοιχίζονται με συγκεκριμένες ονομασίες των οντοτήτων. Μάλιστα η έκφραση των ονομάτων πρέπει να είναι συνεπής και αυτό γιατί μπορεί να γίνει αντιστοίχηση γνωρισμάτων σε μια οντότητα σε μια περιοχή και έπειτα να γίνει αποτίμηση της από κάποια άλλη οντότητα σε άλλη περιοχή.

- **Έλεγχος χρήστη (auditing):** Η απαίτηση για σωστή ονομασία, αφορά και τον έλεγχο χρήστη καθώς τα ονόματα των οντοτήτων και των ενεργειών τους, συχνά καταγράφονται σε αρχεία logs. Άρα και εδώ πρέπει να υπάρχει συνέπεια στην ονομασία.

3.5.2 Μετατροπή μεταξύ περιοχών ασφάλειας (Translating between Security Realms)

Είναι αναγκαία η δυνατότητα μετατροπής ή καλύτερα μετάφρασης μιας ενέργειας ανάμεσα σε περιοχές ασφάλειας όπως όταν γίνεται κάποιο αίτημα για μια απομακρυσμένη υπηρεσία. Αυτή η μετάφραση έγκειται στην ύπαρξη διαφορετικών μηχανισμών ασφάλειας, διαφορετικών οργανισμών, δομών κτλ. Για αυτό το σκοπό, αναπτύχθηκαν TOGAS υπηρεσίες που φροντίζουν για την μετατροπή των τύπων των πιστοποιητικών για την αντιστοίχηση ονομασιών, πολιτικών ασφάλειας κτλ.

3.5.3 Μηχανισμός αυθεντικοποίησης

Πρόκειται για ένα από τα κυριότερα χαρακτηριστικά της αρχιτεκτονικής ασφάλειας OGSA. Η OGSA πρέπει να υποστηρίζει πολλαπλούς μηχανισμούς αυθεντικοποίησης (agnostic) συμπεριλαμβανομένης της υποδομής δημοσίου κλειδιού PKI και Kerberos. Μάλιστα θα ήταν επιθυμητό οι υλοποιήσεις OGSA να υποστηρίζουν ταυτόχρονα πολλούς μηχανισμούς προκείμενου να γεφυρώσουν τις όποιες διαφορές των μηχανισμών αυθεντικοποίησης ανάμεσα σε διαφορετικά domains.

Υποδομή δημοσίου κλειδιού

Συχνά είναι καλό οι υλοποιήσεις OGSA να συνεργάζονται με διαφορετικές παραλλαγές του PKI όπως X.509, PGP, AADS.
Σε κάθε περίπτωση η υλοποίηση OGSA πρέπει να τηρεί απαρέγκλιτα τις τοπικές πολιτικές αξιολόγησης πιστοποιητικών.
Προκειμένου όμως να επιτευχθεί αυτός ο διαλειτουργικός χαρακτήρας του PKI πρέπει να καθορισθεί μια υπηρεσία αξιολόγησης πιστοποιητικών που να μπορεί να συνεργάζεται με όλες τις υλοποιήσεις OGSA προκειμένου να αναλύεται το πιστοποιητικό, να γίνεται αξιολόγησή του με βάση την τοπική πολιτική ασφάλειας και να επεξεργαστούν οι όποιες ενδιαφέρουσες πληροφορίες του.

Kerberos

Το σύστημα αυτό, χρησιμοποιεί το δικό του τύπο μηνυμάτων καθώς και πρωτόκολλα αυθεντικοποίησης και ετικέτες αιτημάτων. Για να διευκολύνουμε τη χρήση του Kerberos στο πλαίσιο της αρχιτεκτονικής OGSA , μπορούμε να 'τυλίξουμε' τα πρωτόκολλα μηνυμάτων του Kerberos για αυθεντικοποίηση, καθώς και τις ετικέτες αιτημάτων , μέσα στα πρωτόκολλα web υπηρεσιών. Και αυτό έτσι ώστε οι επικοινωνίες πελάτη-Kerberos server και πελάτης-PKI Server να χρησιμοποιούν το ίδιο πρωτόκολλο , τις ίδιες δυνατότητες δρομολόγησης καθώς και μηχανισμούς ανακάλυψης υπηρεσιών πόρων του πλέγματος.

3.5.4 Εξουσιοδότηση

Οποιαδήποτε αλληλεπίδραση ανάμεσα σε δύο πλευρές στο πλέγμα, απαιτεί αποφάσεις εξουσιοδότησης και από τους δύο. Ο αιτών μια υπηρεσία στο πλέγμα, εξακριβώνει ότι η πολιτική ασφάλειας του επιτρέπει να κάνει αίτημα. Οι κανόνες ασφάλειας μπορεί να είναι απλοί ή πιο περίπλοκοι , αλλά πρέπει σε κάθε περίπτωση να μπορούν να καθορίσουν αν ένα αντικείμενο, πόρος μπορεί να προσπελαστεί από τον αιτούντα.

3.6 ΑΣΦΑΛΕΙΑ ΕΙΚΟΝΙΚΩΝ ΟΡΓΑΝΙΣΜΩΝ (Virtual Organization Security)

Ο εικονικός οργανισμός **είναι ένα σύνολο είτε μεμονωμένων χρηστών είτε διαφόρων οργανισμών / εταιρειών ή ινστιτούτων, που μέσω του πλέγματος , συνεργάζονται για την επίλυση δύσκολων και απαιτητικών επιστημονικών προβλημάτων. [2]**

Βασικό πρόβλημα που καλούνται να αντιμετωπίσουν οι επιστήμονες, είναι να παρέχουν ασφαλείς μηχανισμούς, ώστε οι πάροχοι και καταναλωτές υπηρεσιών και πόρων να μπορούν να καθορίσουν με σαφήνεια αυτά που πρέπει να διαμοιραστούν , ποιος επιτρέπεται να τα χρησιμοποιήσεις και υπό ποιες συνθήκες.

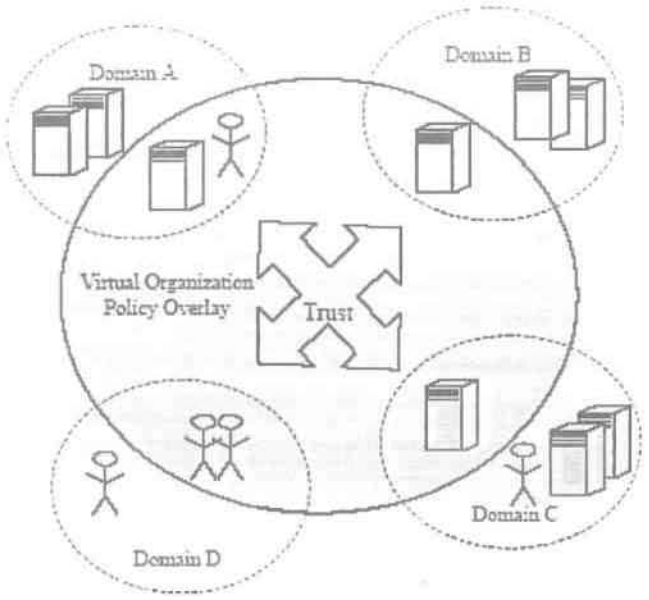
Η προσέγγιση των προκλήσεων ασφάλειας πλέγματος, στο [22] δίνει βαρύτητα στην υποστήριξη κλιμακώσιμων, δυναμικών, κατανεμημένων εικονικών οργανισμών (virtual organization-VOs). Σε μια τέτοια περίπτωση , οι συμμετέχοντες και οι πόροι ελέγχονται από κανόνες και πολιτικές των κλασσικών οργανισμών των οποίων αποτελούν μέρος.

Μια θεμελιώδη απαίτηση με βάση και το [22] είναι η δυνατότητα των VO να έχουν πρόσβαση στους πόρους που υπάρχουν μέσα στους πραγματικούς οργανισμούς, οι οποίοι με τη σειρά τους έχουν πολιτικές χρήσης και ασφάλειας που αναφέρονται σε τοπικούς χρήστες. Φαίνεται ξεκάθαρα η ανάγκη ενός μηχανισμού διαμεσολάβησης.

Αυτού του είδους η πρόσβαση των VO πρέπει να βασίζεται μόνο σε 'δυαδικές' σχέσης εμπιστοσύνης που θα υπάρχουν μεταξύ

1. του τοπικού χρήστη και του οργανισμού
2. του VO και του χρήστη.

Οι μηχανισμοί ασφάλειας πλέγματος, επιλαμβάνονται των προκλήσεων αυτών, επιτρέποντας ένα VO να θεωρείται σαν ένα ενιαίο τμηματικό σύνολο πολιτικής (policy domain overlay) όπως φαίνεται στην παρακάτω εικόνα.



Ενοποίηση πολιτικών ασφάλειας διαφόρων εικονικών οργανισμών σε μια ενιαία που τις συνδυάζει

Αυτό που συμβαίνει , είναι ότι πολλαπλοί πόροι ή οργανισμοί κοινοποιούν σε κάποιο VO μια συγκεκριμένη πολιτική ελέγχου , ο οποίος αναλαμβάνει να συντονίζει όλες τις κοινοποιημένες πολιτικές με ένα συνεπή τρόπο, ώστε να επιτρέπεται η συντονισμένη διαμοίραση πόρων καθώς και η χρήση τους. Επιπροσθέτως , όπως αναφέρθηκε και πιο πάνω, το όλο μοντέλο βασίζεται σε σχέσεις εμπιστοσύνης μεταξύ των συμμετεχόντων στο πλέγμα.
Παρακάτω δίνονται συνοπτικά οι βασικές απαιτήσεις και προκλήσεις που σχετίζονται με την ασφάλεια των εικονικών οργανισμών, και έπειτα αναλύουμε κάποιες έννοιες των πολιτικών ασφάλειας VO. [18]

- **ΔΙΑΧΕΙΡΙΣΗ VO**

1. Ανακάλυψη εικονικών οργανισμών από τους άλλους συμμετέχοντες στο πλέγμα.

2. Αυθεντικοποίηση και εξουσιοδότηση των συμμετεχόντων προκειμένου να έχουν πρόσβαση στο VO

3. Έλεγχος πρόσβασης σε κοινά διαμοιράσιμους πόρους VO

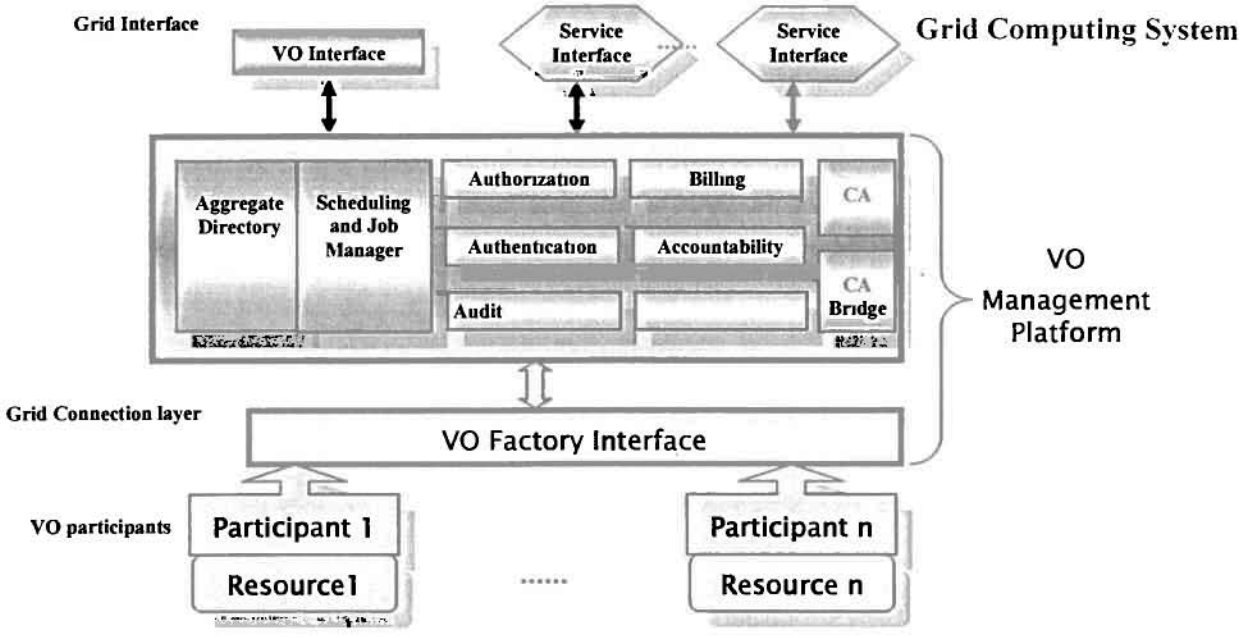
- **ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ VO**

1. Μεγάλος αριθμός κατανεμημένων πόρων.

2. Δυναμικές και περίπλοκες σχέσεις ανάμεσα σε οργανισμούς και περιοχές εμπιστοσύνης.

3. Δύσκολη διαχείριση της χρήσης των πόρων του πλέγματος

Η παρακάτω εικόνα μας δίνει μια αναπαράσταση όλων των παραπάνω



3.6.1 Πολιτική ασφάλειας σε εικονικούς οργανισμούς

Η πολιτική ασφάλειας για εικονικούς οργανισμούς , με βάση το [29] μπορεί να χωριστεί σε τρεις κατηγορίες:

- **Συνολική λειτουργική πολιτική VO (VO-wide operational policy)→** Η συγκεκριμένη πολιτική αποτελείται από συνθήκες σχετικά με τη λειτουργική κατάσταση του εικονικού οργανισμού. Συγκεκριμένα αυτός ο τύπος πολιτικής περιγραφή την κατανομή της χρήσης των πόρων κατά μήκος ολόκληρου του εικονικού οργανισμού. Μια τέτοια πολιτική θα μπορούσε να είναι η εξής "Ο φόρτος εργασία του εικονικού οργανισμού πρέπει να μοιραστεί εξίσου σε όλους τους χρήστες μέλη του", ή η ακόλουθη "όλες οι εργασίες να πραγματοποιηθούν σε συστήματα ουράς από τις 9 το πρωί μέχρι τις 5 το απόγευμα."
  Για τον καθορισμό τέτοιας πολιτικής, πρέπει να καθοριστούν σαφείς κανόνες διαχείρισης. Π.χ μια συνθήκη-κανόνας μπορεί να είναι της μορφής "αν ένα site δεν επιτυγχάνει το 25% της συνολικής εργασίας, των υπολοίπων , όλη η εργασία θα επαναπρογραμματιστεί πάνω σε αυτό μέχρι να εξισορροπηθεί το συνολικό έργο στο πλέγμα". Αυτή περιγράφει μια δυναμική συνθήκη που υπό συγκεκριμένες καταστάσεις, μπορεί να παρέμβει μέσω συγκεκριμένων ενεργειών.

- **Πολιτική για τους πόρους (VO policy on resources)→** Η συγκεκριμένη πολιτική περιγράφει τους κανόνες του εικονικού οργανισμού, που αφορούν την 'συμπεριφορά' των πόρων –μελών του. Αυτού του είδους η πολιτική είναι χρήσιμη για τον καθορισμό κανόνων που θα αφορούν σε συγκεκριμένους πόρους μέσα στον εικονικό οργανισμό, παρά κατά μήκος όλου του οργανισμού.

Χαρακτηριστικά παραδείγματα είναι τα ακόλουθα "Το τμήμα Χημείας πρέπει να παρέχει στο VO του πανεπιστημίου τη δυνατότητα χρήσης υπολογιστικών πόρων από τα μεσάνυχτα μέχρι τις 6 το πρωί " , και το "το τμήμα αστρονομίας πρέπει να παρέχει στο VO το 20% του χρόνου για χρήση τηλεσκόπιου". Όπως και στην προηγούμενη πολιτική ασφάλειας, έτσι και εδώ η συγκεκριμένη πολιτική πρέπει να διατυπώνεται με συγκεκριμένους κανόνες που θα περιγράφουν την εφαρμογή της. Στο [29] τονίζεται ότι αν ένας πόρος δεν ικανοποιεί τις απαιτήσεις της πολιτικής του VO, τότε σαν ανταπόδοση το site μπορεί να έχει μειωμένη πρόσβαση στους υπόλοιπους πόρους του εικονικού οργανισμού.

- **Πολιτική για τους χρήστες (VO policy on users)** : Πρόκειται για το τρίτο είδος πολιτικής που καθορίζει κανόνες για τους χρήστες των πόρων του εικονικού οργανισμού, αλλά αυτή τη φορά από την οπτική γωνία του εικονικού οργανισμού. Αυτοί οι κανόνες δεν χρειάζεται να είναι αποκλειστικά της μορφής «επιτρέπω /απαγορεύω συγκεκριμένες ενέργειες» , απλώς μπορούν να προσδιορίζουν τι ακριβώς πρέπει να κάνει ο χρήστης προτού προβεί σε μια συγκεκριμένη ενέργεια, αλλά και τι πρέπει να κάνει μετά από αυτή.

Δύο χαρακτηριστικές πολιτικές ασφάλειας , με βάση το [29] είναι οι παρακάτω:

Πολιτική 1: Η συνολική χρήση πόρων διαιρείται ισομερώς σε όλους τους πόρους-μέλη του πλέγματος (Πολιτική 1/N)

Πολιτική 2: Κάθε χρήστης λαμβάνει τόση πρόσβαση σε ένα πόρο (για χρήση) όση πρόσβαση παρέχει και ο ίδιος σε άλλους χρήστης (you-get-what-you-give)

Επιπροσθέτως, σημαντικό ρόλο έχει η πολιτική ασφάλειας VO και για τη μέτρηση της χρήσης πόρων. Και αυτό γιατί πολλές φορές είναι αναγκαίο να εξακριβωθεί αν μια πολιτική χρήσης εκπληρώνεται πλήρως. Αυτό μπορεί να γίνει μέσω κάποιων μηχανισμών μέτρησης της χρήσης (Utilization Measurement). Ένα χαρακτηριστικό παράδειγμα είναι ένα Web portal μέσω του οποίου οι χρήστες μπορούν να ανεβάζουν τα αρχεία τους (uploading) στον εικονικό οργανισμό από τους υπολογιστές τους, ενώ το portal από μόνο του καθορίζει που μπορεί ο χρήστης να αποθηκεύσει τα αρχεία του.

Αυτή η αρχιτεκτονική, παρέχει ένα μοναδικό σημείο από όπου όλη η πληροφορία διαχέεται από και προς τον VO και έτσι μπορεί να ελεγχθεί η συνολική χρήση πόρων μέσω των αιτημάτων και των συναλλαγών των πελατών. Αυτή η ευκολία της μέτρησης χρήσης θα βοηθήσει και στην κοστολόγηση (accounting) που μπορεί να εφαρμόσει κάποιος VO για το domains του. Η υπηρεσία κοστολόγησης, αυτό που κάνει είναι να μεταγλωττίζει τις πληροφορίες που αφορούν τη χρήση πόρων και έπειτα γίνεται έλεγχος για τη σωστή εφαρμογή της πολιτικής ασφάλειας.

Κλείνοντας την ενότητα αυτή της ασφάλειας , τονίζουμε ότι ένα ακόμα σημαντικό ζήτημα και για τα 3 είδη πολιτικών που είδαμε, είναι η εξακρίβωση όλων των μηνυμάτων που δέχεται μια υπηρεσία VO. Καθώς ο εικονικός οργανισμός γίνεται ολοένα και μεγαλύτερος, περιλαμβάνοντας πολλά μέλη, υπάρχει μεγάλος κίνδυνος δημιουργίας πλαστών δεδομένων χρήσης υπηρεσιών και πόρων, πράγμα που θα ήταν ολέθριο για τον εικονικό οργανισμό.

Μία λύση σε αυτό το πρόβλημα, είναι η χρήση ψηφιακών υπογραφών στα μηνύματα που ανταλλάσσουν οι υπηρεσίες. Αυτό μπορεί να επιτευχθεί με τη χρήση κρυπτογραφίας δημοσίου κλειδιού καθώς και με την χρήση πιστοποιητικών X.509.

Επομένως, οποιαδήποτε αναφορά σχετικά με χρήση δεδομένων , στέλνεται στο σύστημα κοστολόγησης από ένα πόρο, θα πρέπει να είναι υπογεγραμμένη από το ιδιωτικό κλειδί αυτού του πόρου.
Αυτό βέβαια υπό την προϋπόθεση ο κάθε πόρος έχει το δικό του πιστοποιητικό. Βέβαια υπάρχει και η περίπτωση, ενώ οι ψηφιακές υπογραφές αποτρέπουν από την παράνομη αλλαγή στοιχείων χρήσης, να έχουμε ψεύτικα αιτήματα χρηστών προς τον πόρο (bogus user request). Αυτό λοιπόν απαιτεί από όλα τα αιτήματα των χρηστών να υπογράφονται από τον ίδιο το χρήστη, δίνοντας έτσι τη δυνατότητα στο πόρο νά εξακριβώσει ότι πράγματι είναι μέλη του εικονικού οργανισμού.

3.7 ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι απαιτήσεις ασφάλειας είναι υψίστης σημασίας για το σχεδιασμό υπολογιστικών πλεγμάτων.
Στο κεφάλαιο αυτό , καταγράψαμε τις απαιτήσεις και τις προκλήσεις ασφάλειας στα συστήματα Grid, και την μορφή που μπορεί να έχει η πολιτική ασφάλειας.
Επίσης καταγράψαμε την αρχιτεκτονική ασφάλειας OGSA , τις βασικές υπηρεσίες της, ενώ καταγράψαμε τους βασικούς μηχανισμούς αυθεντικοποίησης και εξουσιοδότησης.
Τέλος καταγράψαμε θέματα που σχετίζονται με την ασφάλεια εικονικών οργανισμών , καθώς και με την πολιτική ασφάλειάς τους, κάτι πολύ σημαντικό αν αναλογιστεί κανείς τον αριθμό των συμμετεχόντων σε πολύ μεγάλα υπολογιστικά πλέγματα.

Συμπερασματικά, η επαρκής αντιμετώπιση των παραπάνω απαιτήσεων κρίνεται απολύτως αναγκαία καθώς σε διαφορετική περίπτωση «κινδυνεύει» η ακεραιότητα και η εμπιστευτικότητα των δεδομένων που ανταλλάσσονται μέσα στο πλέγμα.
Προτού λοιπόν να υλοποιηθεί ένα υπολογιστικό πλέγμα, καλό (και απαραίτητο) είναι ο μηχανικός να μελετήσει προσεκτικά όλες τις πτυχές ασφάλειας και τις απαιτήσεις του πλέγματος που θέλει να υλοποιήσει.

ΜΕΡΟΣ 2: ΠΡΟΤΥΠΑ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ GRID SECURITY

Κεφάλαιο 4: Grid Security Infrastructure (GSI)

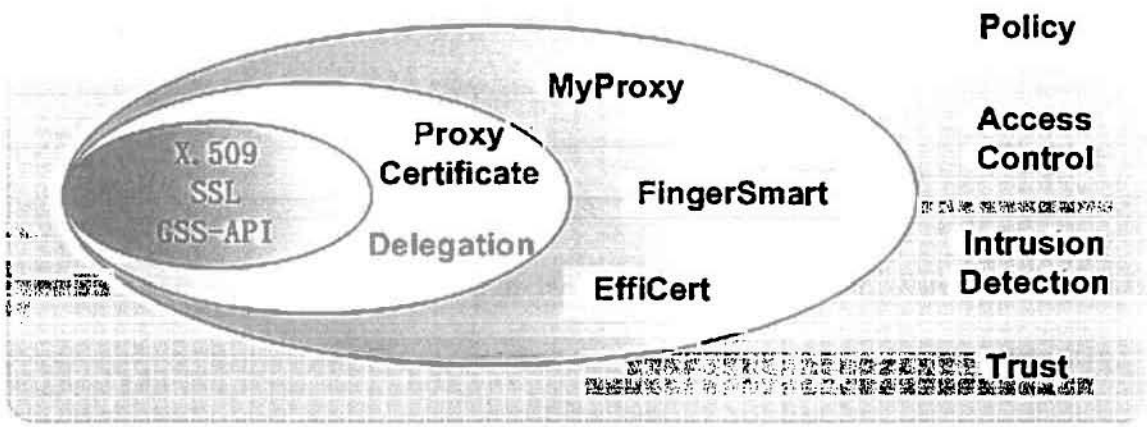
Κεφάλαιο 5: Globus Toolkit- Υλοποιήσεις ασφάλειας σε γνωστά Grid Projects

ΚΕΦΑΛΑΙΟ 4: ΥΠΟΔΟΜΗ ΑΣΦΑΛΕΙΑΣ ΠΛΕΓΜΑΤΟΣ (Grid Security Infrastructure-GSI)

Περίληψη

Το κεφάλαιο αυτό αποτελεί την εισαγωγή στο δεύτερο μέρος της διπλωματικής εργασίας στο οποίο μελετούνται πρότυπα και τεχνολογίες Grid Security, και ειδικότερα το θέμα μελέτης είναι υποδομή ασφάλειας πλέγματος GSI. (Grid Security Infrastructure). Πρόκειται για ένα σύνολο εργαλείων και τεχνολογιών πάνω στα οποία βασίζονται οι επιστήμονες προκειμένου να κτίσουν με ασφάλεια ένα υπολογιστικό πλέγμα. Παραθέτουμε σε αυτό το κεφάλαιο, τις γενικές απαιτήσεις GSI, τα χαρακτηριστικά του, τα δομικά του συστατικά . Επίσης αναλύουμε ένα καινούργιο είδος πιστοποιητικών, τα πιστοποιητικά πληρεξουσιότητας (proxy certificates) καθώς και ένα σύστημα άμεσης αποθήκευσής και επεξεργασίας τους, το MyProxy. Το παρών κεφάλαιο κλείνει με περιγραφή γενικών αρχών ασφάλειας όσο αφορά την γενικότερη υποδομή του πλέγματος.

4.1 ΕΙΣΑΓΩΓΗ



Στην ενότητα αυτή, πρόκειται να μελετήσουμε κάποιες βασικές τεχνολογίες και πρότυπα grid security που χρησιμοποιούνται από διάφορα τεχνολογικά εργαλεία προκειμένου να εισάγουν ασφάλεια σε πλέγματα υπολογιστικής (Grid Computing). Υπάρχουν βασικές απαιτήσεις για το σχεδιασμό ενός ασφαλούς πλέγματος, και για το λόγο αυτό έχουν αναπτυχθεί διάφορα εργαλεία και τεχνολογίες ασφάλειας. Ένα τέτοιο σύνολο τεχνολογιών ασφάλειας που χρησιμοποιείται σε ένα γνωστό εργαλείο (Globus) είναι το GSI (Grid Security Infrastructure). [32]

Οι βασικές απαιτήσεις ασφάλειας σε οποιοδήποτε πληροφοριακό–υπολογιστικό ή δικτυακό σύστημα, είναι οι εξής [32]:

- **Αυθεντικοποίηση:** Διαδικασία κατά την οποία εξακριβώνεται η εγκυρότητα της ταυτότητας ενός προσώπου (ότι πράγματι είναι αυτός που λέει). Η αυθεντικοποίηση δεν περιορίζεται μόνο σε φυσικά πρόσωπα, αλλά και σε άλλες οντότητες όπως εφαρμογές και υπηρεσίες.

- **Εξουσιοδότηση:** Διαδικασία διαβεβαίωσης ότι κάθε χρήστης ή υπολογιστής που χρησιμοποιεί μια υπηρεσία, επιτρέπεται να τη χρησιμοποιεί .

- **Ακεραιότητα δεδομένων :** Χαρακτηριστικό της ασφάλειας, που εγγυάται ότι τα δεδομένα δεν αλλάζουν ούτε καταστρέφονται κατά την μεταφορά ή αποθήκευσή τους κατά παράνομο τρόπο.

- **Εμπιστευτικότητα:** Χαρακτηριστικό που εξασφαλίζει ότι ευαίσθητες πληροφορίες δεν θα γίνονται γνωστές σε τρίτους.

- **Διαχείριση κλειδιών:** Διαδικασία κατά την οποία παράγονται, διανέμονται και αποθηκεύονται με ασφάλεια τα κλειδιά κρυπτογράφησης – αυθεντικοποίησης.

4.1.1 Ορισμός

Ένας κατάλληλος ορισμός για το GSI , σύμφωνα με το [33] είναι ο ακόλουθος :

«Η υποδομή ασφάλειας πλέγματος (GSI) είναι ένα σύνολο από εργαλεία, βιβλιοθήκες και πρωτόκολλα που χρησιμοποιούνται στο Globus, προκειμένου να επιτρέπουν στους χρήστες και στις εφαρμογές την ασφαλή πρόσβασή τους σε πόρους του υπολογιστικού πλέγματος (Grid Computing)»

Οι βασικοί στόχοι του GSI είναι να παρέχει καθολική πιστοποίηση (θα μελετηθεί αργότερα) σε πολλαπλά συστήματα πλέγματος και εφαρμογές, καθώς και να προσφέρει ασφαλείς μηχανισμούς που θα εφαρμόζονται μεταξύ διαφορετικών οργανισμών χωρίς την ύπαρξη μιας κεντρικής αρχής διαχείρισης. [24]

4.2 ΑΠΑΙΤΗΣΕΙΣ GSI

Η υποδομή ασφάλειας πλέγματος (GSI) , υλοποιήθηκε σαν συστατικό μέρος του Globus Toolkit, παρέχοντας μηχανισμούς ασφάλειας. Το GSI ακολουθεί το γενικό πρότυπο το GSS-API, το οποίο είναι πρωτόκολλο IETF για την προσθήκη μηχανισμών αυθεντικοποίησης, ανάθεσης εξουσίας, ακεραιότητας και εμπιστευτικότητας μηνυμάτων [31]. Η υλοποίησή του GSI χρησιμοποιεί ψηφιακά πιστοποιητικά X.509 και βιβλιοθήκες OpenSSL.
Με βάση λοιπόν το [30] οι βασικές απαιτήσεις στην υποδομή GSI είναι οι εξής:

- Κάθε οντότητα ή αντικείμενο που έχει πρόσβαση σε πόρους πλέγματος (χρήστη, συσκευή, πόρο, διεργασία, εφαρμογή κτλ) πρέπει να έχει μοναδική ταυτότητα. Αυτή η ταυτότητα μπορεί να αναπαρίσταται μέσω της χρήσης πιστοποιητικών . Αυτά τα πιστοποιητικά εκδίδονται από την αρχή πιστοποίησης (CA). Το Globus Toolkit χρησιμοποιεί X.509v3 πιστοποιητικά.

- Η ταυτότητα ενός αντικειμένου πρέπει να πιστοποιείται ή να αυθεντικοποιείται. Αυτή η διαδικασία παρέχεται από το πρωτόκολλο αυθεντικοποίησης TLS (στην ουσία μια εξέλιξη στο SSLv3). Η πληροφορία που παρέχει την πιστοποίηση και εγγυάται για την ταυτότητα του χρήστη, είναι στην ουσία η εμπιστοσύνη που εμπνέει η αρχή πιστοποίησης και η πολιτική υπογραφής της.

- Πρέπει να επιτρέπεται σε ένα χρήστη να τρέχει διεργασίες σε απομακρυσμένους πόρους οι οποίοι ανήκουν στο πλέγμα και οι οποίοι έχουν δώσει το δικαίωμα πρόσβασης στο χρήστη. Η οντότητα που δρα εκ μέρους του χρήστη σε απομακρυσμένο πόρο καλείται **πληρεξούσιος χρήστη** (*user proxy*). Το Globus παράγει ένα proxy με ένα καινούργιο πιστοποιητικό που είναι έγκυρο για περιορισμένο χρονικό διάστημα, και υπογράφεται από το πιστοποιητικό του χρήστη.

- Η απομακρυσμένη συσκευή μπορεί να εξακριβώσει το πιστοποιητικό πληρεξουσιότητας (*proxy certificate*) από την υπογραφή του χρήστη, η οποία με την σειρά της εξακριβώνεται από την αρχή πιστοποίησης CA που εμπιστεύεται η απομακρυσμένη συσκευή. Με αυτό τον τρόπο η απομακρυσμένη συσκευή αυθεντικοποιεί τον χρήστη , ο οποίος είναι στην ουσία πίσω από το proxy certificate.

- Σε ένα πλέγμα, πολλές διεργασίες μπορούν να δημιουργηθούν για τους υπολογισμούς, και οι οποίες είναι πιθανό να απαιτούν πρόσβαση σε απομακρυσμένους πόρους. Για αυτές τις διεργασίες, που ανήκουν ουσιαστικά στο χρήστη, δημιουργούνται μια ομάδα πιστοποιητικών πληρεξουσιότητας (proxy certificates) που καθιστούν εύκολη την αυθεντικοποίησή τους στους πόρους.

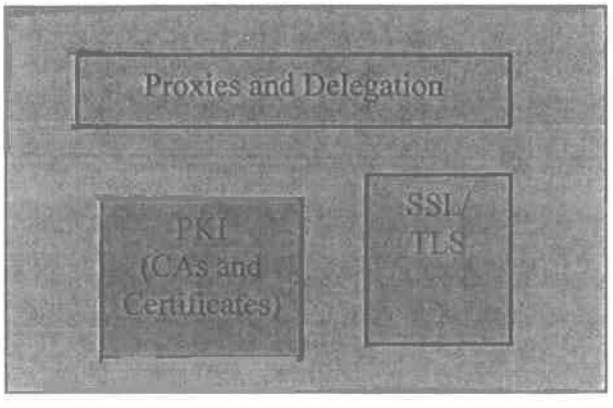
- Κάθε πόρος είναι σε θέση να επιτρέψει ή όχι την πρόσβαση σε αυτόν (εξουσιοδότηση) εφόσον μπορεί να δεχθεί ανάλογο αίτημα που θα βασίζεται σε λίστες ελέγχου πρόσβασης (Access Control Lists-ACL).

- Έπειτα από την αυθεντικοποίηση, το τελευταίο βήμα για την εξουσιοδοτημένη χρήση , είναι η αντιστοίχηση του παγκόσμιου προσδιοριστή ταυτότητας (global identifier) σε ένα τοπικό όνομα. Το παγκόσμιο όνομα βασίζεται στο subject-όνομα του proxy certificate στη μορφή του αναγνωριστικού ονόματος X.500 (Distinguished Name-DN). Οι πόροι του πλέγματος έχουν δημόσιους πίνακες πλέγματος (gridmaps) που περιέχουν τις αντιστοιχήσεις μεταξύ DNs και τοπικών ονομασιών. Αυτή η μέθοδος διασφαλίζει ότι ο αιτών θα πάρει όλα τα σχετικά δικαιώματα χρήσης.

4.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ GSI

Με τον όρο 'χαρακτηριστικά GSI' εννοούμε όλες εκείνες τις υπηρεσίες και οι ιδιότητες των συστατικών μερών του που αυξάνουν το επίπεδο ασφάλειας στο πλέγμα. Τέτοια μπορούν να θεωρηθούν η αυθεντικοποίηση (απλή και αμοιβαία), καθολική πιστοποίηση, ασφαλείς επικοινωνίες μέσω SSL, χρήση πιστοποιητικών πληρεξουσιότητας κτλ.

Η υποδομή ασφάλειας πλέγματος (GSI) αποτελείται από κάποια θεμελιώδη συστατικά μέρη όπως δείχνει και η παρακάτω εικόνα:



GSI

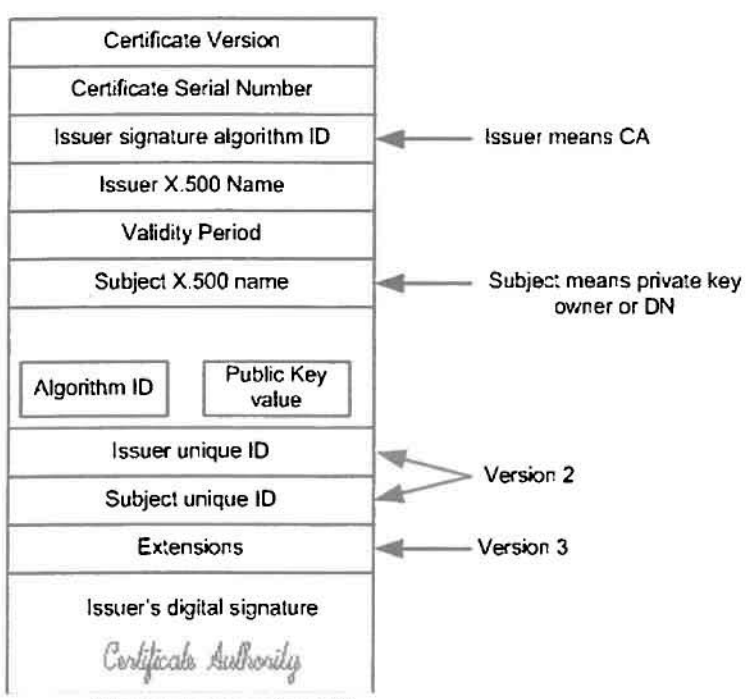
Στην ουσία τα συστατικά του GSI είναι τα εξής:

4.3.1 Υποδομή δημοσίου κλειδιού (PKI)

Η υποδομή δημοσίου κλειδιού, παρέχει συγκεκριμένους μηχανισμούς που επιτρέπουν σε χρήστες και οντότητες να αυθεντικοποιούνται μέσω **ψηφιακών πιστοποιητικών (X.509)** και **αρχών πιστοποίησης (Certificate authorities).**
Τα **ψηφιακά πιστοποιητικά**, χρησιμοποιούνται από το GSI κυρίως για αυθεντικοποίηση, και βασίζονται σε δημόσια κλειδιά X.509 αλλά και στο SSL. Αυτά τα πιστοποιητικά, αναθέτουν σε οντότητες του πλέγματος, σαφείς ονομασίες που υπογράφονται από την αρχή πιστοποίησης (CA). Η μορφή του πιστοποιητικού ουσιαστικά αποτελείται από :

- Αριθμός και έκδοση πιστοποιητικού
- Όνομα και ID του αντικειμένου και του εκδότη
- Δημόσιο κλειδί του αντικειμένου
- Περίοδος ισχύος του πιστοποιητικού
- Επεκτάσεις του πιστοποιητικού
- Προσδιορισμός του αλγορίθμου υπογραφής.
- Ψηφιακή υπογραφή της αρχής πιστοποίησης CA

Στην ουσία, τα ψηφιακά πιστοποιητικά είναι ψηφιακά έγγραφα που συσχετίζουν ένα πόρο του πλέγματος (γενικά μια οντότητα) με το δικό του συγκεκριμένο δημόσιο κλειδί , ενώ η CA πιστοποιεί ότι το περιεχόμενο δημόσιο κλειδί ανήκει στην οντότητα που αναφέρεται στο πιστοποιητικό [32].
Στην παρακάτω εικόνα δίνεται μια γραφική άποψη της δομής ενός X.509 πιστοποιητικού



Πιστοποιητικό x.509

Κεντρικό ρόλο στη διανομή και υπογραφή πιστοποιητικών, παίζει η εκάστοτε **αρχή πιστοποίησης (Certificate Authority).**

Μια σωστά υλοποιημένη **αρχή πιστοποίησης** έχει πολλές **αρμοδιότητες** όπως είναι οι παρακάτω [32]:

- Ασφαλής εξακρίβωση της ταυτότητας οντοτήτων που ζητούν πιστοποιητικά
- Έκδοση, ανάκληση και αρχειοθέτηση των πιστοποιητικών με βάση και την πολιτική έκδοσης πιστοποιητικών της συγκεκριμένης αρχής.
- Προστασία του εξυπηρετητή της αρχής πιστοποίησης (CA-server). Και αυτό γιατί το ιδιωτικό κλειδί της CA είναι ένα από τα σημαντικότερα κομμάτια της υποδομής δημοσίου κλειδιού. Σε περίπτωση κλοπής του ή παράνομης χρήσης του, θα υπάρχουν πολύ αρνητικές συνέπειες στην υπολογιστική πλέγματος.
- Διατήρηση ενός χώρου ονομάτων για μοναδικές ονομασίες των πιστοποιημένων χρηστών.
- Διατμηματική πιστοποίηση CA: Πολύ σημαντική αρμοδιότητα που σχετίζεται με την παρουσία δύο εικονικών οργανισμών μέσα σε ένα πλέγμα. Οι δύο λοιπόν VOs έστω ότι θέλουν να επικοινωνήσουν μεταξύ τους. Αυτό όμως απαιτεί ότι και οι δύο αρχές πιστοποίησής τους εμπιστεύονται η μία την άλλη και κατά συνέπεια και τα πιστοποιητικά που εκδίδει κάθε μια στους χρήστες της. Άρα είναι απαραίτητη η εγκαθίδρυση σχέσεων εμπιστοσύνης που θα βοηθήσει στη επικοινωνία διατμηματικών αρχών πιστοποίησης.
  Λύση σε τέτοια προβλήματα μπορεί να δοθεί και μέσω μιας ανεξάρτητης τρίτης έμπιστης πηγής Grid CA που θα υπογράφει τα πιστοποιητικά και των δύο υφιστάμενων CA , αποδεικνύοντας έτσι ότι και οι δύο VOs ανήκουν νόμιμα στο πλέγμα.

Σε ορισμένα μάλιστα περιβάλλοντα PKI, λειτουργεί αρχή καταχώρησης (Registrant Authority-RA) ώστε σε συνδυασμό με την CA να μπορέσουν να φέρουν εις πέρας την αποστολή τους.
Παρακάτω θα μελετήσουμε το ρόλο της κεντρικής αρχής πιστοποίησης του πλέγματος (Grid Certificate Authority).

4.3.2 Αρχή πιστοποίησης Πλέγματος (Grid CA)

Ένας ορισμός, σύμφωνα με το [37] είναι ο ακόλουθος:

«Grid CA, είναι ουσιαστικά μια CA που είναι ανεξάρτητη από οποιοδήποτε μεμονωμένο οργανισμό, και ο σκοπός της οποίας είναι να υπογράφει πιστοποιητικά για ξεχωριστές οντότητες που τους επιτρέπεται να έχουν πρόσβαση σε πόρους του πλέγματος, ή σε διακομιστές ή υπηρεσίες που τρέχουν σε κάποιο άλλο υπολογιστή».

Τυπικά, η Grid CA υπογράφει πιστοποιητικά μόνο για τέτοιου είδους οντότητες και όχι για χρήστες υφιστάμενων CA. Η Grid CA διαφέρει σημαντικά από την αρχή πιστοποίησης ενός τυπικού οργανισμού, η οποία υπογράφει μόνο στα μέλη του οργανισμού, ενώ η Grid CA όπως αναφέραμε και πιο πάνω, σε όσους δικαιούνται πρόσβαση στο πλέγμα.

4.3.3 Απόκτηση ψηφιακού πιστοποιητικού από CA

Η απόκτηση ενός πιστοποιητικού από την αρχή της πιστοποίησης CA, σύμφωνα με το [32] περιλαμβάνει τα παρακάτω βήματα :

1. Ο χρήστης που ζητά πιστοποιητικό, παράγει ένα ζεύγος κλειδιών (ιδιωτικό και το αίτημα πιστοποιητικού που περιλαμβάνει το δημόσιο κλειδί)

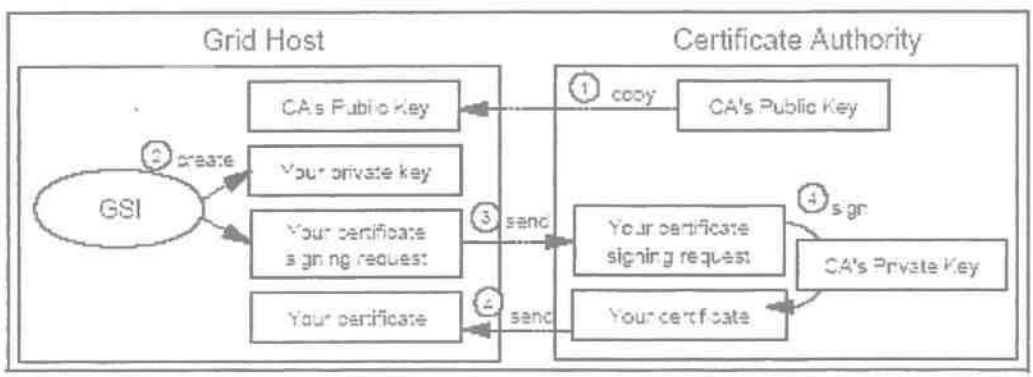
2. Ο χρήστης υπογράφει το δικό του δημόσιο κλειδί, και οποιαδήποτε άλλη πληροφορία απαιτείται από την CA. Υπογράφοντας το πιστοποιητικό, σημαίνει αυτόματα, ότι ο υπογράφων στην πραγματικότητα είναι ο κάτοχος και του ιδιωτικού κλειδιού, καθώς κάνοντας αποκρυπτογράφηση της υπογραφής με το δημόσιο κλειδί προκύπτει το hash δεδομένων το οποίο συγκρίνει με αυτό που γράφει στο πιστοποιητικό.

3. Η υπογεγραμμένη πληροφορία στέλνεται στη CA. Το ιδιωτικό κλειδί παραμένει στον πελάτη και μπορεί να αποθηκευτεί με ασφάλεια , π.χ σε μια έξυπνη κάρτα.

4. Η αρχή πιστοποίησης CA εξακριβώνει ότι ο χρήστης πράγματι κατέχει το ιδιωτικό κλειδί που βασίζεται στο δημόσιο κλειδί του .

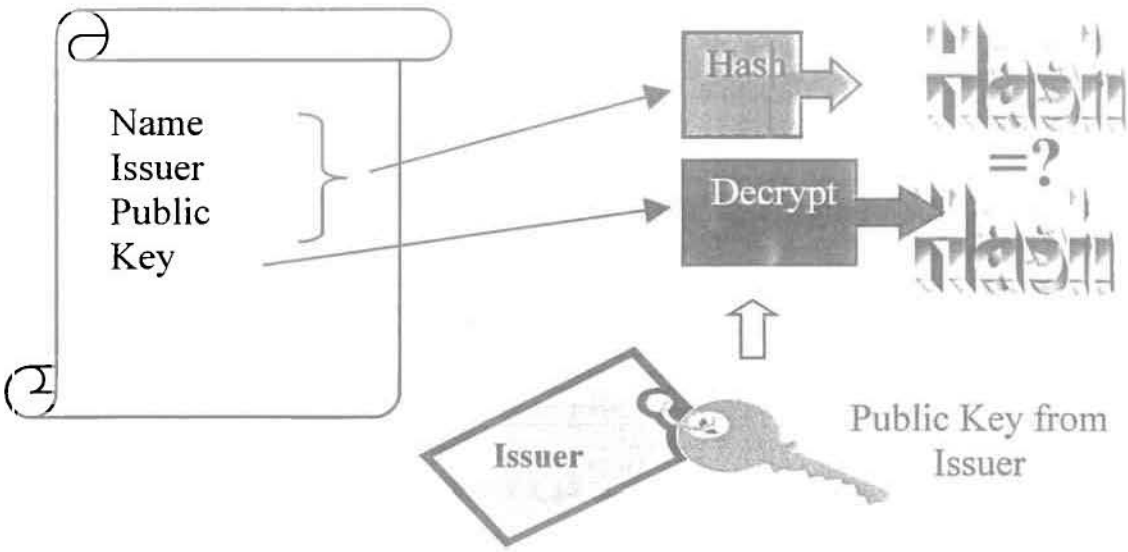
5. Η αρχή πιστοποίησης πρέπει να εξακριβώσει την αληθινή ταυτότητα του χρήστη **ως προς το πλέγμα (ότι πράγματι είναι νόμιμος χρήστης του πλέγματος).** Αυτό μπορεί να συμβεί π.χ με τη χρήση email ή τηλεφώνου σε κάποιο υπεύθυνο στο πλέγμα, ή μέσω κάποιου ψηφιακού πιστοποιητικού που υπογράφεται από την κεντρική Grid CA. Η (τοπική) CA μπορεί να χρησιμοποιήσει για το σκοπό αυτό, το σύστημα εγγραφών από κάποια άλλο οργανισμό, που θα πιστοποιεί ότι ο τάδε χρήστης που ζητά πιστοποιητικό, **πράγματι είναι χρήστης του πλέγματος αυτού του οργανισμού.**

6. Αφού γίνει λοιπόν η εξακρίβωση, η αρχή πιστοποίησης δημιουργεί ένα πιστοποιητικό υπογράφοντας το δημόσιο κλειδί του χρήστη, συσχετίζοντας έτσι το χρήστη με το συγκεκριμένο κλειδί. Το πιστοποιητικό θα προωθηθεί στην αρχή καταχώρησης RA για να το διανέμει στο χρήστη.



Διαδικασία απόκτησης ψηφιακού πιστοποιητικού από CA

Η συνολική διαδικασία για την εγκαθίδρυση ασφαλούς επικοινωνίας και απόκτησης πιστοποιητικού σε πλέγμα φαίνεται στην παραπάνω εικόνα που παρατίθεται στο [32]



Διαδικασία εξακρίβωσης κατοχής ιδιωτικού κλειδιού μέσω υπογραφής-βήμα 4

Όταν ολοκληρωθεί η διαδικασία, και ο χρήστης παραλάβει το υπογεγραμμένο του ψηφιακό πιστοποιητικό, στον υπολογιστή του θα υπάρχουν 3 σημαντικά αρχεία

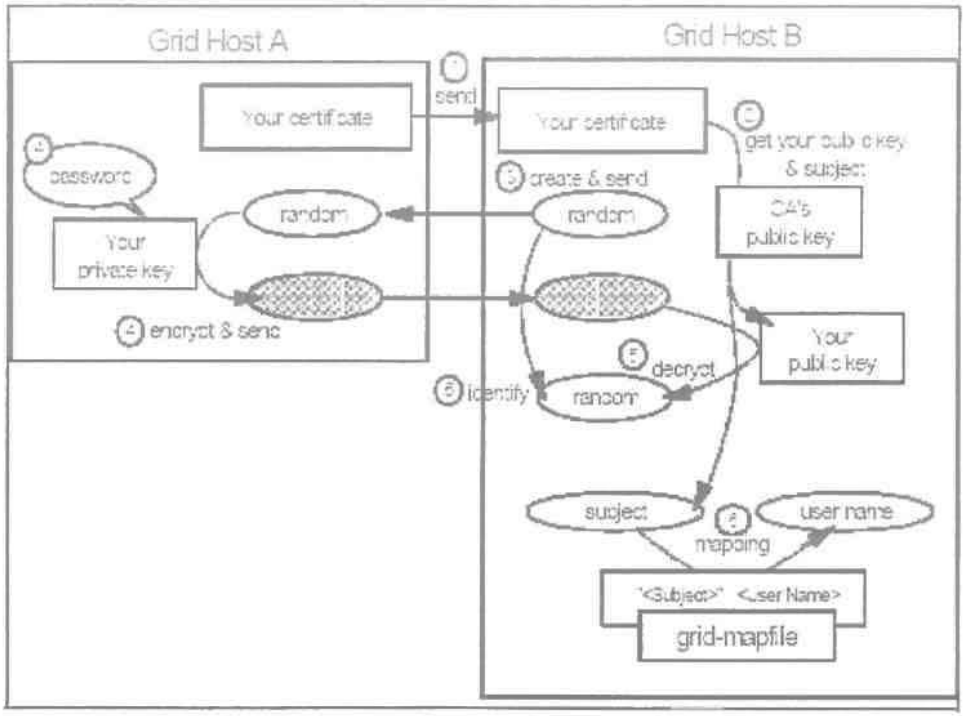
1. Το δημόσιο κλειδί της αρχής πιστοποίησης
2. Το ιδιωτικό κλειδί του ίδιου του χρήστη
3. Το ψηφιακό πιστοποιητικό του χρήστη.

Προκειμένου να υπάρχει ασφαλής αυθεντικοποίηση και επικοινωνία δεν θα πρέπει οι άλλοι να έχουν πρόσβαση στο ιδιωτικό κλειδί. Για αυτό συχνά χρησιμοποιείται μια μυστική φράση-pass phrase την οποία ξέρει μόνο ο κάτοχος, και την οποία χρησιμοποιεί μαζί με το ψηφιακό πιστοποιητικό. Και αυτό ώστε να αποτραπεί η πιθανότητα κάποιος να κλέψει το ψηφιακό πιστοποιητικό και να έχει έτσι πρόσβαση σε πόρους του πλέγματος.

Επιπροσθέτως πρέπει να τονιστεί ότι υπολογιστές του πλέγματος που ανήκουν σε διαφορετικά domains ή VOs , χρειάζεται να αλληλοεμπιστεύονται τα πιστοποιητικά τους είτε μέσω έμπιστων σχέσεων που θα εγκαθιδρύονται μεταξύ τους ή ακόμα και μέσω μιας τρίτης έμπιστής CA που θα είναι ανεξάρτητη από τις επιμέρους CA.

4.3.4 Αυθεντικοποίηση και εξουσιοδότηση

Ας υποθέσουμε ότι χρειάζεται να επικοινωνήσουμε με μια εφαρμογή πλέγματος σε άλλο υπολογιστή, που ανήκει στο πλέγμα , και θέλουμε να διασφαλίσουμε ότι τα δεδομένα που μας στέλνονται είναι πράγματι από εκείνον. Όμως και ο άλλος υπολογιστής πρέπει να μας εμπιστευτεί , ότι πράγματι είμαστε νόμιμοι χρήστες του πλέγματος. Σε μια τέτοια περίπτωση πρέπει να εφαρμοστεί η παρακάτω διαδικασία αυθεντικοποίησης στο GSI [32]:



Διαδικασία αυθεντικοποίησης ανάμεσα σε δύο Grid clients

1. Στέλνουμε (σαν host A) το πιστοποιητικό μας στον άλλο client (host B) στον οποίο θα γίνει η αυθεντικοποίησή μας.

2. Ο Host B παίρνει το δημόσιο κλειδί και το θέμα (subject) του πιστοποιητικού μέσω του δημοσίου κλειδιού CA

3. Ο Host B δημιουργεί ένα τυχαίο αριθμό και μας τον στέλνει.

4. Εμείς αφού τον παραλάβουμε, τον κρυπτογραφούμε με το ιδιωτικό μας κλειδί και το στέλνουμε πίσω στον B.

5. Ο B τον αποκρυπτογραφεί με το δημόσιό μας κλειδί και πιστοποιεί ότι πράγματι εμείς κατέχουμε το συγκεκριμένο ζεύγος κλειδιών (private-public) . Ο B αυθεντικοποιεί το πιστοποιητικό , γιατί μόνο εμείς μπορούμε να το κρυπτογραφήσουμε με το ιδιωτικό μας κλειδί.

6. ***Εξουσιοδότηση***: Έπειτα από την αυθεντικοποίηση ακολουθεί η διαδικασία αντιστοίχησης (mapping) της παγκόσμιας ονομασίας μας (global name) που φαίνεται στο subject του πιστοποιητικού, σε ένα τοπικό όνομα, μέσω gridmap file. Το subject είναι στην μορφή DN (distinguished name) περίπου κάπως έτσι "O=Grid/O=Globus/OU=grid.inf.uth.gr/CN=npapadop", και στην ουσία είναι το όνομα που χρησιμοποιείται από LDAP (εξυπηρετητές καταλόγου) για να καθορίζουν τις ονομασίας οντοτήτων μέσα στο πλέγμα. Έτσι , εμείς έχοντας πλέον ονομασία DN , είμαστε αυθεντικοποιημένοι και εξουσιοδοτημένοι από το host B να ενεργήσουμε σαν τοπικός χρήστης στο host B.

Σε περιβάλλοντα πλέγματος, κάποιες φορές ο υπολογιστής μας θα είναι client και κάποιες server, κυρίως σε περιπτώσεις όπου υπάρχει διαμοίραση πόρων. Για αυτό πρέπει να υπάρχει αμοιβαία αυθεντικοποίηση (mutual authentication) πάνω από ασφαλή επικοινωνία SSL.

4.4 ΠΛΗΡΕΞΟΥΣΙΑ- ΕΚΧΩΡΗΣΗ ΔΙΚΑΙΩΜΑΤΩΝ (Proxies- Delegation)

Πρόκειται για το δεύτερο θεμελιώδες συστατικό του GSI το οποίο περιλαμβάνει μηχανισμούς ασφάλειας που σχετίζονται με λειτουργίες πληρεξουσιότητας εκ μέρους του χρήστη (user proxy), πιστοποιητικών πληρεξουσιότητας (proxy certificates) , εκχώρηση δικαιωμάτων χρήσης (credential delegation), και καθολικής πιστοποίησης (single sign-on).

Στο προηγούμενο κεφάλαιο και πιο συγκεκριμένα στην ενότητα για την *αρχιτεκτονική ασφάλειας πλέγματος*, είχαμε δώσει τον ορισμό για τον πληρεξούσιο χρήστη και πόρου (user, resource proxy). Στην παρούσα ενότητα, θα μελετήσουμε, πως συμβάλλουν οι μηχανισμοί αυτοί στην εκχώρηση δικαιωμάτων (delegation) και στην καθολική πιστοποίηση στο GSI.
Επίσης θα μελετήσουμε τα πιστοποιητικά πληρεξουσιότητας (Proxy Certificates), καθώς και τη χρησιμότητα και το ρόλο τους μέσα στο GSI.

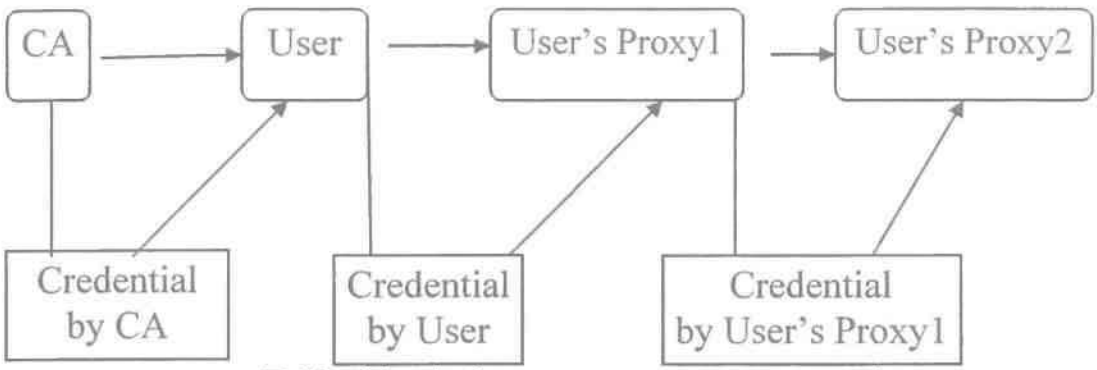
4.4.1 X.509 Πιστοποιητικά πληρεξουσιότητας (Proxy Certificates)

Τα πιστοποιητικά πληρεξουσιότητας (ή καλύτερα **proxy πιστοποιητικά**) βασίζονται στα ψηφιακά πιστοποιητικά X.509 που χρησιμοποιούνται από υποδομές δημοσίου κλειδιού (PKI's). Δημιουργήθηκαν , ώστε να συντελέσουν στην ευκολότερη εκτέλεση μιας διεργασίας σε ένα απομακρυσμένο πόρο, στον οποίο ο χρήστης έχει δικαίωμα πρόσβασης (εξουσιοδοτημένος) , και ο οποίος ανήκει στο πλέγμα.
Οπωσδήποτε η χρήση ψηφιακών πιστοποιητικών X.509 καθώς και οι αρχές πιστοποίησης, παρέχουν μία αρκετά καλή υποδομή αυθεντικοποίησης για τις μόνιμες οντότητες των πλεγμάτων. Ωστόσο υπάρχουν και ορισμένες ανάγκες κάποιων χρηστών που δεν καλύπτονται.

Μια τέτοια ανάγκη είναι για ***καθολική πιστοποίηση***. Διεργασίες , που ανήκουν σε ένα χρήστη , μπορούν να 'τρέχουν' σε πολλά απομακρυσμένα μηχανήματα-πόρους του πλέγματος, κάνοντας χρήση των proxy πιστοποιητικών , κάνοντας έτσι ευκολότερη την αυθεντικοποίησή τους, χωρίς να είναι ανάγκη ο χρήστης να αυθεντικοποιεί τον εαυτό του.
Έτσι δεν απαιτείται η συνεχής παρουσία του, ενώ αποφεύγεται η επαναλαμβανόμενη αυθεντικοποίηση του [30]. Η παροχή αυτής της δυνατότητας-χαρακτηριστικού ονομάζεται **καθολική πιστοποίηση (single sign-on)** και είναι εξαιρετικά χρήσιμη.

Χαρακτηριστικό παράδειγμα είναι και η **δυναμική εκχώρηση δικαιωμάτων (dynamic delegation).** Τα proxy πιστοποιητικά, επιτρέπουν σε μια οντότητα , που κατέχει ένα X.509 δημοσίου κλειδιού πιστοποιητικό , να εκχωρεί κάποια ή όλα τα προνόμια χρήσης που έχει σε μια άλλη οντότητα που μπορεί να μην έχει ως τότε πιστοποιητικό, εξουσιοδοτώντας την για διάφορες ενέργειες, για περιορισμένο συνήθως χρονικό διάστημα.
Αυτή η εκχώρηση μπορεί να γίνει δυναμικά, χωρίς την αρωγή μιας τρίτης έμπιστης πλευράς. Στο [34] αναφέρεται ένα τέτοιο παράδειγμα όπου ένας χρήστης που χρειάζεται να μεταφέρει κάποια σύνολα δεδομένων, για χρήση τους σε υπολογισμούς, θέλει να δώσει κάποια προνόμια –δικαιώματα χρήσης, σε μια υπηρεσία αξιόπιστης μεταφοράς δεδομένων.

Έτσι αυτή η υπηρεσία θα έχει τα απαραίτητα δικαιώματα πρόσβασης του χρήστη, για να πάρει τα δεδομένα και να τα αποθηκεύσει εκ μέρους του.
Αξίζει να τονιστεί ότι αυτή η διαδικασία δημιουργίας proxy πιστοποιητικών μπορεί να έχει αλυσιδωτή μορφή όπως φαίνεται στην ακόλουθη εικόνα, όπου μπορούν να μεσολαβούν πολλά επίπεδα διαμεσολάβησης ανάμεσα στον χρήστη και στον πόρο του πλέγματος.



Πολλαπλά επίπεδα user proxy και πιστοποιητικών

4.4.2 Περιεχόμενα X.509 proxy πιστοποιητικών

Τα proxy πιστοποιητικά, βασίζονται στα X.509 πιστοποιητικά , και έχουν ως στόχο να αντιστοιχήσουν ένα μοναδικό δημόσιο κλειδί σε ένα όνομα-subject όπως κάνουν και τα απλά ψηφιακά πιστοποιητικά. Η χρήση της ίδιας μορφής με τα απλά X.509 πιστοποιητικά, επιτρέπει στα proxy να χρησιμοποιούνται από πρωτόκολλα και βιβλιοθήκες, σαν να πρόκειται για τα απλά πιστοποιητικά. Παρά όμως τις ομοιότητες υπάρχουν και διαφορές οι οποίες σύμφωνα με το [34] είναι οι εξής:

- Αντιθέτως λοιπόν με τα δημοσίου κλειδιού πιστοποιητικά που εκδίδονται από τις CAs , τα proxy πιστοποιητικά υπογράφονται και εκδίδονται από δημοσίου κλειδιού πιστοποιητικά ή από κάποιο πληρεξούσιο χρήστη (user proxy). Αυτή η προσέγγιση, επιτρέπει στα proxy πιστοποιητικά, να δημιουργούνται δυναμικά, χωρίς να απαιτείται η χρονοβόρα διαδικασία ελέγχου και έγκρισης από την αρχή πιστοποίησης CA.

- Το όνομα του θέματος του proxy πιστοποιητικού, ορίζεται από το αντίστοιχο όνομα του εκδότη, προκειμένου να επιτευχθεί μοναδικότητα, ενώ και ο σειριακός αριθμός του πρέπει να είναι μοναδικός. Αυτό επιτυγχάνεται χρησιμοποιώντας ένας μέρος hash του δημοσίου κλειδιού.

- Το δημόσιο κλειδί του proxy πιστοποιητικού, διαφέρει από το δημόσιο κλειδί του εκδότη, καθώς μπορούν να έχουν διαφορετικές ιδιότητες (π.χ μήκος κλειδιού)

- Ένα ακόμα σημαντικό χαρακτηριστικό των proxy πιστοποιητικών είναι το PCI (Proxy Certificate Information). Πρόκειται για πληροφορία, μέσω της οποίας μπορεί ο χρήστης-εκδότης να δηλώσει στο proxy πιστοποιητικό την επιθυμία του να εκχωρούνται τα δικαιώματα του στον 'κομιστή' του proxy πιστοποιητικού, και να βάλει όρια στην δημιουργία περαιτέρω proxy πιστοποιητικών που θα εκδίδονται από τον 'κομιστή'.

Συνοπτικά, μπορούμε να δούμε τις διαφορές μεταξύ των απλών X.509 και των αντίστοιχων proxy πιστοποιητικών , στον παρακάτω πινακα:

Χαρακτηριστικό πιστοποιητικού	X.509 δημοσίου κλειδιού πιστοποιητικό	X.509 proxy πιστοποιητικό
Εκδότης / Υπογράφων	Αρχή πιστοποίησης (CA)	Ένα δημοσίου κλειδιού πιστοποιητικό ή άλλο proxy πιστοποιητικό
Όνομα	Οποιοδήποτε , με βάση την πολιτική του εκδότη (CA)	Μοναδικό, που καθορίζεται από την ονομασία του εκδότη
Εκχώρηση από τον εκδότη	Όχι	Λαμβάνει υπόψη ορισμένες πολιτικές εκχώρησης
Ζεύγος κλειδιών	Χρήση μοναδικού ζεύγους κλειδιών	Χρήση μοναδικού ζεύγους κλειδιών

Σύγκριση μεταξύ X.509 δημοσίου κλειδιού πιστοποιητικών και των αντίστοιχων proxy

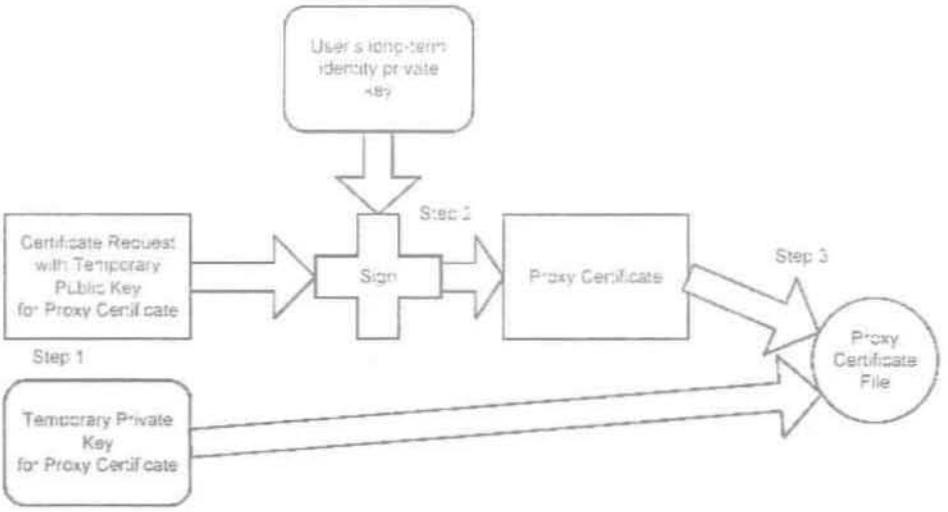
Τα πιστοποιητικά πληρεξουσιότητας συμβάλλουν στην εφαρμογή δύο πολύ σπουδαίων για το πλέγμα μηχανισμών. Αυτό της καθολικής πιστοποίησης και της εκχώρησης δικαιωμάτων χρήσης.
Παρακάτω περιγράφουμε πως χρησιμοποιούνται αυτά τα πιστοποιητικά, για να υλοποιήσουν τους προαναφερθέντες μηχανισμούς.

4.4.3 Καθολική Πιστοποίηση (Single Sign-On)

Το ιδιωτικό κλειδί του χρήστη, προστατεύεται από διάφορες μεθόδους (pass phrase...) που απαιτούν 'χειροκίνητη' αυθεντικοποίηση (manual authentication). Αυτή η διαδικασία, είναι απαραίτητη για την προστασία του κλειδιού. Αλλά από την άλλη μεριά, είναι δύσκολη και η συνεχής πρόσβαση σε αυτό , για τις αναγκαίες αυθεντικοποιήσεις του χρήστη , όποτε αυτές χρειαστούν.

Το proxy πιστοποιητικό επιλαμβάνεται του προβλήματος αυτού, καθιστώντας εφαρμόσιμη την **καθολική πιστοποίηση**. Και αυτό γιατί επιτρέπει στον χρήστη να αυθεντικοποιεί τον εαυτό του χειρονακτικά, μόνο μια φορά κατά τη διαδικασία δημιουργίας του proxy πιστοποιητικού. Έτσι το παραγόμενο πιστοποιητικό, μπορεί να χρησιμοποιηθεί επανειλημμένα για περαιτέρω αναγκαίες αυθεντικοποιήσεις αλλά για περιορισμένο χρονικό διάστημα.

Η διαδικασία δημιουργίας ενός τέτοιου πιστοποιητικού , φαίνεται στην παρακάτω εικόνα:



Δημιουργία proxy πιστοποιητικού για καθολική πιστοποίηση

Τα βήματά της δημιουργίας proxy πιστοποιητικού είναι τα εξής [30]:

1. Δημιουργείται ένα νέο ζεύγος κλειδιών που αποτελείται από ένα δημόσιο και ένα ιδιωτικό , για να χρησιμοποιηθεί στο proxy πιστοποιητικό.

2. Το proxy πιστοποιητικό , υπογράφεται από το ιδιωτικό κλειδί του χρήστη, που σχετίζεται με το δημόσιο κλειδί του αρχικού του πιστοποιητικού. Μέσα στο proxy πιστοποιητικό περιέχεται και το νέο δημόσιο κλειδί που παράχθηκε στο προηγούμενο βήμα.

3. Το proxy πιστοποιητικό και το σχετιζόμενο με αυτό ιδιωτικό κλειδί αποθηκεύονται σε ένα αρχείο το οποίο προστατεύεται από το τοπικό σύστημα αρχείων.

Όταν λήξει η περίοδος ισχύος του proxy πιστοποιητικού , η παραπάνω διαδικασία επαναλαμβάνεται , και ο χρήστης παράγει ένα νέο ζεύγος κλειδιών και ένα νέο proxy πιστοποιητικό.
Ένα πολύ σημαντικό θέμα που ανακύπτει κατά τη δημιουργία proxy πιστοποιητικού είναι το θέμα της απόδοσης ή διαφορετικά, της χρονικής καθυστέρησης κατά τη δημιουργία κλειδιών.
Σύμφωνα με το [34], το μήκος των νέων κλειδιών που παράγονται, παίζει σημαντικό ρόλο στη χρονική καθυστέρηση παραγωγής του proxy πιστοποιητικού. Συγκεκριμένα αναφέρεται ότι στις συγκεκριμένες δοκιμές παράχθηκε ένα ζευγάρι κλειδιών RSA, σε υπολογιστή Pentium 4 2.8 GHz με χρήση της βιβλιοθήκης OpenSSL 0.9.7 . Τα αποτελέσματα του παρακάτω πίνακα δείχνουν του λόγου το αληθές:

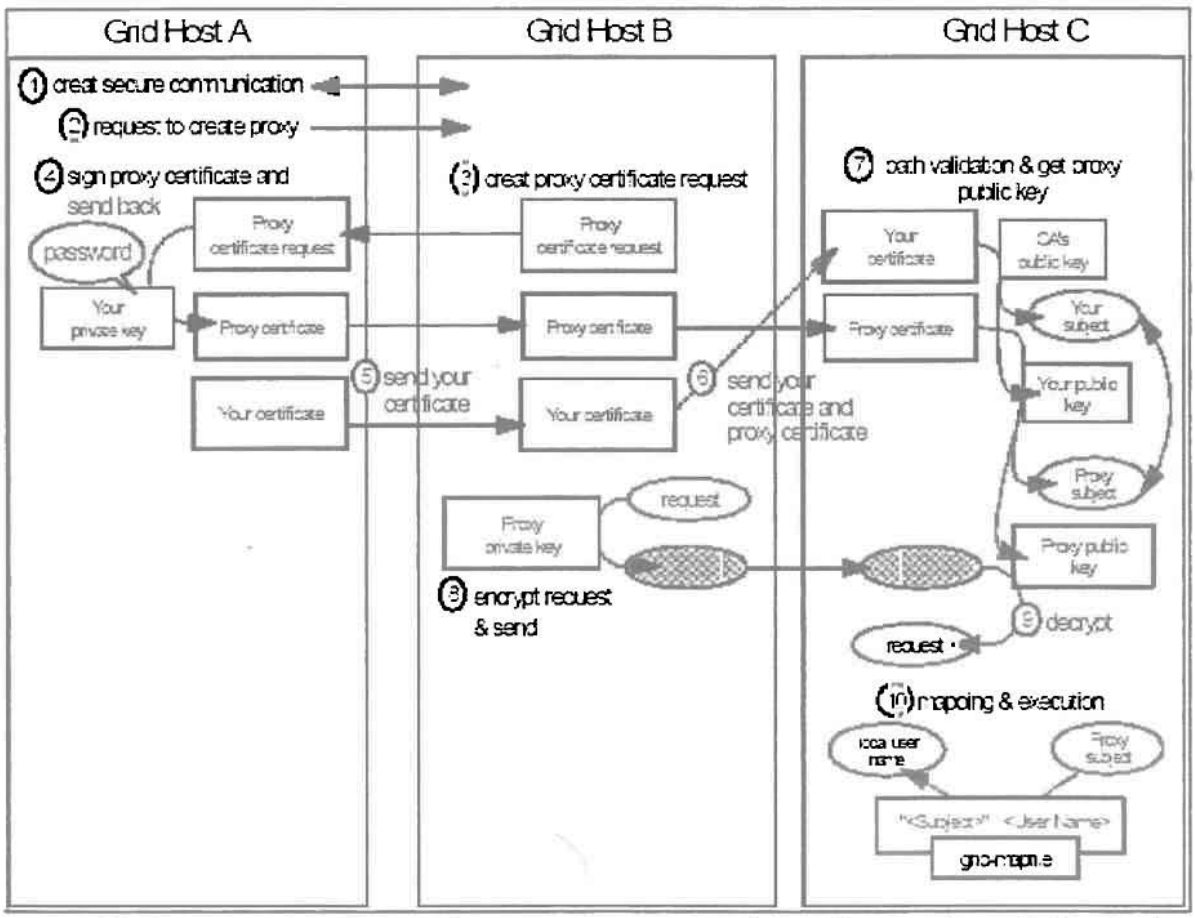
Μήκος(bits)	Χρόνος(sec)
512	0.040
768	0.094
1024	0.176
1536	0.415
2048	1.348

Χρόνοι δημιουργίας RSA κλειδιών

Συνεπώς, η δημιουργία κλειδιών φυσιολογικού μήκους, μπορεί να καταναλώσει σημαντικό μέρος της ισχύς CPU, ιδιαίτερα για hosts που λαμβάνουν εκχωρημένα proxy πιστοποιητικά από πολλαπλούς χρήστες. Από την μία λοιπόν , είναι πρόκληση η χρήση μικρότερου μήκους κλειδιών , από τη στιγμή μάλιστα που ο χρόνος διάρκειάς τους είναι σχετικά μικρός. Ωστόσο πρέπει να θυμόμαστε ότι ενδέχεται να μεταφέρονται πολύ σημαντικά δεδομένα (π.χ ιατρικά) και θα μπορούσε κάποιος ευκολότερα να 'σπάσει' ένα μικρού μήκους κλειδί παρά ένα μεγάλο.

4.4.4 Εκχώρηση δικαιωμάτων χρήσης (Delegation)

Ας υποθέσουμε ότι κατανέμουμε διάφορες εργασίες σε απομακρυσμένους υπολογιστές πλέγματος και αφήνουμε αυτές να ακολουθήσουν την ίδια διαδικασία με τις διεργασίες-παιδιά σε άλλες μηχανές του πλέγματος. Όλα αυτά βέβαια συμβαίνουν σύμφωνα με τη δική μας πολιτική ασφάλειας, προϋποθέτοντας τη δημιουργία πληρεξούσιου χρήστη (user proxy) . Στην ακόλουθη εικόνα φαίνεται ένα πιθανό , σενάριο όπου έστω ότι είμαστε χρήστες στο host A. Μπορούμε να δημιουργήσουμε το πληρεξούσιό μας -proxy στον host B προκειμένου να του εκχωρήσουμε-αναθέσουμε την εξουσία να δρα εκ μέρους μας. Τα βήματα , σύμφωνα με το [32], που περιγράφουν την διαδικασία της δημιουργίας του proxy σε απομακρυσμένη μηχανή πλέγματος καθώς και την υποβολή αίτησης (από το proxy) σε άλλη απομακρυσμένη μηχανή εκ μέρους μας δίνονται παρακάτω:



Χρήση proxy certificates μέσω user proxy και εκχώρηση δικαιωμάτων (delegation)

Δημιουργία πληρεξούσιου χρήστη (User Proxy Creation)

1. Αποκαθίσταται ασφαλής επικοινωνία μεταξύ host A, B

2. Ο host A κάνει αίτημα στο host B για δημιουργία proxy που θα του αναθέσει την εξουσία να δρα εκ μέρους του A.

3. Ο B δημιουργεί το αίτημα για το πιστοποιητικό πληρεξουσιότητας (proxy certificate) και το επιστρέφει στον host A.

4. Ο A, υπογράφει το request για την δημιουργία του proxy certificate μέσω του ιδιωτικού κλειδιού και το στέλνει ξανά στο B.

5. Ο A στέλνει το ψηφιακό πιστοποιητικό του στον host B.

Δράση πληρεξούσιου χρήστη (User Proxy action)

6. Το proxy (user B) στέλνει το ψηφιακό πιστοποιητικό και το proxy πιστοποιητικό στον host C

7. Ο C παίρνει το δημόσιο κλειδί του proxy μέσα από την διαδικασία επικύρωσης μονοπατιού πιστοποίησης (path validation). Ο host C παίρνει το θέμα και το δημόσιο κλειδί από το πιστοποιητικό χρησιμοποιώντας το δημόσιο κλειδί της CA. Έπειτα ο C παίρνει το θέμα του proxy και το δημόσιο του κλειδί από το proxy πιστοποιητικό, μέσω του δημοσίου μας κλειδιού. Το θέμα (subject) στο πιστοποιητικό , είναι στη μορφή DN (distinguished name) περίπου όπως το συγκεκριμένο παράδειγμα "O=Grid/O=Globus/OU=itso.grid.com/CN=your name". Το subject του proxy πιστοποιητικού είναι παρόμοιο με το subject του κατόχου και έχει μορφή "O=Grid/O=Globus/OU=itso.grid.com/CN=your name/CN=proxy". Έτσι προκειμένου να επικυρωθεί η νομιμότητα του proxy certificate , ο host C αρκεί να ελέγξει ότι οι λέξεις που προηγούνται του /CN=proxy είναι ακριβώς οι ίδιες με αυτές του δικού μας subject. Εφόσον επικυρωθεί , το proxy μας που δημιουργήθηκε, είναι αυθεντικοποιημένο από τον host C και είναι πλέον εξουσιοδοτημένο να δρα εκ μέρους μας, καθώς ο χρήστης C είναι πεπεισμένος ότι το user proxy που του έστειλε το proxy certificate, πράγματι αντιπροσωπεύει νόμιμα τον αρχικό χρήστη.

8. Το proxy κρυπτογραφεί ένα μήνυμα με αίτημα , χρησιμοποιώντας το ιδιωτικό κλειδί και το στέλνει στον host C

9. Ο host C αποκρυπτογραφεί αυτό που του έστειλε το proxy χρησιμοποιώντας το δημόσιό του κλειδί και λαμβάνει το αίτημα.

10. Ο host C 'τρέχει' το αίτημα κάτω από την εξουσιοδότηση του τοπικού χρήστη. Το όνομα του χρήστη καθορίζεται από τον πίνακα αντιστοίχησης mapping file μεταξύ των χρηστών πλέγματος και των τοπικών χρηστών.

Η παραπάνω διαδικασία, αναπαριστά την απομακρυσμένη ανάθεση δικαιωμάτων χρήσης-εκπροσώπευσης (remote delegations), όπου ένας χρήστης δημιουργεί ένα πληρεξούσιο σε μια απομακρυσμένη μηχανή.

Μάλιστα. είναι δυνατό διεργασίες που ανήκουν σε ένα χρήστη , αλλά τρέχουν σε πολλούς απομακρυσμένους πόρους, να χρησιμοποιούν τα proxy πιστοποιητικά, ώστε να αυθεντικοποιηθούν χωρίς την ανάγκη για συνεχή αυθεντικοποίηση του ίδιου του χρήστη. [30]

Ωστόσο υπάρχουν προβλήματα ασφάλειας που αφορούν την διαφύλαξη των ιδιωτικών κλειδιών και του χρήστη και των πληρεξούσιών του. Και αυτό γιατί ο τοπικός υπερχρήστης στην απομακρυσμένη μηχανή, όπου δημιουργήθηκε το proxy, μπορεί να έχει πρόσβαση στο ιδιωτικό proxy κλειδί. Προκειμένου να αποφευχθούν όλες οι απειλές πλαστοπροσωπίας, είναι καλό το proxy να εφαρμόζει πιστά κάποιες περιοριστικές πολιτικές , όπως στην περίπτωση του πρωτοκόλλου GRAM [32].

4.5 ΑΣΦΑΛΕΙΣ ΕΠΙΚΟΙΝΩΝΙΕΣ ΜΕΣΩ SSL/TLS

Το άλλο θεμέλιο συστατικό του GSI, αφορά εκείνους τους μηχανισμούς και τεχνολογίες που καθιστούν ασφαλείς τις επικοινωνίες ανάμεσα σε κόμβους (χρήστες, πόρους) του πλέγματος. Εξ'ορισμού η υποκείμενη επικοινωνία βασίζεται στην **αμοιβαία αυθεντικοποίηση** (mutual authentication) των ψηφιακών πιστοποιητικών καθώς και στα πρωτόκολλα SSL/TLS.

Τα ψηφιακά πιστοποιητικά που έχουν εγκατασταθεί σε υπολογιστές του πλέγματος, συμβάλλουν στην αμοιβαία αυθεντικοποίηση μεταξύ των δύο πλευρών. Η διαδικασία αυτή ξεκινά όταν δύο χρήστες του πλέγματος θέλουν να μοιραστούν πόρους. Αντί λοιπόν να χρησιμοποιηθεί ένας χώρος φύλαξης κλειδιών, κάθε χρήστης αυθεντικοποιείται στον άλλο και το αντίθετο. Η όλη διαδικασία, λαμβάνει χώρα κατά την εφαρμογή χειραψίας SSL .

Έστω λοιπόν ότι ένας πελάτης Grid θέλει να επικοινωνήσει με ένα Grid server,. Η διαδικασία χειραψίας ανάμεσά τους αποτελείται από τα εξής βήματα [32]:

1) Ο Grid client επικοινωνεί με τον απομακρυσμένο server για να ξεκινήσουν μια ασφαλή επικοινωνία χρησιμοποιώντας ένα ψηφιακό πιστοποιητικό X.509.

2) Αυτόματα ο client στέλνει στο server την έκδοση SSL, καθώς και τους υποστηριζόμενους αλγορίθμους κρυπτογράφησης.

3) Ο server αποκρίνεται , στέλνοντας στον client το δικό του ψηφιακό πιστοποιητικό, καθώς και αντίστοιχες ρυθμίσεις για την κρυπτογράφηση.

4) Ο χρήστης - client ελέγχει την πληροφορία του ψηφιακού πιστοποιητικού του server και επιβεβαιώνει ότι :
   a) Το πιστοποιητικό του server είναι έγκυρο .
   b) Η αρχή πιστοποίησης που έκδωσε το πιστοποιητικό του χρήστη, είναι πιστοποιημένη από κάποια τρίτη έμπιστη CA.
   c) Το εκδομένο δημόσιο κλειδί της CA, που έχει ο client, πιστοποιεί την ψηφιακή υπογραφή του server
   d) Το όνομα domain που γράφεται στο πιστοποιητικό το server, πράγματι ταιριάζει με το πραγματικό.

5) Εφόσον ο server αυθεντικοποιηθεί επιτυχώς , τότε ο client παράγει ένα μοναδικό κλειδί με το οποίο θα κρυπτογραφείται οτιδήποτε μεταφέρεται ανάμεσα στις δύο πλευρές, κάνοντας χρήση ασύμμετρης κρυπτογράφησης.

6) Ο client κρυπτογραφεί αυτό το κλειδί, με το δημόσιο κλειδί του server και του το στέλνει .

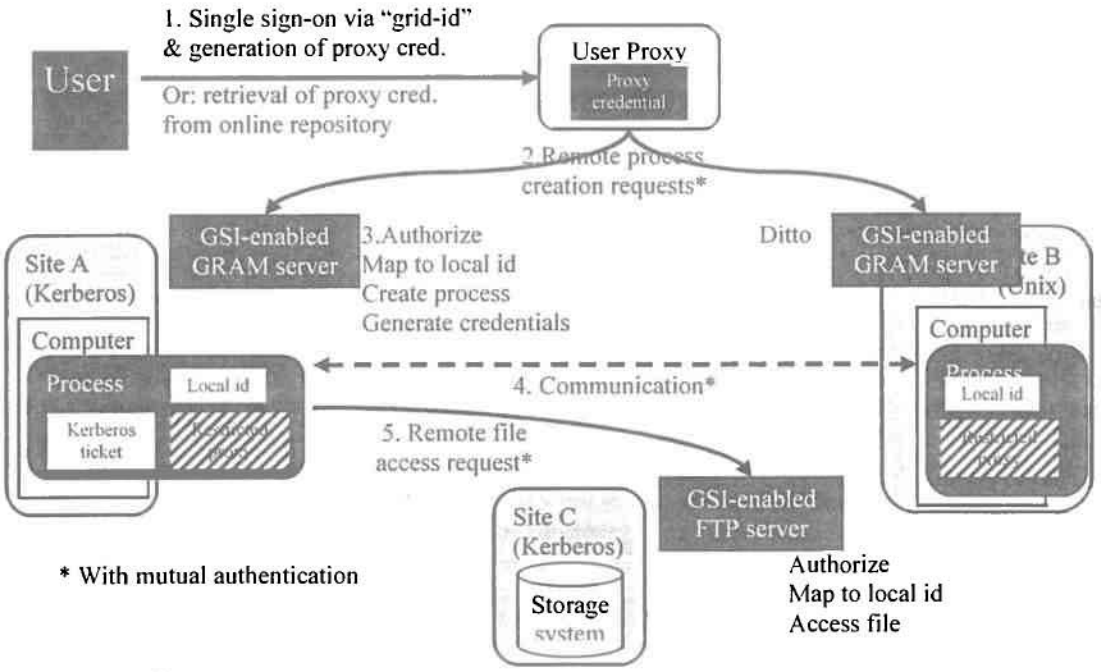
7) Έτσι μόνο ο server με το ιδιωτικό του κλειδί θα μπορεί να το αποκρυπτογραφήσει.

8) Συμφωνούν και οι δύο πλευρές για τη χρήση αυτού του κλειδιού για την κρυπτογράφηση όλων των μηνυμάτων στο μέλλον.

9) Εγκαθίσταται ασφαλής επικοινωνία ανάμεσα σε client και server. Τονίζουμε ότι και ο server μπορεί να κάνει ανάλογο έλεγχο στο πιστοποιητικό του client προκειμένου να τον αυθεντικοποιήσει.

Εφόσον λοιπόν και οι δύο πλευρές έχουν έγκυρα ψηφιακά πιστοποιητικά, η διεργασία της αμοιβαίας αυθεντικοποίησης θα είναι επιτυχημένη. Γίνεται κατανοητό σε αυτή την περίπτωση, πως συνδυάζεται ασύμμετρη και συμμετρική κρυπτογραφία μέσα σε περιβάλλον πλέγματος.

Συνολικά η λειτουργία του GSI φαίνεται παρακάτω [33]:



Λειτουργία GSI

4.6 ΣΥΣΤΗΜΑ ΑΜΕΣΗΣ ΑΠΟΘΗΚΕΥΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΠΛΕΓΜΑΤΟΣ (MyProxy)

Οι πύλες πλέγματος (Grid Portals) , που βασίζονται σε πρότυπες Web τεχνολογίες, χρησιμοποιούνται ολοένα και περισσότερο προκειμένου να παρέχουν φιλικές προς τον χρήστη διεπαφές, για την είσοδό του σε πλέγματα υπολογιστικής.. Ωστόσο έχουν ένα μειονέκτημα όσο αφορά την ασφάλεια, και αυτό είναι ότι δεν βασίζονται σε μηχανισμούς GSI και απαιτείται η ύπαρξη άλλου μηχανισμού που θα επιτρέπει την εκχώρηση –ανάθεση εξουσίας (delegation).
Σύμφωνα λοιπόν με το [40] υπάρχουν ορισμένες απαιτήσεις ασφάλειας που πρέπει να πληρούν τα Grid portals:

- Οι χρήστες πρέπει να μπορούν να χρησιμοποιούν πρότυπους web browsers για να αποκτήσουν πρόσβαση σε Grid portals.

- Οι χρήστες πρέπει να μπορούν να χρησιμοποιούν web browser από τοποθεσίες όπου δεν θα έχουν απευθείας πρόσβαση στα Grid πιστοποιητικά τους.

- Οι χρήστες πρέπει να μπορούν να κάνουν οτιδήποτε δικαιούνται νομίμως, σύμφωνα με την εξουσιοδότηση που παρέχουν τα πιστοποιητικά τους.

Ένα χαρακτηριστικό παράδειγμα είναι εκείνο κατά το οποίο ο χρήστης θέλει να έχει πρόσβαση στο πλέγμα, κάνοντας χρήση ενός web browser σε ένα κιόσκι αεροδρομίου, με την ίδια ευκολία, που θα μπορούσε να το κάνει αυτό από το ιδιωτικό του σύστημα στο γραφείο.

Εκτός από τις παραπάνω απαιτήσεις, υπάρχουν (σύμφωνα με το ίδιο άρθρο) δύο περιορισμοί-αδυναμίες του λογισμικού:

1. Από την στιγμή που τα Grid πιστοποιητικά αποθηκεύονται σε αρχεία, που υποστηρίζονται από συγκεκριμένα συστήματα αρχείων, και εφόσον τα ιδιωτικά κλειδιά πρέπει να είναι μυστικά, ο χρήστης θα πρέπει να έχει ασφαλή πρόσβαση στο σύστημα αρχείων, για να χρησιμοποιήσει τα πιστοποιητικά του. Αυτό, ουσιαστικά σημαίνει ότι ο χρήστης πρέπει να κάθεται στο δικό του μηχάνημα ή να συνδέεται με ασφαλή τρόπο (Secure shell session). Αυτό εμποδίζει πολλές φορές το χρήστη να έχει πρόσβαση στα πιστοποιητικά του, όταν είναι μακριά από το ιδιωτικό του μηχάνημα. Βέβαια, η έξυπνες κάρτες θα μπορούσαν να ήταν μια λύση, αλλά από τη στιγμή που δεν υπάρχει ευρεία υποστήριξη πάνω σε αυτή την τεχνολογία, αυτομάτως αποκλείονται.

2. Ο δεύτερος περιορισμός είναι ότι δεν υποστηρίζουν όλες οι εφαρμογές του Grid, τους μηχανισμούς GSI, και άρα στερούνται της δυνατότητας χρήσεως της εκχώρησης proxy πιστοποιητικών. Οι πελάτες με τους browsers μπορούν να χρησιμοποιήσουν Grid πιστοποιητικά για αυθεντικοποίηση, αλλά δεν υπάρχει η δυνατότητα του GSI για την εκχώρησή τους (credential delegation).

   Πιο απλά , αυτό σημαίνει ότι , αν και ο χρήστης μπορεί να αυθεντικοποιηθεί στο portal, εντούτοις δεν μπορεί να του εκχωρήσει την εξουσία, ώστε να δρα αυτό εκ μέρους του.

Πιθανή κατοχή των proxy πιστοποιητικών των χρηστών από το ίδιο το portal, θα αύξανε σημαντικά τον κίνδυνο κλοπής ή παράνομης χρήσης τους. Έτσι αναπτύχθηκε από τους συγγραφείς του [40] ένα σύστημα με όνομα MyProxy με στόχο:

- Να επιτρέπει στους χρήστες να έχουν πρόσβαση στα πιστοποιητικά τους από οπουδήποτε αυτοί συνδέονται , ακόμα και από συστήματα χωρίς λογισμικό Grid και χωρίς ασφαλή πρόσβαση στα ιδιωτικά τους κλειδιά.

- Να σβήνει , όσα περισσότερα πιστοποιητικά μπορεί από το portal εκτός βέβαια από αυτά που χρειάζονται, προκειμένου να μειώσει τον κίνδυνο απώλειας ή κλοπής τους, σε περίπτωση που το ίδιο το portal υποκύψει σε επίθεση.

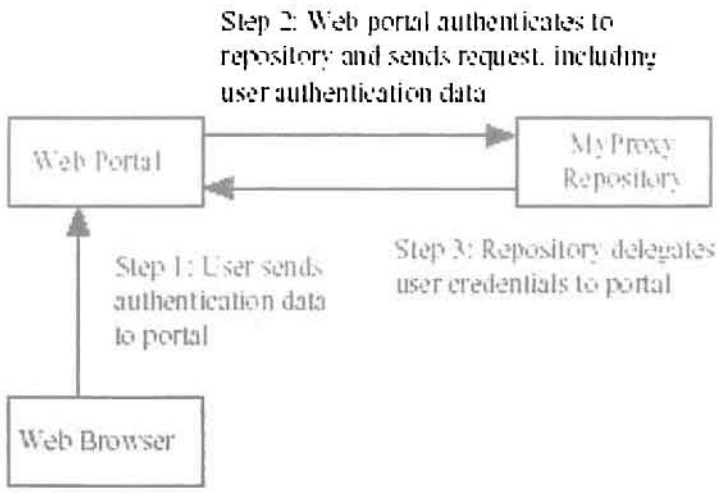
- Να μπορεί να δίνει στο χρήστη όσο περισσότερο έλεγχο των πιστοποιητικών του γίνεται. Ο ρόλος των portals περιορίζεται στη ανάκτηση και μόνο των πιστοποιητικών , εφόσον τους το επιτρέπει ο χρήστης.

Πρόκειται για μια on-line αποθήκη proxy πιστοποιητικών τα οποία ανήκουν σε χρήστες του πλέγματος, με δύο βασικές λειτουργίες αυτή της **εκχώρησης-αποθήκευσης του πιστοποιητικού (credential delegation to repository)** στο σύστημα αποθήκευσης, και αυτή της **ανάκτησής του (credential retrieval from repository)** από αυτό.

Το σύστημα αποθήκευσης MyProxy αποτελείται από ένα server αποθήκευσης και ένα σύνολο εργαλείων για πελάτες που μπορούν να χρησιμοποιηθούν για εκχώρηση και ανάκληση από την αποθήκη. Τυπικά ένας χρήστης ξεκινά μια διεργασία δημιουργίας σύνδεσης με το σύστημα MyProxy. Ο χρήστης στέλνει την πληροφορία με την οποία θα αυθεντικοποιείται (user id, password) και θα μπορεί να ανακτά το πιστοποιητικό του. Αυτή η πληροφορία την διαλέγει ο ίδιος ο χρήστης, και ελέγχεται από το σύστημα MyProxy repository για να διαπιστωθεί αν είναι έγκυρη (π.χ ως προς το μήκος). Επίσης το user id είναι διαφορετικό από το DN που υπάρχει στο πιστοποιητικό του χρήστη, και αυτό γιατί δημιουργείται αργότερα σε σχέση με το X.509 πιστοποιητικό.

Επίσης υπάρχει χρονικός περιορισμός κατά την ανάκτηση των proxy πιστοποιητικών ίσος με την διάρκεια ζωής των πιστοποιητικών. Συνήθως η διάρκεια ζωής των εκχωρημένων proxy πιστοποιητικών είναι μια εβδομάδα. Βέβαια ο χρήστης μπορεί να τον αλλάξει , ενώ το MyProxy repository του δίνει τη δυνατότητα διαγραφής κάποιου πιστοποιητικού μέσω ενός client προγράμματος MyProxy-destroy. [40]

Αφού γίνει η εκχώρηση proxy πιστοποιητικών στο σύστημα αποθήκευσης, ο χρήστης (ή μια υπηρεσία που δρα εκ μέρους του σε άλλη χρονική στιγμή), χρησιμοποιεί το πρόγραμμα MyProxy-get-delegation προκειμένου να επικοινωνήσει με το server και να κάνει αίτηση για ανάκτηση ενός πιστοποιητικού . Ο χρήστης είναι υποχρεωμένος να δώσει τα ίδια στοιχεία αυθεντικοποίησης (id,password) με αυτά που είχε δώσει αρχικά στο repository. Αφού γίνει η αυθεντικοποίηση, επιστρέφεται το πιστοποιητικό στον αιτούντα χρήστη (ή κάποια υπηρεσία πλέγματος). Έτσι αυτό το πιστοποιητικό μπορεί να χρησιμοποιηθεί όπως οποιοδήποτε άλλο proxy και να δράσει εκ μέρους του χρήστη μέσα στο πλέγμα.



Ο χρήστης συνδέεται στο portal, το οποίο με τη σειρά του αλληλεπιδρά με το MyProxy repository

Όσο αφορά τη χρήση του MyProxy Repository με το Grid Portal , αφού γίνει η εκχώρηση του πιστοποιητικού στο σύστημα αποθήκευσης, μετέπειτα ο χρήστης συνδέεται με το Grid portal (με ένα web browser) και δίνει μέσω κατάλληλης φόρμας την πληροφορία αυθεντικοποίησης . Έπειτα το portal συνδέεται με το MyProxy και δίνοντας την πληροφορία του χρήστη, εφόσον γίνει αυθεντικοποίηση του χρήστη (και του portal!), παίρνει το πιστοποιητικό από το MyProxy. Έτσι το portal μπορεί να έχει πρόσβαση στο πλέγμα και στους πόρους του και δρα νόμιμα εκ μέρους του χρήστη.

Κατά τη λειτουργία log out του χρήστη, διαγράφονται από το portal τα εκχωρημένα πιστοποιητικά σε αυτό, ενώ σε περίπτωση που ο χρήστης ξεχάσει να κάνει log off τα πιστοποιητικά θα παραμείνουν στο portal μέχρι λήξει η διάρκεια ισχύος τους. Τότε επαναλαμβάνει την ίδια διαδικασία μέσω του portal προκειμένου να τα επαναποκτήσει.
Όπως γίνεται κατανοητό, ο προφανής κίνδυνος σε ένα τέτοιο σύστημα αποθήκευσης πιστοποιητικών είναι πιθανή κλοπή τους ή παράνομη χρήση τους. Εφόσον ο διακομιστής στον οποίο φιλοξενείται το σύστημα, υποκύψει σε επίθεση, τότε ο επιτιθέμενος, μπορεί να αποκτήσει πρόσβαση σε αυτά και να τα χρησιμοποιήσει. Για να υπάρξει λοιπόν μεγαλύτερη ασφάλεια, σύμφωνα και με το [40] το όλο σύστημα πρέπει να 'τρέχει' σε ασφαλή host (εφάμιλλο του Kerberos).

Επιπροσθέτως, για να μειωθεί ακόμα περισσότερο η πιθανότητα επίθεσης στα πιστοποιητικά, το σύστημα αποθήκευσης, κρυπτογραφεί τα πιστοποιητικά με το password που δίνει ο χρήστης. Έτσι ακόμα και σε περίπτωση κλοπής, ο εισβολέας, θα είναι σχεδόν αδύνατο να βρει το μυστικό κλειδί κρυπτογράφησης, οπότε το μόνο που έχει να κάνει είναι να συνδεθεί μέσω portal με το σύστημα αποθήκευσης και να στείλει κάποια στοιχεία.

Αλλά και σε μια τέτοια περίπτωση υπάρχουν δύο ενδεχόμενα: είτε τα πιστοποιητικά θα έχουν λήξει είτε ο εισβολέας θα έχει ανιχνευτεί μέσω συστημάτων (Intrusion Detections). Τονίζουμε ότι όλες οι ευαίσθητες πληροφορίες μεταξύ των πελατών και του MyProxy Server κρυπτογραφούνται μέσω μηχανισμών ασφάλειας του GSI (π.χ SSL/TLS που θα δούμε παρακάτω). Όμως και μεταξύ του web portal και του client εγκαθιδρύεται ασφαλής επικοινωνία μέσω του πρωτοκόλλου HTTPS, καθιστώντας έτσι πολύ πιο δύσκολη την υποκλοπή των password των χρηστών.

Το συγκεκριμένο σύστημα αποθήκευσης πιστοποιητικών είναι πολύ χρήσιμο για την υπολογιστική πλέγματος , καθώς έχει αποδειχθεί ότι καθιστά ευκολότερη τη χρήση στο πλέγμα και ιδιαίτερα μέσω των portals. Ακόμα, σύμφωνα με το [40] βρίσκει εφαρμογή σε πολλά portals όπως του NCSA,NASA Information Power Grid κτλ.

4.7 ΑΣΦΑΛΕΙΑ ΥΠΟΔΟΜΗΣ ΠΛΕΓΜΑΤΟΣ (Grid Infrastructure Security)

Εκτός από τα διάφορα συστατικά του GSI, εξακολουθούν να υπάρχουν 'κλασσικοί' μηχανισμοί ασφάλειας, που πρέπει να εφαρμοστούν προκειμένου να διασφαλιστεί και η φυσική ασφάλεια ενός πλέγματος. [32]
Αρχικά πρέπει να διασφαλιστεί το φυσικό περιβάλλον ενός συστήματος του πλέγματος. Αν π.χ οι servers είναι σε ανοικτό δωμάτιο, όσο ασφαλείς και να είναι οι εφαρμογές, δεν μπορεί να διασφαλιστεί το πλέγμα. Για αυτό τέτοια συστήματα και ιδιαίτερα αυτά των αρχών πιστοποίησης (CA) πρέπει να κλειδώνονται και η πρόσβαση σε αυτά να επιτρέπεται στο κατάλληλο και μόνο προσωπικό.
Για την ασφάλεια λειτουργικών συστημάτων, πρέπει να λαμβάνονται ορισμένα μέτρα για την πιο εύρυθμη λειτουργία των συστημάτων.
Τέτοια μέτρα αποτελούν:

- Η διαγραφή διεργασιών που δεν είναι αναγκαίες (π.χ διεργασία FTP ή αποστολής email)
- Η χρήση ισχυρών password για τους χρήστες του πλέγματος
- Ενημέρωση του server με όλα τα τελευταία διορθωτικά πακέτα.
- Απαγόρευση πρόσβασης στον φάκελο '/globus'...κτλ

Ένα άλλο πολύ σημαντικό μέτρο προστασίας, είναι η εγκατάσταση συστημάτων firewall στο πλέγμα. Τα firewalls μπορούν να χρησιμοποιηθούν σε δικτυακά περιβάλλοντα προκειμένου να χωρίσουν σε διαφορετικά domains το δίκτυο και να εφαρμόσουν αποτελεσματικότερα κανόνες ασφάλειας και πρόσβασης. Η χρήση του στην υπολογιστική πλέγματος, θα αυξήσει σημαντικά το επίπεδο ασφάλειας σε αυτό.

Τέλος τα συστήματα ανίχνευσης εισβολέων (Intrusion Detection Systems-IDS) συμβάλλουν και αυτά στην αντιμετώπιση σοβαρών κινδύνων εισβολής στο πλέγμα. Σε περίπτωση που ένα IDS ανιχνεύσει κάτι 'περίεργο' στο πλέγμα (αλλαγή σε αρχεία, μεγάλη χρήση CPU, απίθανες ενέργειες από κάποιο χρήστη) μπορεί να στείλει σήμα ειδοποίησης στην κεντρική κονσόλα ώστε να ειδοποιηθούν οι αρμόδιοι της ασφάλειας και να αντιμετωπίσουν τους κινδύνους.

Συμπερασματικά δεν αρκεί μόνο η ασφάλεια του GSI, αλλά είναι απαραίτητος ο συνδυασμός του GSI με την εφαρμογή κλασικών μηχανισμών φυσικής (και όχι μόνο) ασφάλειας, προκειμένου να κτίσουμε ένα ασφαλές πλέγμα υπολογιστικής.

4.8 ΣΥΜΠΕΡΑΣΜΑΤΑ

Αναμφισβήτητα η σχεδίαση και υλοποίηση ενός ασφαλούς υπολογιστικού πλέγματος είναι πολύ σημαντικό. Στο συγκεκριμένο κεφάλαιο μελετήσαμε ένα συστατικό του Globus toolkit, το GSI που φροντίζει για την ασφάλεια του υπολογιστικού πλέγματος.
Πιο συγκεκριμένα μελετήσαμε τις απαιτήσεις και τα χαρακτηριστικά του GSI.
Επίσης αναλύσαμε μια πολύ σημαντική για τα συστήματα Grid, έννοια, αυτή των πιστοποιητικών πληρεξουσιότητας (Proxy Certificates).
Δώσαμε ιδιαίτερη βαρύτητα σε μια πολύ σημαντική λειτουργία του GSI , την καθολική πιστοποίηση (Single Sign-On) και πως αυτή συμβάλλει στην ευελιξία του συστήματος πλέγματος και στην ευκολότερη χρήση από τον ίδιο χρήστη .

Ακόμα, περιγράψαμε τον τρόπο με τον οποίο το GSI καθιστά ασφαλείς τις επικοινωνίες μέσα στο πλέγμα μέσω των πρωτοκόλλων SSL/TLS, ενώ καταγράψαμε και ένα ακόμα χαρακτηριστικό του GSI που αναπτύχθηκε στις τελευταίες εκδόσεις του Globus. Πρόκειται για το σύστημα άμεσης αποθήκευσης ,το MyProxy που καθιστά πιο ευέλικτη τη χρήση των πιστοποιητικών πληρεξουσιότητας από τον χρήστη , ιδιαίτερα όταν αυτός είναι μακριά από το σύστημά του.

Τέλος, κλείνουμε το κεφάλαιο αυτό με μια σύντομη αναφορά σε βασικούς τρόπους με τους οποίους μπορούμε να παρέχουμε φυσική ασφάλεια στο όλο σύστημα. Πρέπει να δοθεί βαρύτητα και στο συγκεκριμένο τομέα, καθώς δεν νοείται ασφαλές πλέγμα χωρίς ασφαλής υποδομή , για τους πόρους , είτε υπολογιστικοί είναι αυτοί είτε αποθηκευτικοί, δικτυακοί κτλ.

Συμπερασματικά, το σύνολο των πρωτοκόλλων , των βιβλιοθηκών και των εργαλείων, που ονομάζονται GSI, παρέχουν λειτουργίες αυθεντικοποίησης, εξουσιοδότησης, και καθολικής πιστοποίησης. Λειτουργίες που οπωσδήποτε μπορούν να κτίσουν ένα περιβάλλον μέσα στο οποίο οι χρήστες ανταλλάσσουν με ασφάλεια δεδομένα αλλά και μπορούν με ασφάλεια να έχουν πρόσβαση στους πόρους που χρειάζονται. Γενικά μπορούμε να πούμε ότι το GSI αποτελεί την καρδιά ενός ασφαλούς υπολογιστικού πλέγματος.

ΚΕΦΑΛΑΙΟ 5: Globus Toolkit- Υλοποιήσεις ασφάλειας σε γνωστά Grid Projects

Περίληψη

Στο κεφάλαιο αυτό μελετάμε το εργαλείο Globus Toolkit. Πρόκειται για ένα σπουδαίο εργαλείο ανάπτυξης υπολογιστικής πλέγματος. Περιγράφουμε ένα τυπικό σενάριο χρήσης του όπως επίσης και τα χαρακτηριστικά του καθώς και το μοντέλο ασφάλειας OGSA που εισάγει. Όσο αφορά στα χαρακτηριστικά του, περιγράφουμε και ένα ακόμα που αναπτύχθηκε στις τελευταίες εκδόσεις του Globus. Πρόκειται για μια υπηρεσία εξουσιοδότησης με όνομα CAS μέσω της οποίας μπορούμε να εξουσιοδοτήσουμε ομάδες χρηστών και όχι κάθε χρήστη ξεχωριστά. Το κεφάλαιο κλείνει με μια σύντομη μελέτη των ***υλοποιήσεων ασφαλών συστημάτων υπολογιστικής πλέγματος (Secure Grid Systems),*** *όπου μελετούμε τις τεχνολογίες, τα εργαλεία και τη μεθοδολογία που εφαρμόστηκαν σε γνωστά project υπολογιστικής πλέγματος.*

5.1 ΕΙΣΑΓΩΓΗ

Μετά από την μελέτη μας πάνω σε θέματα ασφάλειας στην υπολογιστική πλέγματος, θα μελετήσουμε το πιο γνωστό ίσως εργαλείο ανάπτυξης συστημάτων πλέγματος καθώς και μηχανισμών ασφάλειας για αυτά τα συστήματα.
Γενικά ένα σύστημα πλέγματος είναι υπεύθυνο για την αποστολή μιας εργασίας σε μια συγκεκριμένη μηχανή προκειμένου να εκτελεστεί. Στα απλούστερα συστήματα πλέγματος, ο χρήστης μπορεί να διαλέξει μια μηχανή κατάλληλη για την εκτέλεση της εργασίας του κα έπειτα να στείλει σε αυτό το μηχάνημα την εργασία. Σε πιο εξελιγμένα συστήματα grid, υπάρχει μηχανισμός προγραμματισμού εργασιών (job scheduler). Αυτοί οι μηχανισμοί αντιδρούν ανάλογα με την διαθεσιμότητα των πόρων στο πλέγμα και φυσικά ανάλογα με τον φόρτο εργασίας στα διάφορα μηχανήματα του πλέγματος.

Αν δηλαδή ένα σύστημα περιέλθει σε αδράνεια, τότε θα 'αναφέρει' την κατάσταση αδράνειάς του στον κόμβο διαχείρισης του πλέγματος, ο οποίος με τη σειρά του θα του αναθέσει την επόμενη εκκρεμούσα διεργασία, προκειμένου γίνει εκμετάλλευση των ελεύθερων πόρων. Από την άλλη όμως πλευρά, σύμφωνα με το [1] αν ο φόρτος του μηχανήματος αυξηθεί, λόγω τοπικών εργασιών που δεν ανήκουν στο πλέγμα, τότε η διεργασία του πλέγματος (έχοντας μικρή προτεραιότητα σε σχέση με την τοπική) θα διακοπεί ή θα καθυστερήσει να ολοκληρωθεί. Όλες αυτές (και άλλες πολλές) οι λειτουργίες καλύπτονται από διάφορους μηχανισμούς και πρωτόκολλα του Globus Toolkit, προκειμένου να μπορεί να αναπτυχθεί ένα σωστό και εύρυθμο πλέγμα υπολογιστικής.

5.2 ΤΙ ΕΙΝΑΙ ΤΟ GLOBUS TOOLKIT

Σύμφωνα με το [44] το project Globus είναι ουσιαστικά μια πολύ-ιδρυματική (multi-institutional) έρευνα που προσπαθεί να συμβάλλει στην κατασκευή πλεγμάτων υπολογιστικής, παρέχοντας, αξιόπιστη πρόσβαση σε υψηλής απόδοσης υπολογιστικούς πόρους, παρά την γεωγραφική κατανομή τόσο των πόρων όσο και των χρηστών.
Ένας κατάλληλος ορισμός του Globus Toolkit είναι αυτός που δίνεται στο [44] σύμφωνα με τον οποίο:

«Το Globus είναι ένας συνδυασμός βασικών υπηρεσιών και δυνατοτήτων που συμβάλλουν στην κατασκευή πλεγμάτων υπολογιστικής».

Με βάση το ίδιο άρθρο, ο σχεδιασμός του Globus Toolkit έγινε με βάση κάποιες απαιτήσεις-αρχές:

- Το Toolkit πρέπει να συνδυάζει ένα σύνολο συστατικών που αναπτύσσουν στοιχειώδεις υπηρεσίες ασφάλειας, εντοπισμού και διαχείρισης πόρων, επικοινωνίας κτλ.

- Το Toolkit κάνει ένα διαχωρισμό μεταξύ τοπικών υπηρεσιών και των global , οι οποίες στην ουσία είναι και πιο περίπλοκες.

- Οι διεπαφές του Globus καθορίζονται έτσι ώστε να διαχειρίζονται ετερογενή συστήματα.

- Το globus χρησιμοποιεί όποτε αυτό είναι δυνατό, κάποια πρότυπα τόσο για τις διεπαφές του όσο και για τις υλοποιήσεις (CORBA,DCE, DCOM...)

5.2.1 Τυπικό σενάριο χρήσης Globus

Παρακάτω δίνονται τα βασικά βήματα μιας τυπικής χρήσης του Globus από ένα χρήστη πλέγματος [41]:

1. Ο χρήστης έχει μια εργασία που πρέπει να εκτελεστεί απομακρυσμένα σε άλλο host / πόρο του πλέγματος
2. Επικοινωνεί με αμοιβαία αυθεντικοποίηση με ένα συστατικό (Gatekeeper) του Globus και εφόσον αυθεντικοποιηθεί
3. αυτός παράγει ένα διαχειριστή εργασίας (Job Manager) ο οποίος θα φροντίσει να βρει τον κατάλληλο υπολογιστικό πόρο για να εκτελέσει την εργασία του χρήστη και
4. έπειτα με SSL θα επικοινωνήσει μαζί του μεταφέροντάς του τα αποτελέσματα.

5.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ GLOBUS TOOLKIT

Το Globus Toolkit συνδυάζει ένα σύνολο συγκεκριμένων τμημάτων το καθένα από τα οποία επιτελεί συγκεκριμένες λειτουργίες μέσα στο πλέγμα. Αυτά τα τμήματα σύμφωνα με το [42] είναι τα εξής:

- **Εντοπισμός και ανάθεση πόρων (Resource location and allocation):** Αυτό το τμήμα παρέχει τους μηχανισμούς για την έκφραση των απαιτήσεων για πόρους των διάφορων εφαρμογών, για τον εντοπισμό πόρων που ικανοποιούν τις απαιτήσεις των χρηστών, και για την χρήση αυτών των πόρων. Οι μηχανισμοί εντοπισμού πόρων είναι απαραίτητοι γιατί οι εφαρμογές δυσκολεύονται γενικά να εντοπίσουν από μόνες τους την ακριβή θέση των απαιτούμενων πόρων , ιδιαίτερα όταν ο φόρτος εργασίας μεταβάλλεται.
  Η ανάθεση πόρων περιλαμβάνει προγραμματισμό της χρήσης και ανάθεσής τους στις διάφορες διεργασίες που δρουν εκ μέρους του χρήστη.

- **Επικοινωνίες:** Αυτό το τμήμα παρέχει τους βασικούς μηχανισμούς επικοινωνίας, οι οποίοι θα πρέπει να επιτρέπουν την υλοποίηση μεγάλου εύρους μεθόδων επικοινωνίας όπως πέρασμα μηνυμάτων (message passing), remote procedure call, κτλ. Επίσης αυτοί οι μηχανισμοί πρέπει να είναι ενήμεροι της ποιότητας των υπηρεσιών του δικτύου, του bandwidth, της καθυστέρησης κτλ.

- **Υπηρεσία ενοποιημένης πληροφορίας πόρων (Unified resource information service):** Αυτό το κομμάτι του Globus είναι υπεύθυνο για την παροχή μηχανισμού για real time ανάκτηση πληροφορίας σχετικά με την δομή του πλέγματος και την κατάσταση (τρέχων φόρτος των πόρων) του. Θα πρέπει να επιτρέπεται στους χρήστες τόσο να λαμβάνουν όσο και να στέλνουν πληροφορία.

- **Διεπαφή αυθεντικοποίησης (Authentication Interface):** Το συγκεκριμένο τμήμα του Globus παρέχει βασικούς μηχανισμούς αυθεντικοποίησης που μπορούν να χρησιμοποιηθούν για την επιβεβαίωση της εγκυρότητας των χρηστών και των πόρων. Εκτός αυτού, παρέχονται και τα εφόδια και για άλλες υπηρεσίες ασφάλειας όπως εξουσιοδότηση και εμπιστευτικότητα, όπου και αυτές χρειάζονται να γνωρίζουν την ακριβή ταυτότητα των χρηστών του πλέγματος.

- **Δημιουργία διεργασίας (Process creation):** Αυτό το τμήμα ασχολείται κυρίως με την αρχικοποίηση ενός υπολογισμού σε ένα πόρο, από την στιγμή που αυτός εντοπίστηκε και ανατέθηκε σε ένα χρήστη ή διεργασία. Συγκεκριμένα εγκαθιστά τα εκτελέσιμα αρχεία, δημιουργεί το κατάλληλο περιβάλλον εκτέλεσης, εκτελεί το exe , περνά τις μεταβλητές ορίσματα και διαχειρίζεται τον τερματισμό της διεργασίας.

- **Πρόσβαση σε δεδομένα (Data access):** Το τελευταίο σύμφωνα με τη συγκεκριμένη προσέγγιση, κομμάτι του Globus αφορά τη πρόσβαση δεδομένων και είναι υπεύθυνο για την παροχή υψηλής ταχύτητας απομακρυσμένης πρόσβασης σε δεδομένα σε αποθηκευτικούς χώρους και αρχεία. Βέβαια, κάποιοι πόροι δεδομένων, όπως οι κατανεμημένες βάσεις δεδομένων, προσπελαύνονται μέσω κατανεμημένων μηχανισμών(CORBA).

Όλα τα παραπάνω τμήματα, μπορούν θεωρητικά να αποτελέσουν ένα μετα-υπολογιστικό εικονικό σύστημα.

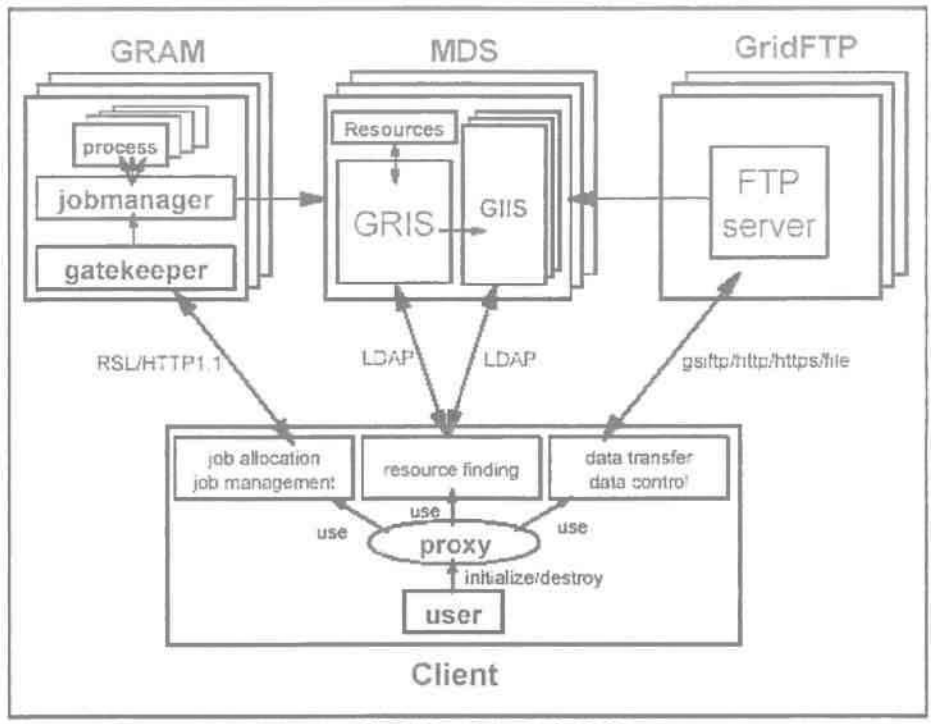
Ωστόσο, στο [32] δίνεται μια διαφορετική προσέγγιση όσο αφορά στα επιμέρους συστατικά του Globus . Σύμφωνα με το συγκεκριμένο άρθρο, το Globus είναι κτισμένο πάνω στο GSI και έχει τρία κύρια συστατικά :

- **Διαχείριση πόρων (resource management):** Υποστηρίζει ανάθεση πόρων, αποστολή εργασιών (submit jobs), διαχείριση κατάστασης εργασιών καθώς και της προόδου τους. Το Globus Toolkit δεν έχει τον δικό του προγραμματιστή εργασιών (job scheduler) για να βρίσκει τους διαθέσιμους πόρους. Αντί αυτού, παρέχει όλα τα απαραίτητα εργαλεία που χρειάζονται για την υλοποίηση τέτοιων μηχανισμών από τους κατασκευαστές πλεγμάτων.

- **Διαχείριση δεδομένων (data management):** Παροχή υποστήριξης για τη μεταφορά αρχείων μεταξύ κόμβων του πλέγματος και για την διαχείριση αυτών των μεταφορών.

- **Υπηρεσίες πληροφόρησης (Information Services):** Παροχή υποστήριξης για συλλογή πληροφορίας του πλέγματος που βασίζεται στο LDAP.

Μπορούμε να έχουμε μια συνολική εικόνα της γενικής δομής του Globus, μέσω της κάτωθι εικόνας :



Δομή Globus Toolkit [32]

Όπως παρατηρούμε, υπάρχουν τρεις βασικές δομές που απαρτίζουν το Globus και είναι το

- **GRAM / GASS**: Πρόκειται για τα επιμέρους συστατικά της διαχείρισης πόρων
- **MDS (GRIS / GIIS)**: Τα δύο επιμέρους συστατικά της υπηρεσίας πληροφόρησης βασίζονται στο πρωτόκολλο LDAP και συνιστούν την λειτουργία που είναι γνωστή με το όνομα MDS (Monitoring and Discovery Service) και έχει να κάνει με τη συλλογή δυναμικής πληροφορίας μέσα στο πλέγμα. Αναλυτικά, θα δούμε αργότερα πως λειτουργεί.
- **GridFTP**: Πρόκειται για το βασικό συστατικό για ασφαλή και υψηλής απόδοσης μεταφορά δεδομένων.

Όλα τα παραπάνω συστατικά του Globus Toolkit είναι 'κτισμένα' πάνω στο GSI. Παρακάτω αναλύουμε κάθε ένα βασικό συστατικό του Globus Toolkit.

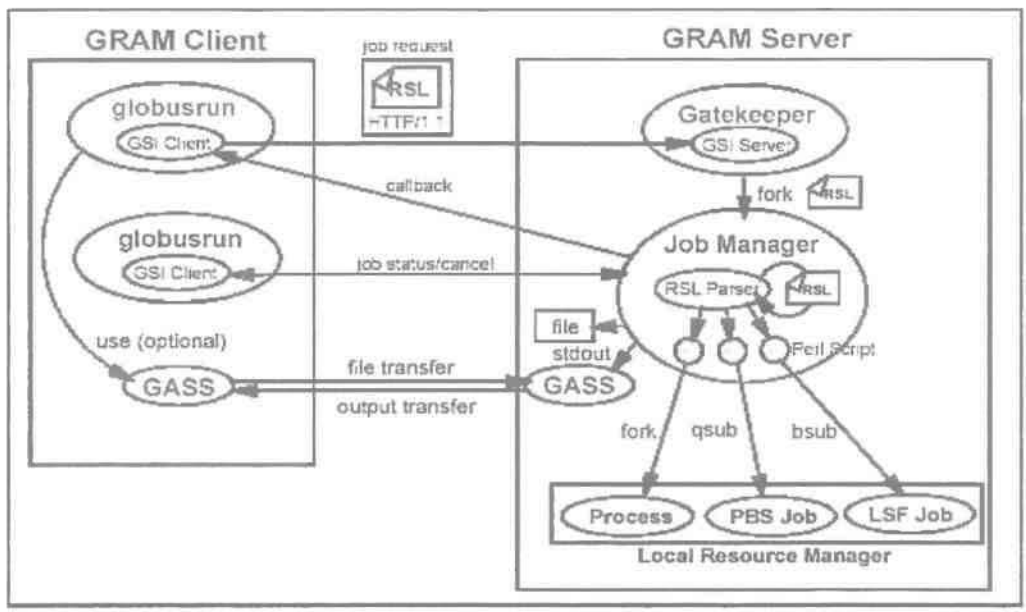
5.3.1 Διαχειριστής ανάθεσης πόρων (Grid resource allocation Manager-GRAM)

Το GRAM είναι ένα κομμάτι του Globus , που παρέχει απομακρυσμένη εκτέλεση εφαρμογών αλλά και διαχείριση της κατάστασης (status) της εκτέλεσης. Όταν υποβάλλεται μια εργασία από τον πελάτη, το αίτημα στέλνεται στον απομακρυσμένο host και η διαχείρισή του γίνεται από μια διεργασία **gatekeeper** που βρίσκεται σε αυτό το μηχάνημα.
Έπειτα ο gatekeeper δημιουργεί ένα διαχειριστή εργασίας (**job manager**) που θα εκτελέσει και θα παρακολουθεί την εργασία.

Όταν η εργασία τελειώσει, ο job manager στέλνει την πληροφορία κατάστασης εργασίας πίσω στον πελάτη και τερματίζει.

Σύμφωνα με το [32] το GRAM , αποτελείται από τα εξής στοιχεία:

- Εντολή globusrun
- Γλώσσα καθορισμού πόρων (Resource Specification Language-RSL)
- Διεργασία gatekeeper
- Job manager
- 'Διχαλωτή' διεργασία (forked process)
- GASS (Global Access to Secondary Storage)
- DUROC (Dynamically-Updated Request Online Co-allocator)



GRAM

Η εντολή **globusrun** υποβάλλει και διαχειρίζεται απομακρυσμένες εργασίες και χρησιμοποιείται σχεδόν από όλα τα εργαλεία GRAM client. Συγκεκριμένα φροντίζει για το αίτημα υποβολής εργασίας σε απομακρυσμένους Η/Υ (μέσω αμοιβαίας αυθεντικοποίησης), και για τη μεταφορά εκτελέσιμων αρχείων .
Η γλώσσα **RSL** χρησιμοποιείται από πελάτες για να υποβάλλουν μια εργασία.. Όλα αυτά τα αιτήματα περιγράφονται σε RSL, συμπεριλαμβανομένου του εκτελέσιμου αρχείου και των συνθηκών εκτέλεσή τους. Μπορούμε σαν χρήστες π.χ να καθορίσουμε το ποσό της μνήμης που χρειάζεται για να εκτελεστεί η εργασία σε απομακρυσμένο υπολογιστή.
Η διεργασία **gatekeeper** εγκαθιδρύει μια ασφαλή επικοινωνία μεταξύ πελατών και εξυπηρετητών. Η διεργασία αυτή είναι παρόμοια με την inetd όσο αφορά την λειτουργικότητά τους.

Τα τεχνικά χαρακτηριστικά του gatekeeper, με βάση το [41] είναι τα εξής:

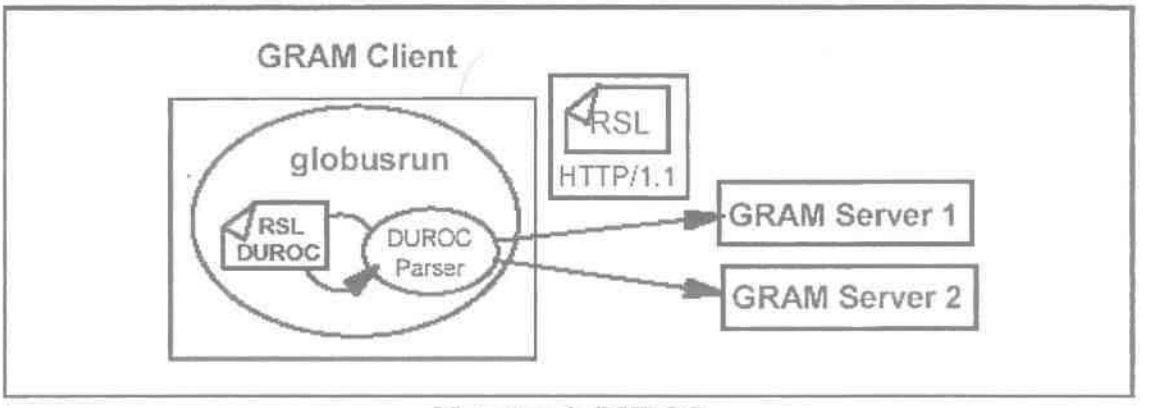
- Συνήθως αρχικοποιείται μέσω εντολών inetd-xinetd
- 'Τρέχει' με δικαιώματα root-administrator
- Πραγματοποιεί αμοιβαία αυθεντικοποίηση, επιβεβαιώνοντας την ταυτότητα του χρήστη, και τη δική του ταυτότητα στον χρήστη

- Αρχικοποιεί τον job manager σαν τοπικό χρήστη, με αντιστοίχηση στον αυθεντικοποιημένο απομακρυσμένο χρήστη. Αφού ο gatekeeper ελέγξει το gridmap file, αντιστοιχεί το DN του χρήστη σε ένα εξουσιοδοτημένο τοπικό όνομα. Έτσι μπορούν να τρέξουν όλες οι διεργασίες στον τοπικό 'λογαριασμό' του απομακρυσμένου χρήστη

Ο **job manager** δημιουργείται από τον gatekeeper. Παρέχει τις διεπαφές για έλεγχο της ανάθεσης κάθε τοπικού διαχειριστή πόρων (PBS,LSF, Schedulers...). Εκτός από αυτό, ο job manager αναλύει μέσω parsing την γλώσσα RSL, και αναθέτει τα αιτήματα εργασιών σε τοπικούς διαχειριστές πόρων. Ακόμα, λαμβάνει την κατάσταση των αιτημάτων διακοπής (εφόσον γίνει κάτι τέτοιο) από τους πελάτες, και στέλνει τα τελικά αποτελέσματα εξόδου πίσω στους πελάτες μέσω του GASS.
Όσο αφορά στα τεχνικά χαρακτηριστικά του, με βάση το [41] ο job manager :

- 'Τρέχει' σαν μια τυπική διεργασία ενός απλού χρήστη στο μηχάνημα gatekeeper
- Επικοινωνεί με τον απομακρυσμένο χρήστη μέσω πρωτοκόλλου HTTPS
- 'Ακούει' για αιτήματα από τον χρήστη σε οποιοδήποτε TCP port μεγαλύτερο του 1024
- Η επιλογή του port γίνεται κατά την επικοινωνία με το Gatekeeper και επιστρέφεται στο χρήστη σαν URL.
- Μπορεί να συνδέεται με απομακρυσμένους χρήστες σε αυθαίρετο TCP port μικρότερο του 1024 (π.χ για να επιστρέψει την εργασία και τα αποτελέσματα)

Το Globus Toolkit δεν υλοποιεί κάποιο job scheduler αλλά παρέχει διεπαφές για πολλούς άλλους (PBS,LSF,Condor). Το GRAM χρησιμοποιεί το GASS για να παρέχει μηχανισμό για μεταφορά του αρχείου εξόδου από τους εξυπηρετητές στους πελάτες, ενώ χρησιμοποιεί έναν μηχανισμό με όνομα DUROC προκειμένου να μπορούν οι χρήστες να υποβάλλουν εργασίες σε διαφορετικούς job managers που βρίσκονται σε διαφορετικούς υπολογιστές.



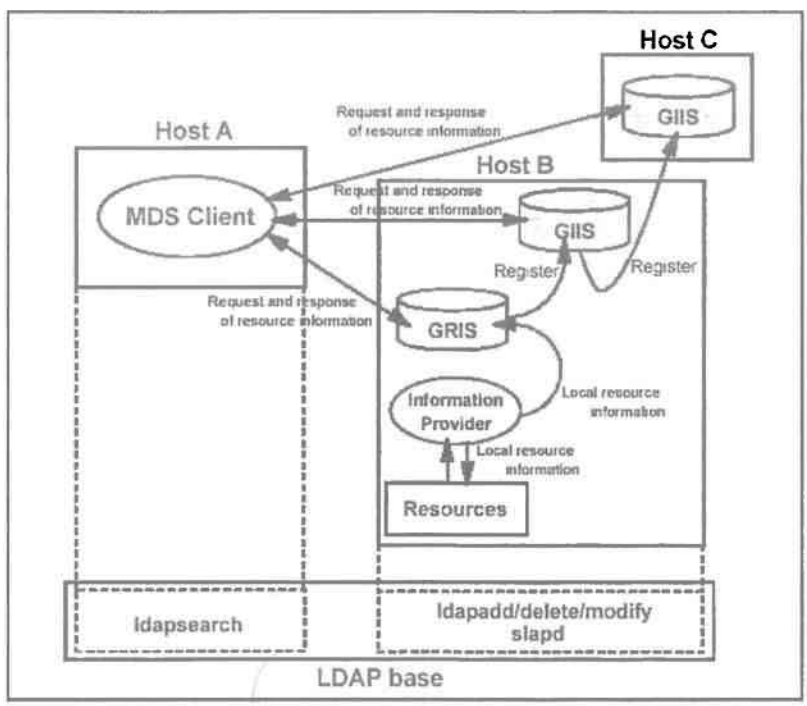
Μηχανισμός DUROC

5.3.2 Υπηρεσία Παρακολούθησης και ανακάλυψης πόρων (Monitoring and Discovery Service-MDS)

Το συγκεκριμένο κομμάτι του Globus παρέχει πρόσβαση σε στατική και δυναμική πληροφορία των πόρων του πλέγματος. Βασικά, αποτελείται από τα ακόλουθα συστατικά [32]:

- Grid Resource Information Service (GRIS)
- Grid Index Information Service (GIIS)
- Information Provider
- MDS client

Η παρακάτω εικόνα αναπαριστά την γενική δομή του MDS. Όπως βλέπουμε, η πληροφορία που σχετίζεται με τους πόρους, αποκτάται από τον πάροχο πληροφορίας (information provider) και προωθείται στο GRIS, το οποίο με την σειρά του την καταγράφει στο GIIS. Το GIIS μπορεί να μεταφέρει την πληροφορία σε άλλο GIIS.



MDS

Οι MDS clients μπορούν να αποκτήσουν την πληροφορία αυτή κατευθείαν από το GRIS (στο τοπικό και όχι μόνο μηχάνημα). Η πληροφορία πόρων, σχετίζεται με στατικά ή δυναμικά αντικείμενα πόρων π.χ όνομα εκτελέσιμης διεργασίας, διεπαφή δικτύου, διεύθυνση IP, μέγεθος μνήμης κτλ.

Το **GRIS** είναι ουσιαστικά ο χώρος αποθήκευσης της πληροφορίας που αφορά τους τοπικούς πόρους του μηχανήματος Αυτή η πληροφορία, παραμένει αποθηκευμένη για περιορισμένο χρονικό διάστημα γνωστό και σαν TTL (Time-To-Live). Αν δεν υπάρξει κάποιο αίτημα απόκτησης αυτής της πληροφορίας, η διάρκεια ζωής θα λήξει και θα διαγραφεί από το GRIS.

Το **GIIS** είναι το άλλο σημαντικό τμήμα του MDS, και είναι ο χώρος αποθήκευσης ευρετηρίων που αφορούν την πληροφορία που βρίσκεται στο GRIS. Οι πάροχοι πληροφοριών (Information providers) μεταφράζουν τις ιδιότητες και την κατάσταση των τοπικών πόρων σε μια μορφή που καθορίζεται από τα αρχεία διαμόρφωσης. Σε περίπτωση λοιπόν που θέλουμε να προσθέσουμε τον δικό μας πόρο για να χρησιμοποιηθεί από το MDS , πρέπει να προσδιορίσουμε συγκεκριμένους πάροχους πληροφορίας που θα μεταφράσουν τις ιδιότητες και την κατάσταση του πόρου μας στο GRIS.

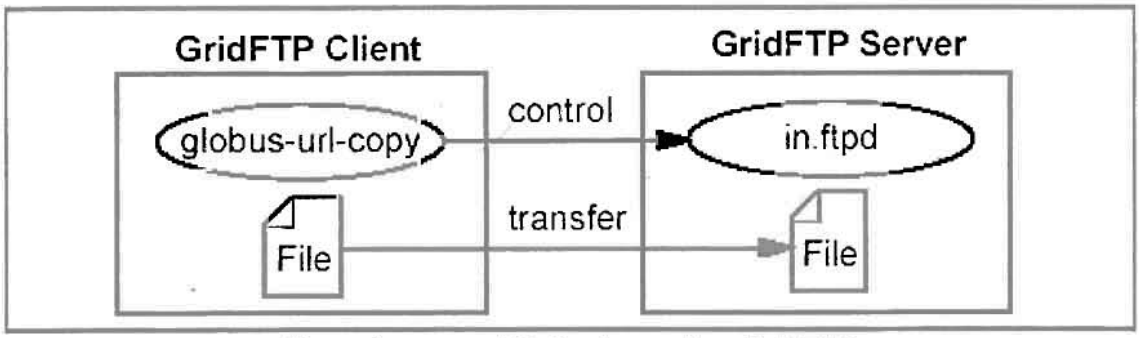
Επιπροσθέτως ο MDS client βασίζεται σε μηχανισμό LDAP και στην εντολή **ldapsearch** προκειμένου να ψάξει για πληροφορία για πόρους του πλέγματος, που θα τον ενδιαφέρουν. Αξίζει να τονίζουμε ότι το MDS έχει ιεραρχική δομή, παρόμοια με αυτή του DNS. Τα GRIS, GIIS των κατώτερων επιπέδων καταγράφουν την πληροφορία στα GIIS των υψηλότερων επιπέδων προκειμένου οι πελάτες να μπορούν πιο εύκολα να αποκτούν την πληροφορία αυτή .

5.3.3 GridFTP

Το συγκεκριμένο τμήμα του Globus καλύπτει τον τομέα της αξιόπιστης και ασφαλής μεταφοράς δεδομένων μέσα στο πλέγμα Πρόκειται, σύμφωνα με το [32] για πρωτόκολλο σχεδιασμένο για τις μεταφορές δεδομένων στο πλέγμα. Βασίζεται στο γνωστό πρωτόκολλο FTP , αλλά το επεκτείνει με πολλές άλλες λειτουργίες όπως multistreaming μεταφορές και μηχανισμούς ασφάλειας.

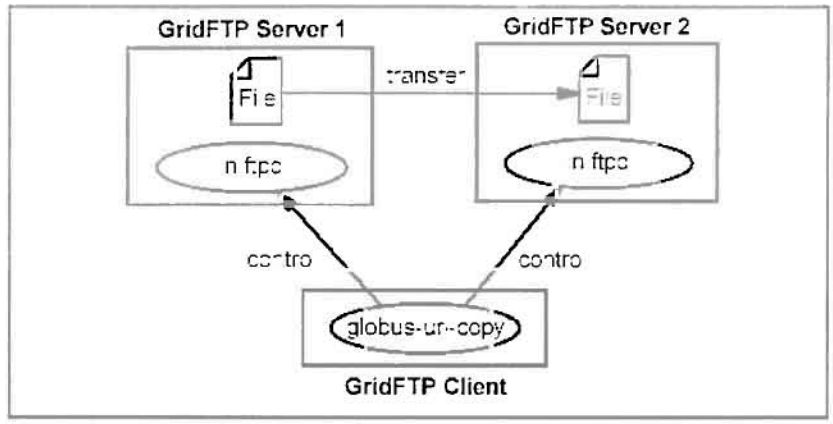
Το Globus Toolkit παρέχει GridFTP server και client που δημιουργούνται μέσω των διεργασιών in.ftpd και την εντολής globus-url-copy αντίστοιχα. Τόσο ο server όσο και ο πελάτης υποστηρίζουν δύο είδη μεταφοράς την τυπική (άμεση) και τη μεταφορά μέσω τρίτης έμπιστης πλευράς.

Στη τυπική μεταφορά δεδομένων, ο client στέλνει και λαμβάνει απευθείας το τοπικό αρχείο από τον server κάτι που φαίνεται και στην ακόλουθη εικόνα:



Τυπική μεταφορά δεδομένων μέσω GridFTP

Η μεταφορά δεδομένων μέσω τρίτης έμπιστης πλευράς (third party) χρησιμεύει όταν ο χρήστης θέλει να μεταφέρει μεγάλου μεγέθους αρχεία από απομακρυσμένο χώρο αποθήκευσης σε ένα άλλο απομακρυσμένο server όπως φαίνεται στην παρακάτω εικόνα:



Μεταφορά δεδομένων μέσω τρίτης έμπιστης πλευράς (third party)

Παρακάτω δίνονται μερικά τεχνικά χαρακτηριστικά GridFTP Server [36]:

- 'Ακούει' συνδέσεις GridFTP συνήθως στο TCP port 2811
- Όπως το κλασσικό FTP, αποτελείται από δύο ή παραπάνω κανάλια ένα για έλεγχο και ένα ή περισσότερα για δεδομένα, με το πρώτο να ακούει στο 2811 port.
- Αρχικοποιείται μέσω των εντολών inetd-xinetd
- Τρέχει ,όπως είναι φυσικό, με δικαιώματα administrator-root
- Υποστηρίζει αμοιβαία αυθεντικοποίηση, μέσω X.509 πιστοποιητικών, στα κανάλια ελέγχου και δεδομένων.
- Τα κανάλια δεδομένων ,λειτουργούν σε οποιοδήποτε port πάνω από το 1024
- Το κανάλι ελέγχου παρέχει μηχανισμούς για προστασία ακεραιότητας και τα αντίστοιχα κανάλια δεδομένων παρέχουν κρυπτογράφηση στην πλευρά του πελάτη.

Αντιστοίχως μερικά χαρακτηριστικά ενός GridFTP client σύμφωνα με το ίδιο άρθρο είναι τα εξής:

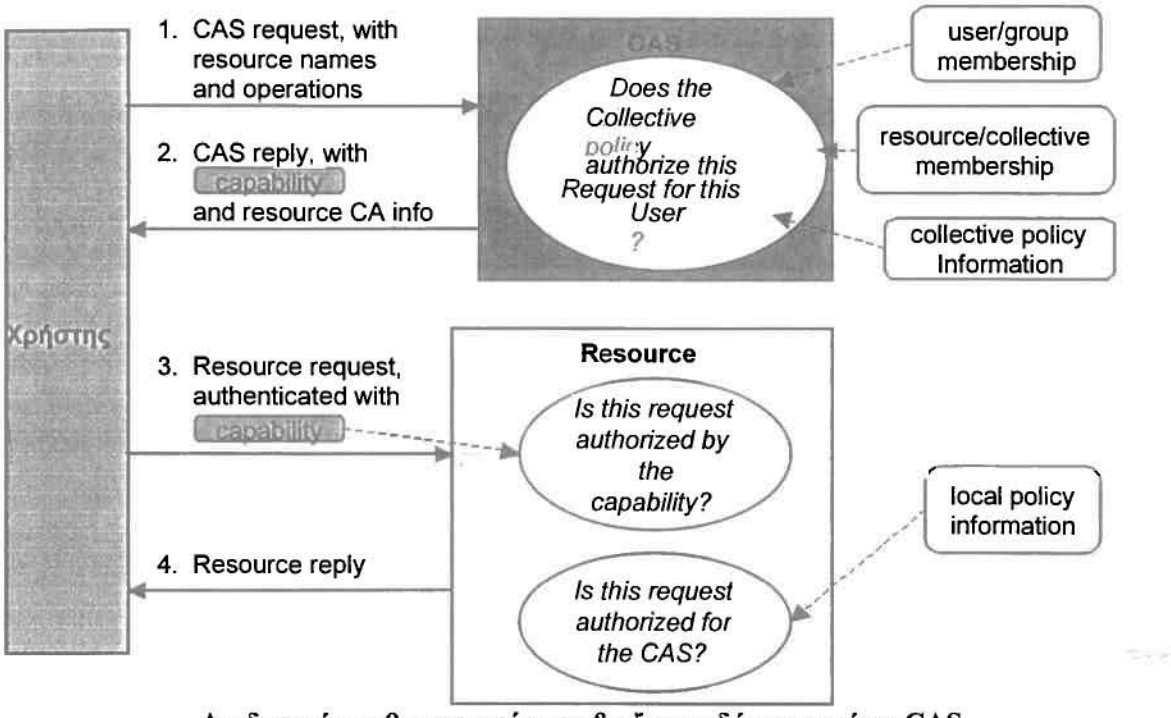
- Δεν απαιτεί να είναι εγκατεστημένα τα συστατικά του server στο τοπικό μηχάνημα
- Χρησιμοποιεί οποιοδήποτε TCP port πάνω από το 1024
- Δεν απαιτεί δικαιώματα root-administrator για να τρέξει
- Μπορεί να αρχικοποιήσει third party μεταφορά δεδομένων ανάμεσα σε δύο απομακρυσμένους GridFTP servers, χαρακτηριστικό το οποίο είναι πολύ χρήσιμο για ένα περιβάλλον πλέγματος.
- Δεν μπορεί να συνδεθεί σε ένα τυπικό FTP Server

5.3.4 Υπηρεσία εξουσιοδότησης ομάδων χρηστών (Community Authorization Service CAS)

Η υπηρεσία εξουσιοδότησης ομάδων χρηστών, είναι ένα καινούργιο συστατικό του Globus (έκδοση 3.2 και πάνω). Το CAS βοηθά τους πάροχους πόρων να δημιουργήσουν πανομοιότυπες πολιτικές ελέγχου για κάθε μέλος μιας ομάδας (community member) [30].
Η υπηρεσία αυτή καθιστά εφικτή την ομαδική επεξεργασία δικαιωμάτων πρόσβασης χρηστών μιας συγκεκριμένης ομάδας.

Αυτό απαιτεί την δημιουργία ενός CAS server που θα λειτουργεί σαν επεξεργαστής των αιτημάτων των χρηστών μιας ομάδας για παροχή υπολογιστικών πόρων του πλέγματος. Με τη χρήση ενός τέτοιου server οι πάροχοι πόρων μπορούν να καθορίσουν πολιτική πρόσβασης για συγκεκριμένη ομάδα-κοινότητα χρηστών.

Με βάση λοιπόν το [30] κάθε ομάδα χρηστών πλέγματος αρχικοποιεί το δικό της CAS server. Ο εκπρόσωπος αυτής της ομάδας αποκτά εξουσιοδότηση GSI προκειμένου να παρουσιάζει την ομάδα –κοινότητα σαν κάτι ενιαίο. Επίσης χρησιμοποιεί το CAS για διαχείριση και έλεγχο έμπιστων σχέσεων καθώς και για δημιουργία ελέγχου πρόσβασης στους πόρους. Τα μέλη μιας ομάδας έχοντας το κατάλληλο δικαίωμα, μπορούν να εξουσιοδοτήσουν άλλα μέλη της ομάδας.



Διαδικασία αυθεντικοποίησης & εξουσιοδότησης μέσω CAS

Η υπηρεσία CAS λειτουργεί ως εξής : Όταν ο χρήστης πλέγματος θέλει να έχει πρόσβαση σε πόρο πλέγματος, που είναι προσβάσιμος μέσω CAS server ο χρήστης δημιουργεί ένα αίτημα στον server. Αν η βάση δεδομένων CAS υποδείξει ότι ο χρήστης έχει τα απαιτούμενα δικαιώματα, τότε εκδίδει ένα προσωρινό GSI proxy πιστοποιητικό για το χρήστη. Αυτό το πιστοποιητικό , έχει επισυναπτόμενη μια πολιτική πρόσβασης, που εξουσιοδοτεί τους χρήστες να πραγματοποιήσουν στον πόρο ορισμένες πράξεις. Ο χρήστης με τη σειρά του χρησιμοποιεί το πιστοποιητικό από τον CAS server που δίνει δικαιώματα πρόσβασης στην ομάδα, για να έχουν πρόσβαση στους πόρους μέσω εργαλείων (GridFTP).

Έπειτα ο πόρος πλέγματος, εφαρμόζει την τοπική πολιτική ασφάλειάς του για να καθορίσει το επίπεδο ασφάλειας πρόσβασης στην ομάδα που έχει το πιστοποιητικό από το CAS server.

5.4 ΜΟΝΤΕΛΟ ΑΣΦΑΛΕΙΑΣ OGSA

Η πιο πρόσφατη έκδοση του Globus Toolkit είναι 4 (Φεβρουάριος 2005 [35]) ωστόσο εμείς θα μελετήσουμε σύντομα την υλοποίηση υπηρεσιών-χαρακτηριστικών OGSA στην έκδοση 3. Το Globus Toolkit 3 σύμφωνα με το [35] :

- Έχει σχεδόν τα ίδια βασικά χαρακτηριστικά με προηγούμενη έκδοση (GSI,GRAM, GridFTP, MDS)
- Βασίζεται σε μηχανισμούς OGSA
- Υποστηρίζει open source υλοποιήσεις OGSI
- Χρησιμοποιεί και επεκτείνει Web υπηρεσίες

Η έκδοση 3 χρησιμοποιεί πρωτόκολλα ασφάλειας WS όπως SOAP, XML πρωτόκολλα, εφαρμογές υπογραφής μέσω XMAL και προτυποποιήσεις για όλες τις επικοινωνίες, καθώς και κλασσικά πρωτόκολλα αυθεντικοποίησης και εμπιστευτικότητας όπως το TLS.

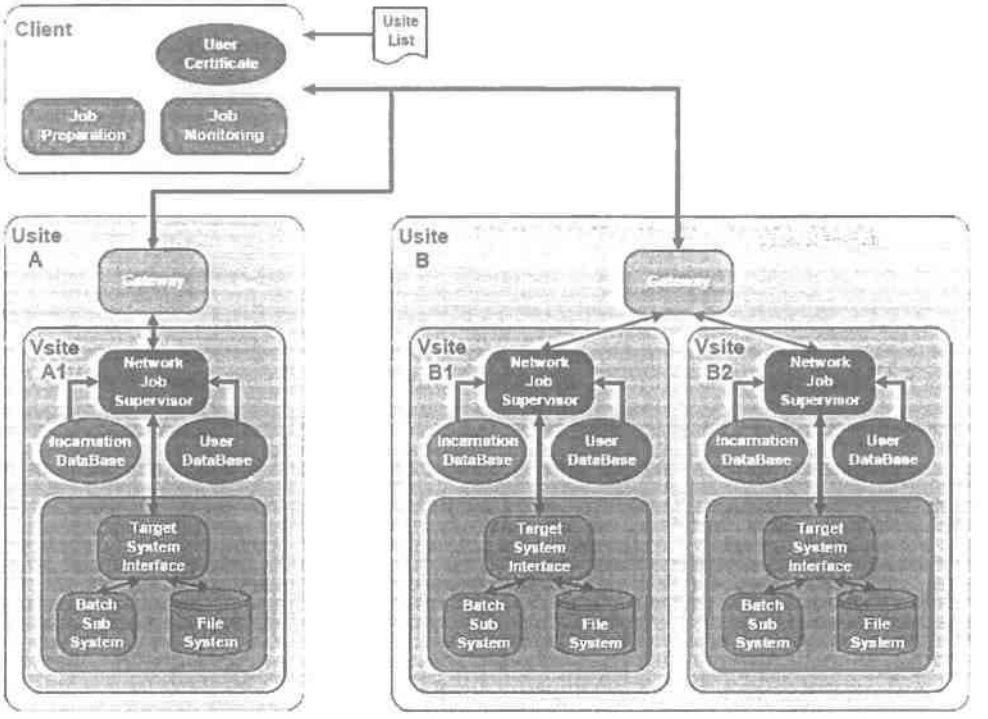
Στην παραπάνω προσέγγιση της δομής GT3 ([35]), το επίπεδο πυρήνα (core layer) αποτελείται κυρίως από υλοποιήσεις πάνω σε διεπαφές OGSI καθώς και από υπηρεσίες συστήματος πλέγματος, π.χ υπηρεσίες admin, logging που αφορούν τον διαχειριστή του πλέγματος καθώς και την διαδικασία εισόδου σε μια υπηρεσία ή πόρο του πλέγματος.
Στο αμέσως ανώτερο επίπεδο , αυτό της ασφάλειας, έχουμε το GSI που το μελετήσαμε πιο πάνω.
Στα υπόλοιπα επίπεδα υλοποιούνται όλοι οι μηχανισμοί που μελετήσαμε πιο πάνω όπως GRAM, MDS, GridFTP κτλ.

Συνοψίζοντας, η έκδοση 3 έχει ουσιαστικό στόχο την ανάπτυξη υπηρεσιών πλέγματος στηριζόμενη στην αρχιτεκτονική OGSA, εν αντιθέσει με προηγούμενες εκδόσεις π.χ 2.4 που στόχευε στην ανάπτυξη ασφαλούς υποδομής πλέγματος (σε κατώτερα grid core επίπεδα). [41]

5.5 ΥΛΟΠΟΙΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΕ GRID PROJECTS

5.5.1 UNICORE (Uniform Interface to Computer Resources)

Πρόκειται για ένα project που χρηματοδοτείται από το υπουργείο παιδείας και έρευνας της Γερμανίας. Παρέχει μια ομοιόμορφη διεπαφή για την εκπόνηση κάποιων διεργασιών καθώς και για την ασφαλή πρόσβαση σε πόρους υπερ-υπολογιστών. Πρόκειται ουσιαστικά για ένα σύστημα πλέγματος που ενσωματώνει μηχανισμούς ασφάλειας, διαχείρισης ροής εργασιών και υποστήριξη ποικίλων πόρων.



Αρχιτεκτονική UNICORE

5.5.1.1 Λειτουργικότητα UNICORE

Οι τελικοί χρήστες του UNICORE μπορούν να αλληλεπιδρούν με άλλα sites και συστήματα που βρίσκονται μέσα στο πλέγμα του UNICORE μέσω γραφικής διεπαφής Client, που υποστηρίζει ευρεία γκάμα συστημάτων Java είτε σε πλατφόρμες Unix είτε σε Windows.
Τα βήματα που ακολουθεί ένας χρήστης μέσα στο UNICORE είναι τα εξής [45]:

- Ο χρήστης ξεκινά το πρόγραμμα UNICORE client
- Ο χρήστης ενεργοποιεί το UNICORE πιστοποιητικό του, εισάγοντας το κατάλληλο password
- Το Client φορτώνει διάφορα plug-in που του υπέδειξε ο χρήσης
- Το Client συνδέεται αυτόματα με sites του πλέγματος, μέσω των gateways που αυτά παρέχουν . Ανακτά την πληροφορία για διαθέσιμους πόρους, συστήματα, προγράμματα κτλ.

Ο χρήστης μπορεί πλέον να δημιουργήσει τις δικές του διεργασίες και να αποφασίσει σε ποιο από τους διαθέσιμους πόρους του πλέγματος θα τις αναθέσει.

Οι διεργασίες μπορούν να διασπαστούν σε επιμέρους ενέργειες προς εκτέλεση. Σε περίπτωση λοιπόν που κάποια από αυτές τις ενέργειες δεν εκτελεστεί τότε 'παγώνει' και η διαδικασία εκτέλεσης της συνολικής διεργασίας του χρήστη.

5.5.1.2 Χαρακτηριστικά ασφάλειας UNICORE --Υποδομή δημοσίου κλειδιού (UNICORE PKI)

Η υποδομή δημοσίου κλειδιού βασίζεται σε μια κεντρικοποιημένη αρχιτεκτονική με μια κεντρικού ρόλου αρχή πιστοποίησης (ΑΠ-CA) και πολλαπλές αρχές καταχώρησης (RA) οι οποίες κάνουν χρήση X.509 ψηφιακών πιστοποιητικών. Γενικά υπάρχει η PKI που αποτελείται από έμπιστη ΑΠ ρίζα (root CA), UNICORE CA (U-CA), λίστες ανάκλησης πιστοποιητικών της root-CA, U-CA, και πιστοποιητικά για κάθε gateway.

Οι συμμετέχοντες στο συγκεκριμένο πλέγμα, ανήκουν σε ένα εικονικό οργανισμό ο οποίος περιλαμβάνει μεγάλα υπολογιστικά κέντρα, δημόσια γραφεία, πανεπιστήμια και πολλοί άλλοι φορείς. Προκειμένου να προστατευθεί η ακεραιότητα και εμπιστευτικότητα των δεδομένων, το UNICORE μέσω της PKI χρησιμοποιεί πιστοποιητικά για την αυθεντικοποίηση χρηστών, καθώς και UNICORE Gateways, για την υπογραφή διεργασιών και λογισμικού.

Γενικά , υπάρχουν δύο επίπεδα στην ιεραρχία πιστοποίησης ,η ΑΠ-ρίζα (Root CA) και η U-CA. Η πρώτη με το δικό της πιστοποιητικό υπογράφει το αντίστοιχο της δεύτερης και αυτή με τη σειρά της πιστοποιεί τους χρήστες, servers κτλ. Σε κάθε περίπτωση , όταν πρέπει να γίνει αυθεντικοποίηση ενός χρήστη ή gateway-server, ελέγχεται το ψηφιακό πιστοποιητικό του και ιδιαίτερα η αλυσίδα των ΑΠ που το υπογράφουν, προκειμένου να ελεγχθεί αν κάποια από αυτές δεν είναι έγκυρες. Ενεργό ρόλο στην έκδοση και υπογραφή πιστοποιητικών παίζουν σύμφωνα και με το [45] οι αρχές καταχώρησης (RA).
Μάλιστα , να τονιστεί ότι ο χρήστης πρέπει να αυθεντικοποιήσει τον εαυτό του στην RA είτε με προσωπική του επίσκεψη στους υπεύθυνους εκεί, είτε μέσω video-διάσκεψης, μια πραγματικά πρωτότυπη τεχνική αυθεντικοποίησης.

Στο συγκεκριμένο σύστημα πλέγματος UNICORE, μπορούν να εφαρμοστούν δύο λύσεις για την ιεραρχία πιστοποίησης. Η πρώτη, περιλαμβάνει μία και μόνο αρχή πιστοποίησης (Single U-CA) η οποία και θα πιστοποιεί τους χρήστες του UNICORE τα Gateways, servers κτλ. αποτελώντας μια ευέλικτη λύση κατάλληλη για μικρό αριθμό χρηστών πλέγματος.
Η δεύτερη λύση περιλαμβάνει πολλαπλές αρχές πιστοποίησης (multiple-CA) και είναι σαφώς πιο πολύπλοκη λύση αλλά και πιο κατάλληλη για μεγαλύτερο αριθμό χρηστών πλέγματος.

5.5.1.3 Εξουσιοδότηση

Προτού ένας χρήστης να υποβάλλει τις διεργασίες του σε ένα συγκεκριμένο σύστημα, πρέπει να του έχει δοθεί πρώτα το δικαίωμα πρόσβασης. Η αυθεντικοποίηση και εξουσιοδότηση λαμβάνει χώρα στο συγκεκριμένο site. Αφού γίνει η αυθεντικοποίηση ελέγχονται τα δικαιώματα χρήσης του χρήστη.

Συγκεκριμένα γίνεται έλεγχος της εγκυρότητας όλων των πιστοποιητικών αλυσίδας που υπογράφουν αυτό του χρήστη, και έπειτα γίνεται έλεγχος στις βάσεις δεδομένων για να ελεγχθούν τα δικαιώματα χρήσης.
Αξίζει να τονιστεί ότι και σε αυτό το σύστημα πλέγματος κυρίαρχο ρόλο παίζει η διαφύλαξη πιστοποιητικών και των ιδιωτικών κλειδιών σε ιδιωτικούς χώρους φύλαξης (private keystore).
Μάλιστα έχουν αναπτυχθεί κάποιοι μηχανισμοί προκειμένου ο χρήστης που τρέχει πολλές εφαρμογές στο πλέγμα (π.χ secure mail, VPN κτλ) να μην χρειάζεται να ανατρέχει σε ξεχωριστούς χώρους φύλαξης των πιστοποιητικών. Αντιθέτως, υπάρχει ένας ενιαίος χώρος φύλαξης όπου ο χρήστης όποτε είναι ανάγκη θα ανατρέχει για να τα χρησιμοποιεί.

Τέλος, το συγκεκριμένο σύστημα πλέγματος UNICORE, μπορεί μέσω του κατάλληλου interface να επικοινωνήσει και με πλέγματα βασισμένα στο Globus. Ιδιαίτερα όταν ένας χρήστης του UNICORE θέλει να εκτελέσει μια διεργασία σε κάποιο πόρο του GLOBUS. Τότε το πιστοποιητικό UNICORE που κατέχει, μετατρέπεται στην αντίστοιχη μορφή του Globus προκειμένου όταν σταλεί σε αυτό να μπορέσει να αυθεντικοποιηθεί και να εξουσιοδοτηθεί.

5.5.2 Information Power Grid (I.P.G)

Πρόκειται για ένα project της NASA, σε συνεργασία με την NSF που έχει στόχο να κτίσει ένα δίκτυο υπερ-υπολογιστών, συσκευών αποθήκευσης δεδομένων, επιστημονικών οργάνων. Ο γενικότερος στόχος του IPG είναι η αύξηση της ικανότητας των επιστημονικών κοινοτήτων της NASA, να επιλύουν προβλήματα που έχουν μεγάλες υπολογιστικές και όχι μόνο απαιτήσεις. Η έρευνα συνεχίζεται σε πολλούς τομείς του IPG , όπως στην δημιουργία υποδομής για τον εντοπισμό, την ομαδοποίηση και τη διαχείριση πόρων που βρίσκονται κατανεμημένοι στα επιστημονικά κέντρα της NASA, έρευνα για την αυθεντικοποίηση των χρηστών, την ανάθεση πόρων, και την **ασφάλεια.**
Τα πλεονεκτήματα που αποκομίζει η NASA από την χρήση ενός τέτοιου πλέγματος είναι πραγματικά πολλά. Ωστόσο για να γίνει αποδοτική εκμετάλλευση αυτών των πλεονεκτημάτων απαιτείται η εκπλήρωση συγκεκριμένων προϋποθέσεων όπως η υπολογιστική υποδομή και η ασφάλεια. [12]

Όσο αφορά την πρώτη , σύμφωνα με το [48] έχει αναπτυχθεί το κατάλληλο **λειτουργικό σύστημα** που αυτή τη στιγμή υποστηρίζει **300 επεξεργαστικούς κόμβους**, πολλούς clusters και σταθμούς εργασίας, **30-100 TeraBytes** προσβάσιμου αποθηκευτικού χώρου καθώς και ύπαρξη δικτύου που υποστηρίζει ταχύτητες τουλάχιστον **100MB/s**.
Ωστόσο πολύ σημαντικό ρόλο παίζει και η ασφάλεια στο πλέγμα. Για αυτό το λόγο συνεχίζονται η έρευνα σε τομείς όπως αυθεντικοποίηση IPG πόρων, κεντρική διαχείριση των διεργασιών που περιμένουν σε ουρές στις εκάστοτε CPU καθώς και η χρήση υποδομής δημόσιου κλειδιού.

Γενικά, το IPG έχει δομημένη αρχιτεκτονική, διαχωρίζοντας τις διάφορες υπηρεσίες στα εκάστοτε επίπεδα.
Το IPG στηρίζεται στις υπηρεσίες του Globus. Τα πιο ενδιαφέροντα για την μελέτη μας, επίπεδα είναι αυτά του Application Oriented Middleware Systems (AOMS) και

του Grid Common Services (GCS), καθώς σε αυτά τα επίπεδα υλοποιούνται οι υπηρεσίες ασφάλειας.

Συγκεκριμένα στο AOMS χρησιμοποιούνται οι υπηρεσίες GASS ,GRAM,MDS, GSI του Globus που αφορούν την διαχείριση και ανάθεση των πόρων καθώς και την ασφάλεια του πλέγματος (GSI).
Στο GCS υλοποιούνται υπηρεσίες προγραμματισμού πόρων , διάσπασης διεργασιών , αυθεντικοποίησης καθώς και οι αρχές πιστοποίησης.

Όσο αφορά στην ασφάλεια και στον έλεγχο πρόσβασης ειδικότερα , υποστηρίζεται η καθολική πιστοποίηση (single sign-on) για όλους τους πόρους, η οποία με την σειρά της βασίζεται σε κρυπτογραφημένα πιστοποιητικά που φυλάσσονται στους υπολογιστές των χρηστών ή στα περιβάλλοντα επίλυσης προβλημάτων (Problem Solve Environment).Επιπροσθέτως, σύμφωνα και με το [48], υποστηρίζονται κρυπτογραφημένα κανάλια επικοινωνίας από άκρη σε άκρη ,προκειμένου να διασφαλιστεί η ακεραιότητα και η εμπιστευτικότητα των δεδομένων.

Σύμφωνα με το [49] , υποστηρίζονται εκτός του IPG και άλλα συγκεκριμένων αρχών, πιστοποιητικά όπως Globus,Alliance,LLB κτλ. Ο χρήστης μπορεί στις κατάλληλες μηχανές του IPG Grid να κάνει ένα αίτημα απόκτησης πιστοποιητικού και ανάλογα με την πολιτική ασφάλειας να αποκτήσει ένα. Μάλιστα ο χρήστης μπορεί να έχει και το δικό του proxy certificate μέσω του προσωπικού του πιστοποιητικού, τον οποίο θα εκπροσωπεί στις 'συναλλαγές' που λαμβάνουν χώρα μέσα στο πλέγμα.
Συμπερασματικά, πρόκειται για ένα φιλόδοξο και σπουδαίο project υπολογιστικής πλέγματος, στο οποίο σημαντικό ρόλο παίζει η ασφάλεια, μέσω και της χρήσης του Globus Toolkit.

5.5.3 European DataGrid

Το συγκεκριμένο project , βρίσκεται υπό την εποπτεία του CERN και ιδρύθηκε από την Ευρωπαϊκή Ένωση με σκοπό την εγκαθίδρυση ενός υπολογιστικού πλέγματος πόρων για την ανάλυση δεδομένων που θα προέρχονται από επιστημονική έρευνα. Κύριος στόχος του DataGrid είναι η ανάπτυξη και ο έλεγχος υποδομής που θα επιτρέπει την ανάπτυξη επιστημονικών συνεργασιών όπου οι ερευνητές και οι επιστήμονες θα μπορούν να εργάζονται ανεξάρτητα της γεωγραφικής τους θέσης. Αυτού του είδους οι συνεργασίες θα επιτρέπουν τις προσωπικές αλληλεπιδράσεις των επιστημόνων καθώς και την διαμοίραση δεδομένων και εργαλείων σε παγκόσμια βάση.[12]
Η δομή του DataGrid Project χωρίζεται σε 12 τμήματα εργασίας (work - packages WP) που με τη σειρά τους κατανέμονται σε 4 ομάδες εργασίας:

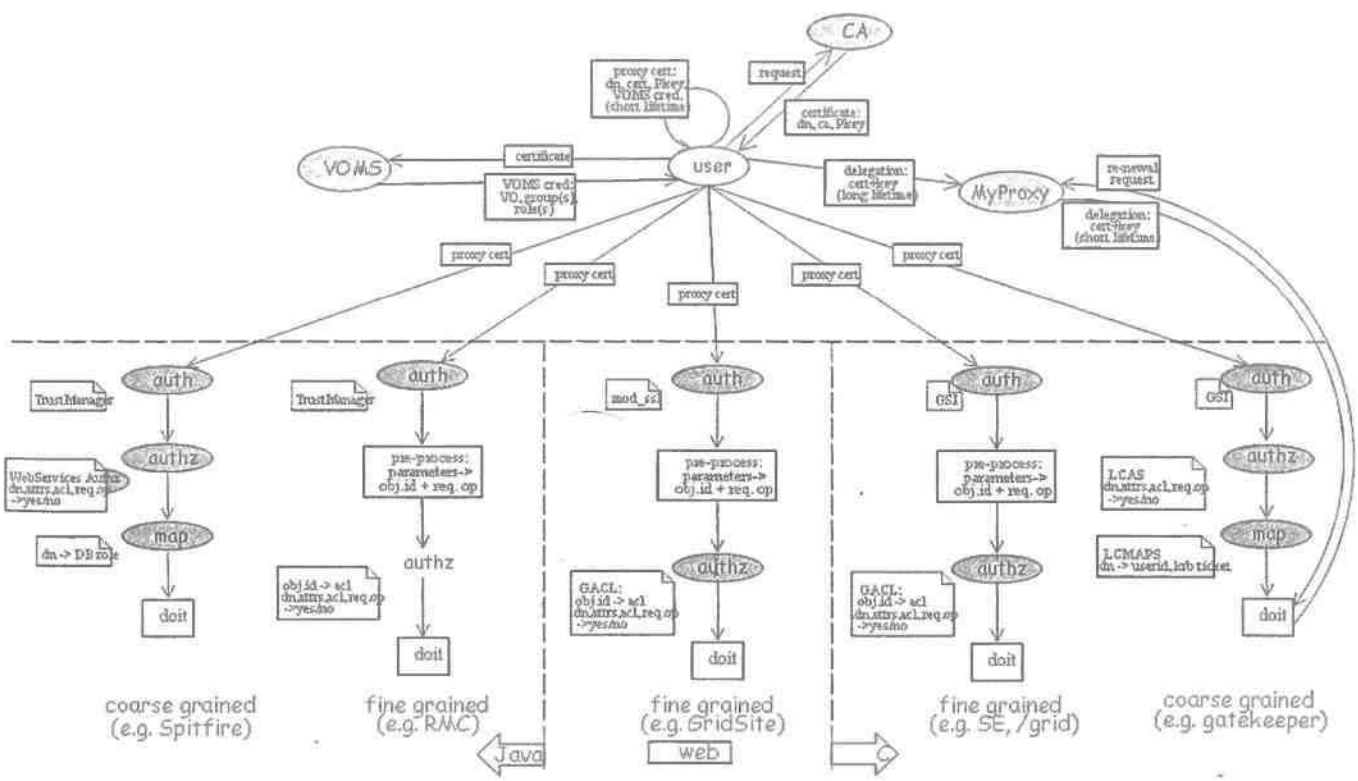
→Υποδομής (testbed and infrastructure)
→Εφαρμογές
→DataGrid Middleware
→Διαχείρισης (management)

Στο project δίνεται έμφαση στην δυνατότητα κατανεμημένης επεξεργασίας δεδομένων που προέρχονται από επιστημονικές εφαρμογές κυρίως φυσικής υψηλής ενέργειας , παρατήρησης φυσικών φαινομένων, βιο-πληροφορικής κτλ.

5.5.3.1 Ασφάλεια DataGrid

Αν και δεν υπάρχει ένα κομμάτι εργασίας (WP) το οποίο ασχολείται αποκλειστικά και μόνο με την ασφάλεια του πλέγματος, ωστόσο με βάση το [51] το WP2 έχει την κύρια ευθύνη υλοποίησης και εφαρμογής μηχανισμών ασφάλειας στο πλέγμα του DataGrid. Βέβαια και τα άλλα τμήματα εργασίας συμβάλλουν ως ένα ποσοστό σε αυτό.
Οι χρήστες μπορούν μέσω της τοπικής αρχής πιστοποίησης (CA) να εκδώσουν το πιστοποιητικό δημοσίου κλειδιού, ενώ μπορούν να είναι μέλη ενός ή περισσότερων εικονικών οργανισμών (VO). Εφόσον ανήκουν σε ένα VO, μπορούν να αποκτήσουν και δικαιώματα χρήσης-πρόσβασης μέσω κατάλληλων διαπιστευτηρίων εξουσιοδότησης από το VO στον οποίο ανήκουν. Εκτός από αυτό, αναπτύσσονται και σχέσεις εμπιστοσύνης ανάμεσα στους διάφορους εικονικούς οργανισμούς αλλά και στις εκάστοτε αρχές πιστοποίησης.

Στην παρακάτω εικόνα μπορούμε να δούμε τον μηχανισμό ασφάλειας του DataGrid. Για τις ανάγκες του project έχουν δημιουργηθεί κάποιες αρχές πιστοποίησης που βασίζονται σε υποδομή δημοσίου κλειδιού για το DataGrid αλλά και για άλλα project πλέγματος (CrossGrid, DataTAG κτλ). Μάλιστα έχουν αναπτυχθεί εργαλεία γραμμένα σε Java για την αυθεντικοποίηση.



Συστατικά ασφάλειας DataGrid

Όπως παρατηρούμε από την εικόνα για την **αυθεντικοποίησή** του ο χρήστης χρησιμοποιεί το πιστοποιητικό του από την αρμόδια CA και μάλιστα μπορεί να κάνει χρήση ενός συστήματος του Globus, το MyProxy προκειμένου να μπορεί και απομακρυσμένα να διαχειρίζεται τα πιστοποιητικά του και να έχει πρόσβαση σε πόρους πλέγματος μέσω Web-portals.

Αφού εκδοθεί το πιστοποιητικό του, ο χρήστης δημιουργεί ένα πιστοποιητικό πληρεξουσιότητας (proxy-cert) το οποίο θα δρα εκ μέρους του στις όποιες αιτήσεις για αυθεντικοποίηση σε απομακρυσμένους πόρους. [51]

Η **εξουσιοδότηση** στο DataGrid είναι λίγο πιο πολύπλοκη , με την έννοια ότι δεν έχουμε μόνο ένα τρόπο εξουσιοδότησης αλλά πολλούς. Πιο συγκεκριμένα μπορούμε να έχουμε εξουσιοδότηση μέσω ελέγχου του πίνακα αντιστοίχησης (Mapping file), μέσω γλώσσας ελέγχου πρόσβασης (access list), αλλά και μέσω υπηρεσιών C/C++.
Ειδικότερα, και σύμφωνα με το [51] κάθε VO έχει κάποιο LDAP server που διαχειρίζεται τα μέλη του VO. Σαν φυσικό επακόλουθο , είναι ο LDAP να παράγει ένα πίνακα αντιστοίχησης των χρηστών για το πλέγμα. Κάθε φορά λοιπόν που χρειάζεται να γίνει εξουσιοδότηση, μπορεί να γίνει έλεγχος σε αυτό το αρχείο για να διαπιστωθεί αν έχει ο χρήστης το δικαίωμα πρόσβασης σε πόρους του πλέγματος.

Σε περιπτώσεις που πρέπει να γίνει έλεγχος εξουσιοδότησης σε τοπικό επίπεδο (π.χ για τοπικούς πόρους), γίνεται χρήση συγκεκριμένων εργαλείων και υπηρεσιών όπως το LCAS (Local Centre Authorization Service), LCMAPS (Local Credential Mapping Service) αλλά και του διαχειριστή εξουσιοδότησης (Java authorization Manager).
Όσο αφορά στην εμπιστευτικότητα, συνεχίζονται οι έρευνες και οι προσπάθειες για την βελτίωση της κρυπτογράφησης των δεδομένων ιδιαίτερα στον τομέα των Βιο-ιατρικών εφαρμογών όπου απαιτείται τα δεδομένα να παραμένουν απόρρητα.
Γενικά, το μοντέλο εξουσιοδότησης βασίζεται στο GSI και στο Globus. Συμπερασματικά, πρόκειται για ένα πολύ χρήσιμο project υπολογιστικής πλέγματος που συμβάλλει σημαντικά στην επιστημονική έρευνα και η εφαρμογή μηχανισμών ασφάλειας, βελτιώνει σημαντικά την απόδοσή του.

5.5.4 Earth Grid System(ESG)

Το συγκεκριμένο σύστημα, αποτελεί project που χρηματοδοτείται από την R&D και έγινε με σκοπό να καταστήσει δυνατή (στους επιστήμονες) την διαχείριση, την ανακάλυψη, και την επεξεργασία των κατανεμημένων ερευνητικών κλιματολογικών δεδομένων [53].
Η δεύτερη έκδοσή του (ESG-II) βασίζεται στην πρώτη (ESG-I) , στο Globus Toolkit, καθώς και σε τεχνολογίες DataGrid. Σε αυτό το project συμμετέχουν ερευνητές και επιστήμονες από πολλά πανεπιστήμια εθνικούς οργανισμούς και ερευνητικά κέντρα όπως είναι το ANL,LBNL,ORNL,NCAR κτλ.

Σε συγκεκριμένα ιδρύματα των ΗΠΑ έχει εγκατασταθεί ειδικός εξοπλισμός (ESG Servers,Clusters,αποθηκευτικοί χώροι) ενώ σε άλλα υλοποιούνται οι παρεχόμενες υπηρεσίες πλέγματος (Grid Services) προκειμένου να υπάρξει κατανεμημένη επεξεργασία της πληροφορίας. Π.χ οι υπηρεσίες πλέγματος του Globus (που μας ενδιαφέρουν και περισσότερο) υλοποιούνται και παρέχονται από το ANL.

Η λειτουργία του συγκεκριμένου πλέγματος, είναι η εξής: παρατηρούνται μέσω αισθητήρων, οργάνων , μετεωρολογικών δορυφόρων και εικόνων οι κλιματολογικές συνθήκες που λαμβάνουν χώρα σε όλο τον πλανήτη (π.χ σύννεφα, πάγοι, ατμοσφαιρικά δεδομένα, όζον). Έπειτα αποθηκεύονται σε δίσκους και μέσω κατάλληλων αλγορίθμων γίνεται η επεξεργασία τους από τους επιστήμονες, προκειμένου να βγάλουν τα ανάλογα συμπεράσματα, για το τι μέλλει γενέσθαι στο πλανήτη μας.

Τα μεγέθη των δεδομένων είναι σε TBytes ενώ η βελτίωση της υπολογιστικής επεξεργασίας είναι της τάξης του O (1000-10000) δηλαδή έχουμε γραμμική βελτίωση στην υπολογιστική επεξεργασία μέσω πλέγματος.

Επίσης τα μετά-δεδομένα που προέρχονται από επεξεργασία κλιματολογικών μοντέλων, αποθηκεύονται σε δίσκους και είναι προσπελάσιμα μέσων των υπηρεσιών αναζήτησης-ανακάλυψης (search-Discovery) όπου και ο επιστήμονας (ανάλογα με την εξουσιοδότηση που έχει) μπορεί να κάνει ένα ερώτημα (query) σε ένα Web portal και να πάρει τα αποτελέσματα της αναζήτησης στις βάσεις δεδομένων. Και αυτό γιατί οι επιστήμονες χρειάζονται συνήθως τμήματα των δεδομένων προκειμένου να πάρουν την πληροφορία που θέλουν.

5.5.4.1 Προκλήσεις του ESG

Σύμφωνα με το [53] υπάρχουν συγκεκριμένες προκλήσεις στο συγκεκριμένο project, τις οποίες καλούνται να αντιμετωπίσουν οι επιστήμονες:

- Δυνατότητα για ομαδική προσομοίωση και διαχείριση δεδομένων
- Δυνατότητα για ανάλυση και οπτικοποίηση των αποτελεσμάτων στην επιστημονική κοινότητα του project (μετεωρολόγοι, γεωφυσικοί) και φυσικά πρόσβαση σε αυτά από τους επιστήμονες .

Αυτές οι προκλήσεις απαιτούν και πολύ καλή υποδομή ,γρήγορο δίκτυο, αποτελεσματικούς επεξεργαστές και καλή διαχείριση των αποθηκευτικών πόρων.

5.5.4.2 Ασφάλεια ESG

Το ESG βασίζεται στο Globus και χρησιμοποιεί πολλές υπηρεσίες και συστατικά του. Συγκεκριμένα για την μεταφορά των δεδομένων χρησιμοποιείται GridFTP Servers σε διάφορα ιδρύματα που συμμετέχουν στο ESG, ώστε οποιοσδήποτε θέλει απομακρυσμένα να μεταφέρει δεδομένα, να μπορεί να το πράξει μέσω του κατάλληλου GridFTP Client.

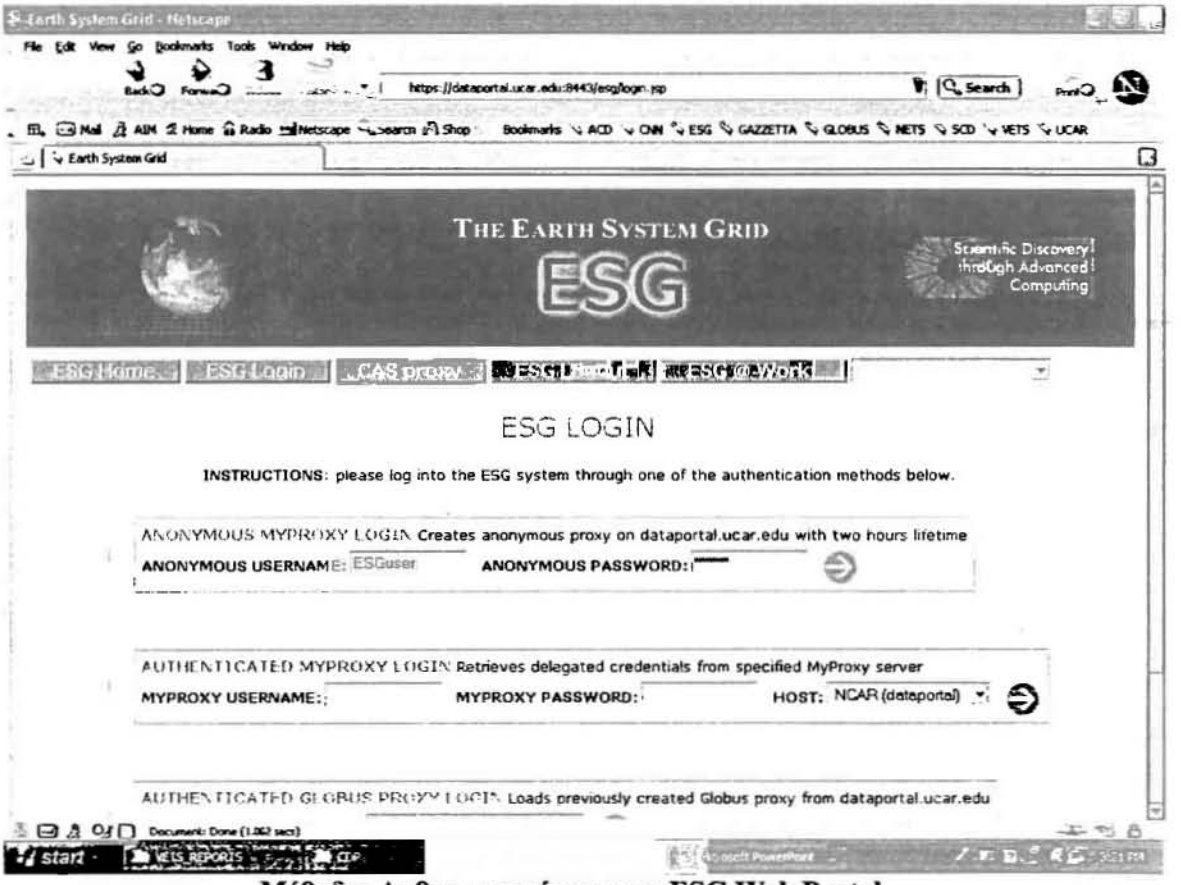
Επίσης , πολύ σημαντικό ρόλο στην ασφάλεια του ESG παίζει η υπηρεσία του GLOBUS CAS (Community Authorization Service) που φροντίζει για την ομαδική εξουσιοδότηση συγκεκριμένων κοινοτήτων. Όποιος δηλαδή είναι μέλος κάποιας εξουσιοδοτημένης κοινότητας, αυτόματα είναι και ο ίδιος εξουσιοδοτημένος. Αυτή η υπηρεσία σύμφωνα με το [53] παρέχεται από το ίδρυμα ANL που είναι υπεύθυνο για την υποστήριξη λειτουργιών του Globus.

Ακόμα, χρησιμοποιείται ο μηχανισμός ανάθεσης και διαχείρισης πόρων του Globus, το GRAM μέσω του οποίου ελέγχονται οι διαθέσιμοι πόροι του ESG και αναθέτονται στους αιτούντες πελάτες.
Όσο αφορά στην αυθεντικοποίηση και εξουσιοδότηση, το ESG χρησιμοποιεί το GSI του Globus. Πιο συγκεκριμένα, οι χρήστες αυθεντικοποιούνται μέσω των πιστοποιητικών πλέγματος που κατέχουν. Μάλιστα για την ευκολότερη διαχείρισή τους αλλά και την χρήση τους μέσω κάποιου απομακρυσμένου Web portal ,χρησιμοποιείται το σύστημα MyProxy.

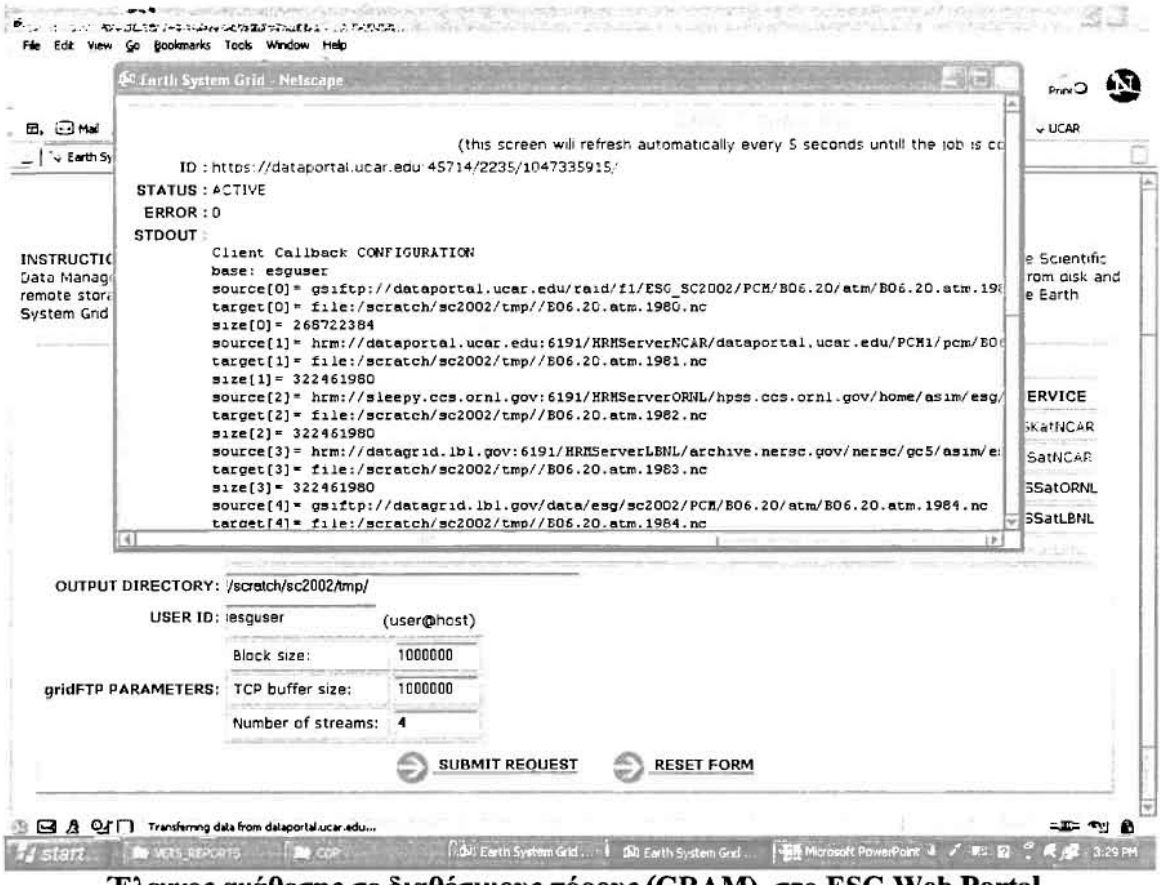
Τα βήματα της αυθεντικοποίησης ενός χρήστη του ESG είναι σύμφωνα με το [54] τα εξής:

1. Ο χρήστης μπαίνει στο Web portal όπου δίνει τα στοιχεία εγγραφής του για το σύστημα ESG
2. Γίνεται έλεγχος του χρήστη και των στοιχείων του και παράγεται από την αρχή πιστοποίησης το πιστοποιητικό του.
3. Το πιστοποιητικό του χρήστη αποθηκεύεται στον MyProxy Server. Σε αυτό το σημείο στέλνεται στο χρήση email που τον ειδοποιεί ότι ο λογαριασμός του στο ESG είναι ενεργοποιημένος και έτοιμος προς χρήση. Έτσι ο χρήστης θα μπορεί να χρησιμοποιεί το ESG portal.
4. Ο χρήστης την ίδια στιγμή, ή σε επόμενη είσοδό του στο σύστημα, δίνει το ID και το password
5. Με τη χρήση του ID/password του ο χρήστης μπορεί να αποκτήσει από το MyProxy Server το πιστοποιητικό πληρεξουσιότητας (proxy certificate)
6. Το Web portal χρησιμοποιεί το proxy certificate για την αυθεντικοποίηση του χρήστη στις ESG υπηρεσίες πλέγματος (Grid Services)

Παρακάτω δίνουμε κάποια screenshot του ESG Web Portal.



Μέθοδοι Αυθεντικοποίησης στο ESG Web Portal



Έλεγχος ανάθεσης σε διαθέσιμους πόρους (GRAM) στο ESG Web Portal

Συμπερασματικά, το ESG είναι πολύ φιλόδοξο project με πολύ σημαντικές πληροφορίες για τους επιστήμονες και φυσικά για τον πλανήτη. Παρατηρούμε ότι και σε αυτό το πλέγμα, η ασφάλεια αποτελεί βασικό συστατικό του, προκειμένου αυτό να λειτουργήσει καλύτερα.

5.5.5 E.G.E.E Project (Enabling Grids for Escience in Europe)

Το EGEE είναι ένα project δημιουργίας και εκμετάλλευσης της υποδομής πλέγματος για την υποστήριξη της επιστημονικής έρευνας κυρίως σε τομείς όπως φυσική υψηλής ενέργειας, παρέχοντας στους ερευνητές σε πανεπιστήμια και βιομηχανία, συνεχή πρόσβαση σε βασικούς υπολογιστικούς πόρους, ανεξάρτητα της γεωγραφικής τους θέσης [55]. Σε αυτό το project συμμετέχουν 70 ιδρύματα σε 27 χώρες, ενώνοντας τα τοπικά γεωγραφικώς πλέγματα, και υλοποιώντας έτσι ένα ενιαίο πανευρωπαϊκό πλέγμα.

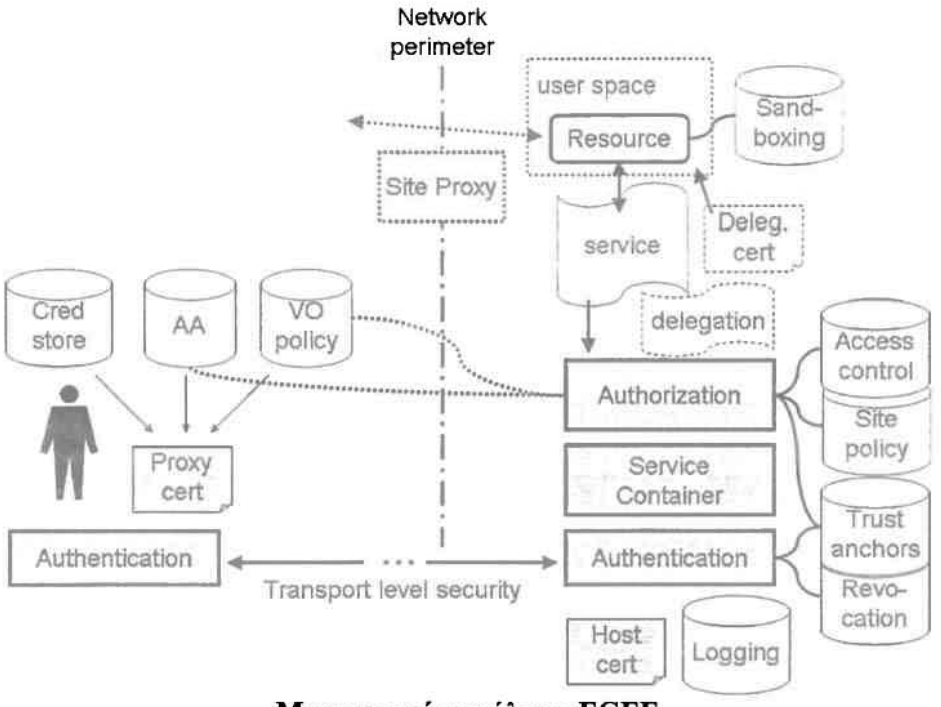
Το EGEE, σύμφωνα με το [55] προσφέρει:

- Απλοποιημένη πρόσβαση στους πόρους που χρειάζεται ο χρήστης όπου και αν βρίσκεται αυτός.
- Γρήγορη πρόσβαση σε πόρους μέσω 'έξυπνης' ανάθεσής τους σε χρήστες
- Βελτιωμένη παροχή υποστήριξης από εξειδικευμένο προσωπικό.

Εκτός της φυσικής υψηλής ενέργειας, το EGEE , 'τρέχει' και άλλου είδους εφαρμογές όπως βιο-πληροφορική, ιατρικές εφαρμογές, διαδραστικές προσομοιώσεις κτλ.

Μάλιστα , είναι δυνατό για το χρήστη να αναπτύξει την δική του επιστημονική εφαρμογή και να την καταθέσει στο EGEE. Η αρμόδια επιτροπή θα την εξετάσει βάσει κάποιων κριτηρίων , και εφόσον αυτά πληρούνται, τότε θα μπορεί να εκτελεστεί στο υπολογιστικό πλέγμα

5.5.5.1 Ασφάλεια EGEE



Μηχανισμοί ασφάλειας EGEE

Για την υλοποίηση της ασφάλειας στο συγκεκριμένο υπολογιστικό πλέγμα, χρησιμοποιούνται πολλοί μηχανισμοί του Globus όπως μηχανισμοί [56]:

- **Αυθεντικοποίησης:** Το μοντέλο που χρησιμοποιείται εδώ βασίζεται στην έννοια της τρίτης έμπιστης πηγής (third trust party), που αναλαμβάνει να αυθεντικοποιήσει χρήστη, πόρους ή υπηρεσίες. Επίσης χρησιμοποιούνται ψηφιακά πιστοποιητικά X.509v3

- **Καθολικής πιστοποίησης (Single Sign on):** Υποστηρίζεται μέσω proxy certificates και της κατάλληλης υποδομής αυθεντικοποίησης.

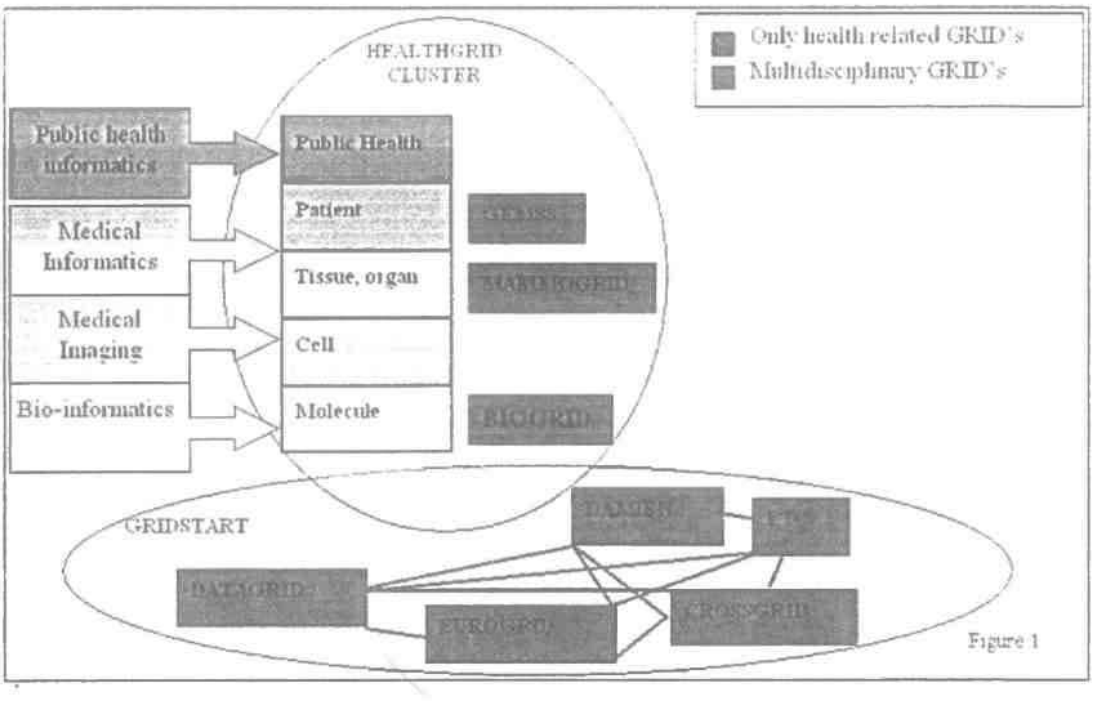
- **Πιστοποιητικά πληρεξουσιότητας (credential delegation):** Χρησιμεύει στην αυθεντικοποίηση, και βασίζεται σε μηχανισμούς GSI

- **Εξουσιοδότησης (authorization):** Χρησιμοποιείται το μοντέλο push στο οποίο , μια υπηρεσία εξουσιοδότησης, εκδίδει κάποια tokens. Ο χρήστης τα συλλέγει και τα δίνει σε όποιον πόρο του τα 'ζητά' προκειμένου να του δώσει πρόσβαση. Όσο αφορά στις υπηρεσίες εξουσιοδότησης, υπάρχουν 2 είδη .Η μία είναι η αρχή γνωρισμάτων που συσχετίζει ένα χρήστη με ένα σύνολο γνωρισμάτων, μέσω των οποίων θα αναγνωρίζεται το δικαίωμα του χρήστη για πρόσβαση και χρήση πόρων . Η άλλη υπηρεσία εξουσιοδότησης σχετίζεται με πολιτικές πρόσβασης , με βάση τις οποίες θα ελέγχεται το δικαίωμα του χρήστη για πρόσβαση .

- **Διαχείριση κλειδιών (Key management) :** υλοποίηση και μέσω MyProxy Server

Συμπερασματικά, παρατηρούμε ότι έχει δοθεί ιδιαίτερη σημασία , στην υλοποίηση της ασφάλειας, μέσω των μηχανισμών του GSI και του Globus. Συνεπώς οι ερευνητές μπορούν με ασφάλεια να 'τρέξουν' τις εφαρμογές τους στο πλέγμα του EGEE

5.5.6 HealthGrids



Πρόκειται για ένα ξεχωριστό τομέα εφαρμογής της υπολογιστικής πλέγματος στον χώρο της υγείας.
Ένας κατάλληλος ορισμός του healthGrid, σύμφωνα με το [57] είναι :

«Healthgrid, είναι η καινοτόμος χρήση της τεχνολογίας πληροφοριών για την υποστήριξη ευρείας πρόσβασης σε ταχεία, οικονομική και υψηλής ποιότητας υγειονομική περίθαλψη».

Πιο απλά, τα health Grid, είναι εξελιγμένα υπολογιστικά πλέγματα, που σχετίζονται στενά με την παροχή υπηρεσιών υγείας, είτε είναι ιατρικές έρευνες (μοριακές, βιο-ιατρικές κτλ) είτε επίλυση ιατρικών προβλημάτων-εφαρμογών που απαιτούν μεγάλη υπολογιστική ισχύ, είτε διακίνηση πληροφοριών ασθενών, μεταξύ ιατρικών μονάδων. Επιγραμματικά, τα πλέγματα healthGrid, παρέχουν υποστήριξη για [57] :

- Επεξεργασία ιατρικών εικόνων (π.χ εγκεφαλογράφημα, καρδιογράφημα...)
- Μοντελοποίηση του ανθρώπινου σώματος για προγραμματισμένη θεραπεία.
- Φαρμακευτική έρευνα και ανάπτυξη
- Γενετικές έρευνες
- Επεξεργασία ιατρικών δεδομένων , που βρίσκονται σε βάσεις δεδομένων. Π.χ ανάκληση και επεξεργασία ιατρικών εικόνων, με βάση το περιεχόμενο.

Τα συγκεκριμένα πλέγματα, έχουν πολύ μεγάλες απαιτήσεις σε ασφάλεια, καθώς είναι ανάγκη να τηρηθούν οι Ευρωπαϊκές και παγκόσμιες νομοθεσίες , καθότι πρόκειται ως επί το πλείστον για προσωπικά δεδομένα ασθενών. Αυτά τα δεδομένα συνήθως συλλέγονται από βάσεις δεδομένων ή αποθηκευτικούς πόρους , μεταδίδονται μέσω του Internet και επεξεργάζονται από τον πάροχο κάποιας Health Grid υπηρεσίας. Η Ευρωπαϊκή νομοθεσία π.χ θεσπίζει στη διάταξη 95/46 ορισμένους κανόνες για την προστασία και την ασφαλή επεξεργασία αυτών των προσωπικών δεδομένων που αφορούν ένα υπαρκτό φυσικό πρόσωπο
Συνεπώς ο σχεδιασμός , η υλοποίηση και εγκατάσταση ενός healthGrid, απαιτεί να δοθεί ιδιαίτερη βαρύτητα στον τομέα της ιδιωτικότητας και προστασίας των προσωπικών ιατρικών δεδομένων.
Ήδη υπάρχουν πολλά project healthgrid ανά τον κόσμο, ένα εκ των οποίο, θα δούμε αμέσως παρακάτω.

5.5.6.1 GEMSS (Grid-enabled Medical Simulation Services)

Το συγκεκριμένο project healthGrid προσφέρει υπηρεσίες επεξεργασίας ιατρικών εικόνων, μοντελοποίησης ανθρώπινου σώματος κτλ. Επίσης δίνει τη δυνατότητα σε ιατρικούς ερευνητές να έχουν πρόσβαση σε προχωρημένου επιπέδου προσομοιώσεις που σχετίζονται με ιατρικές εικόνες.

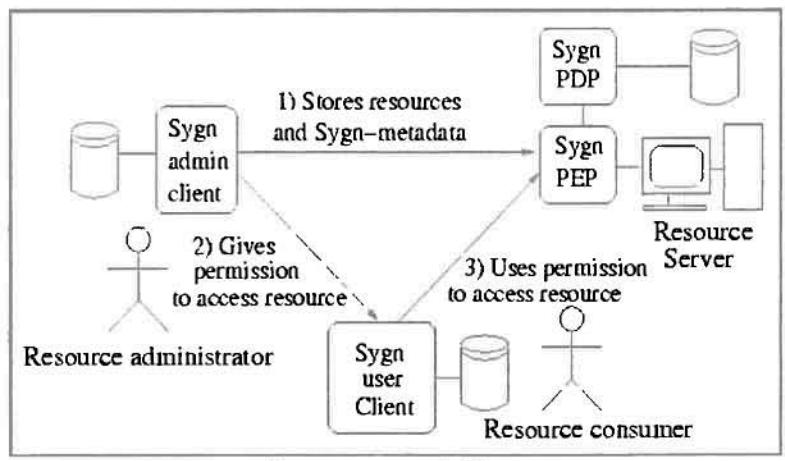
5.5.6.2 Ασφάλεια GEMSS

Το GEMSS υποστηρίζει μηχανισμούς ασφάλειας για την προστασία των προσωπικών δεδομένων, διασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα τους όπως επίσης και την αυθεντικοποίηση και εξουσιοδότηση αυτών που τα επεξεργάζονται [60].
Η υποδομή ασφάλειας του GEMSS βασίζεται στην υποδομή δημοσίου κλειδιού (PKI), υλοποιώντας τις αρχές πιστοποίησης, καταχώρησης και την τρίτη έμπιστη πηγή.
Επίσης, όλα τα πιστοποιητικά GEMSS, είναι του τύπου X.509 και χρησιμοποιούνται από ανθρώπους ή μηχανήματα για την αυθεντικοποίηση, ταυτοποίηση και εξουσιοδότηση τους κατά τις συναλλαγές μέσα στο πλέγμα.

Όσο αφορά στη επικοινωνία μέσα στο πλέγμα GEMSS, χρησιμοποιείται το πρωτόκολλο https προκειμένου να υπάρξει ένα ασφαλές κανάλι επικοινωνίας που θα εγγυάται την ακεραιότητα και ιδιωτικότητα των δεδομένων.
Ακόμα, τα δεδομένα, προτού μεταδοθούν μέσω του Internet, επεξεργάζονται από εξουσιοδοτημένα άτομα (επιστήμονες, οργανισμούς, εργαστήρια) με βάση κάποια συγκεκριμένη πολιτική ασφάλειας.

Τα πιστοποιητικά GEMSS, δεν χρησιμοποιούνται μόνο για αυθεντικοποίηση αλλά και για εξουσιοδότηση, καθώς μέσω αυτών σχετίζονται / αναθέτονται διάφορα δικαιώματα πρόσβασης σε συγκεκριμένους χρήστες ή εικονικούς οργανισμούς. Αν και ο κίνδυνος εισβολής στο σύστημα και στα προσωπικά δεδομένα , είναι γενικά μικρός, ωστόσο στην υποδομή ασφάλειας του GEMSS συμπεριλαμβάνεται και σύστημα ανίχνευσης εισβολέων (intrusion detection) προκειμένου να υπάρξει ακόμα υψηλότερο επίπεδο ασφάλειας στο πλέγμα. Συνεπώς τα αρχεία logs που παράγονται , μπορούν να χρησιμοποιηθούν σαν αποδείξεις για διάφορες ενέργειες που λαμβάνουν χώρα στο σύστημα.

Εκτός των παραδοσιακών τρόπων εξουσιοδότησης, χρησιμοποιείται συχνά και ένα άλλο σύστημα εξουσιοδότησης το Sygn [58]. Αυτό το σύστημα περιλαμβάνει Server ελέγχου πρόσβασης (PDP), ενώ χρησιμοποιεί μια γλώσσα αιτημάτων πρόσβασης που βασίζεται στην XML. Επίσης υποστηρίζει αποκεντρωμένη διαχείριση αδειών (decentralized permission management), όπως επίσης και πληρεξουσιότητα (delegation) , μέσω των κατάλληλων πιστοποιητικών.
Στην ακόλουθη εικόνα μπορούμε να δούμε τον τρόπο λειτουργίας αυτού του συστήματος.



Αρχιτεκτονική Sygn

Το πλεονέκτημα του συγκεκριμένου συστήματος είναι ότι επιτρέπει τη διαχείριση πολύπλοκων περιπτώσεων ελέγχου πρόσβασης σε health Grid.
Συμπερασματικά, η διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των ιατρικών δεδομένων σε περιβάλλοντα healthGrid όπως το GEMSS είναι ύψιστης σημασίας. Για αυτό χρησιμοποιούνται διάφοροι μηχανισμοί του GSI για την εκπλήρωση του υπάρχοντος νομοθετικού πλαισίου που αφορά τα απόρρητα ιατρικά δεδομένα ενός ασθενούς.

5.6 ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο συγκεκριμένο κεφάλαιο μελετήσαμε το Globus Toolkit. Περιγράψαμε τι είναι, καθώς και ένα πιθανό σενάριο χρήσης του στην καθημερινή, επιστημονική (κυρίως) ζωή.
Επίσης παρουσιάστηκαν τα θεμελιώδη συστατικά του όπως είναι το GRAM, MDS,Grid FTP, CAS ενώ καταγράψαμε και τις βασικές λειτουργίες που αυτά παρέχουν όπως είναι η καθολική πιστοποίηση, εξουσιοδότηση ,αυθεντικοποίηση, παρακολούθηση πόρων κτλ.
Επιπροσθέτως καταγράψαμε συνοπτικά την χρήση του μοντέλου ασφάλειας OGSA μέσα στο Globus Toolkit.

Γενικά το Globus Toolkit αποτελεί μια από τις πιο γνωστές προσεγγίσεις ασφάλειας για την υπολογιστική πλέγματος. Για το λόγο αυτό βρήκαμε ενδιαφέρον να καταγράψουμε τις προσεγγίσεις ασφάλειας γνωστών παγκοσμίως project υπολογιστικής πλέγματος, την μεθοδολογία τους καθώς και τα εργαλεία που χρησιμοποιούν προκειμένου να υλοποιήσουν ένα ασφαλές υπολογιστικό πλέγμα.

Συμπερασματικά, το Globus Toolkit είναι ένα σπουδαίο εργαλείο και η χρήση του συμβάλλει στην άρτια και ασφαλή λειτουργία ενός υπολογιστικού πλέγματος.

Επίσης, είδαμε περιληπτικά, κάποιες γνωστές υλοποιήσεις πλεγμάτων συστημάτων, διαφόρων ειδών (data-grids, υπολογιστικά, health Grids), από τις οποίες φαίνεται ξεκάθαρα η ολοένα και μεγαλύτερη χρησιμότητα της τεχνολογίας πλέγματος, και ιδιαίτερα της εφαρμογής μηχανισμών ασφάλειας σε αυτά, γεγονός που προσδίδει μεγαλύτερη αξιοπιστία στην λειτουργία τους.

ΜΕΡΟΣ 3: ΠΕΙΡΑΜΑΤΙΚΗ ΥΛΟΠΟΙΗΣΗ-ΣΥΜΠΕΡΑΣΜΑΤΑ

Κεφάλαιο 6: Περιβάλλον πειραματικής εφαρμογής ασφάλειας σε υπολογιστική πλέγματος (Grid Computing Security)

Κεφάλαιο 7: Συμπεράσματα

Κεφάλαιο 6: Περιβάλλον πειραματικής εφαρμογής ασφάλειας σε υπολογιστική πλέγματος (Grid Computing Security)

Περίληψη

Στο κεφάλαιο αυτό περιγράφουμε την πειραματική εφαρμογή της ασφάλειας σε συστήματα πλέγματος (Grid System). Αναλύεται η διαδικασία που ακολουθήθηκε για την εγκατάσταση ενός υποτυπώδους πλέγματος συστημάτων, όπως επίσης και η διαδικασία χρήσης των μηχανισμών ασφάλειας που παρέχονται μέσα σε αυτό το πακέτο.
Ακόμα, περιγράφονται τα τεχνολογικά χαρακτηριστικά της υλοποίησης καθώς και τα συμπεράσματα που αποκομίστηκαν από την συγκεκριμένη πειραματική εφαρμογή.

6.1 ΕΙΣΑΓΩΓΗ

Εκτός της θεωρητικής μελέτης του πακέτου Globus, στο συγκεκριμένο κεφάλαιο επιχειρούμε μια πειραματική εφαρμογή κάποιων μηχανισμών ασφάλειας στο Globus. Στόχος της πειραματικής αυτής εφαρμογής είναι να δούμε πως λειτουργούν αυτοί οι μηχανισμοί και πως διασφαλίζουν ένα αξιόπιστο υπολογιστικό πλέγμα.

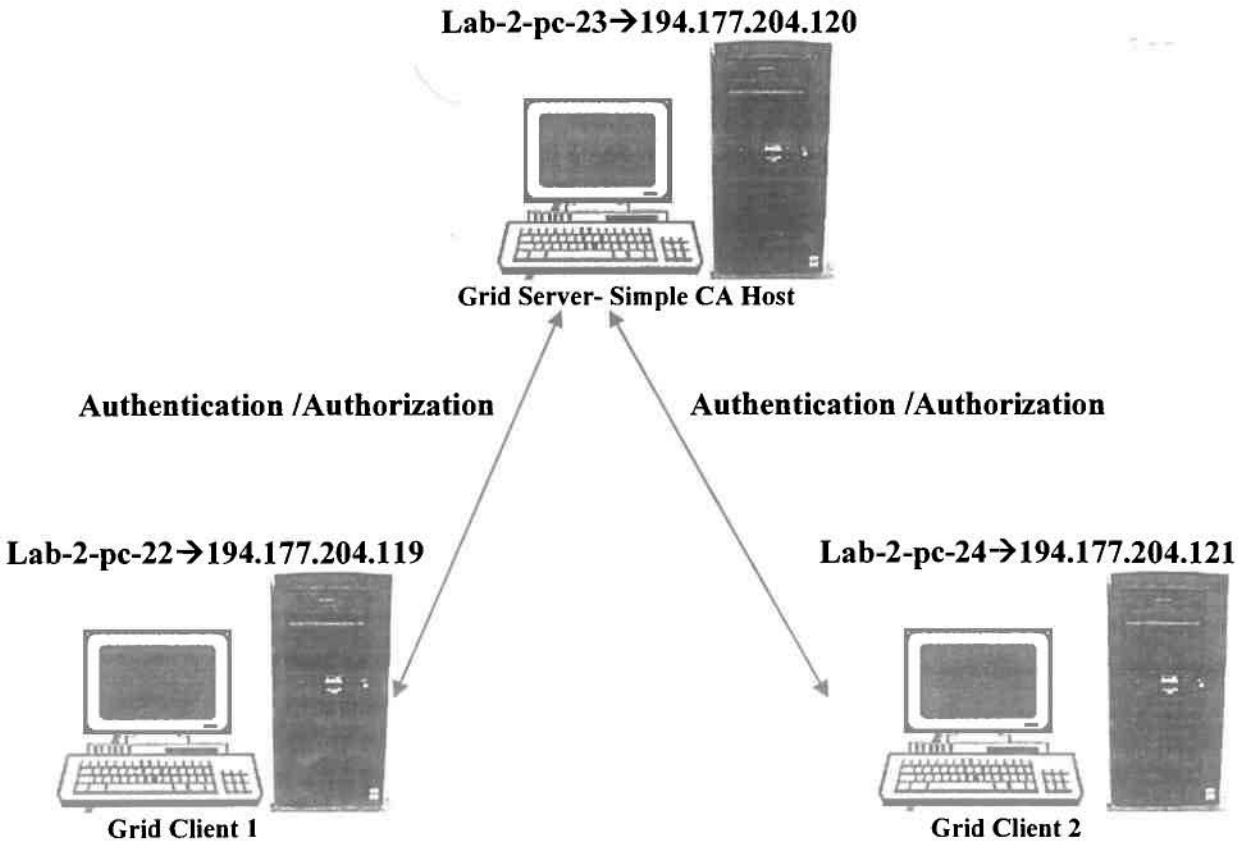
6.2 ΤΟ ΠΕΡΙΒΑΛΛΟΝ ΥΛΟΠΟΙΗΣΗΣ

Για την ανάπτυξη ενός πρότυπου πλέγματος συστημάτων , χρησιμοποιήθηκαν συστήματα υπολογιστών του εργαστηρίου του τμήματος Μηχανικών Η/Υ τηλεπικ.& δικτύων. Συγκεκριμένα έγινε χρήση 3 υπολογιστών του εργαστηρίου, με δικαιώματα root , με τα εξής τεχνικά χαρακτηριστικά:

- CPU: Intel Pentium 4 2.8GHz
- Μνήμη: 1GB RAM
- Σκληρό Δίσκο: 80GB
- Λειτουργικό Σύστημα : Linux , διανομή SuSe 9.2

Οι τρεις υπολογιστές ήταν συνδεδεμένοι στο τοπικό δίκτυο του τμήματος με DNS ονομασίες που σχετίζονται με το εργαστήριο π.χ ο κεντρικός υπολογιστής, που παίζει το ρόλο του Grid Server έχει ονομασία lab-2-pc-23.inf.uth.gr με IP 194.177.204.120.

6.2.1 Τοπολογία πλέγματος συστημάτων



6.3 ΣΕΝΑΡΙΟ ΧΡΗΣΗΣ

Το πλέγμα που εγκαταστήσαμε, ήταν για τυπική χρήση και μόνο. Για αυτό το λόγο, περιοριστήκαμε αποκλειστικά σε εγκατάσταση και χρήση command lines που παρέχονται από το ίδιο το πακέτο Globus, προκειμένου να μελετήσουμε τους μηχανισμούς ασφάλεια που υποστηρίζει.

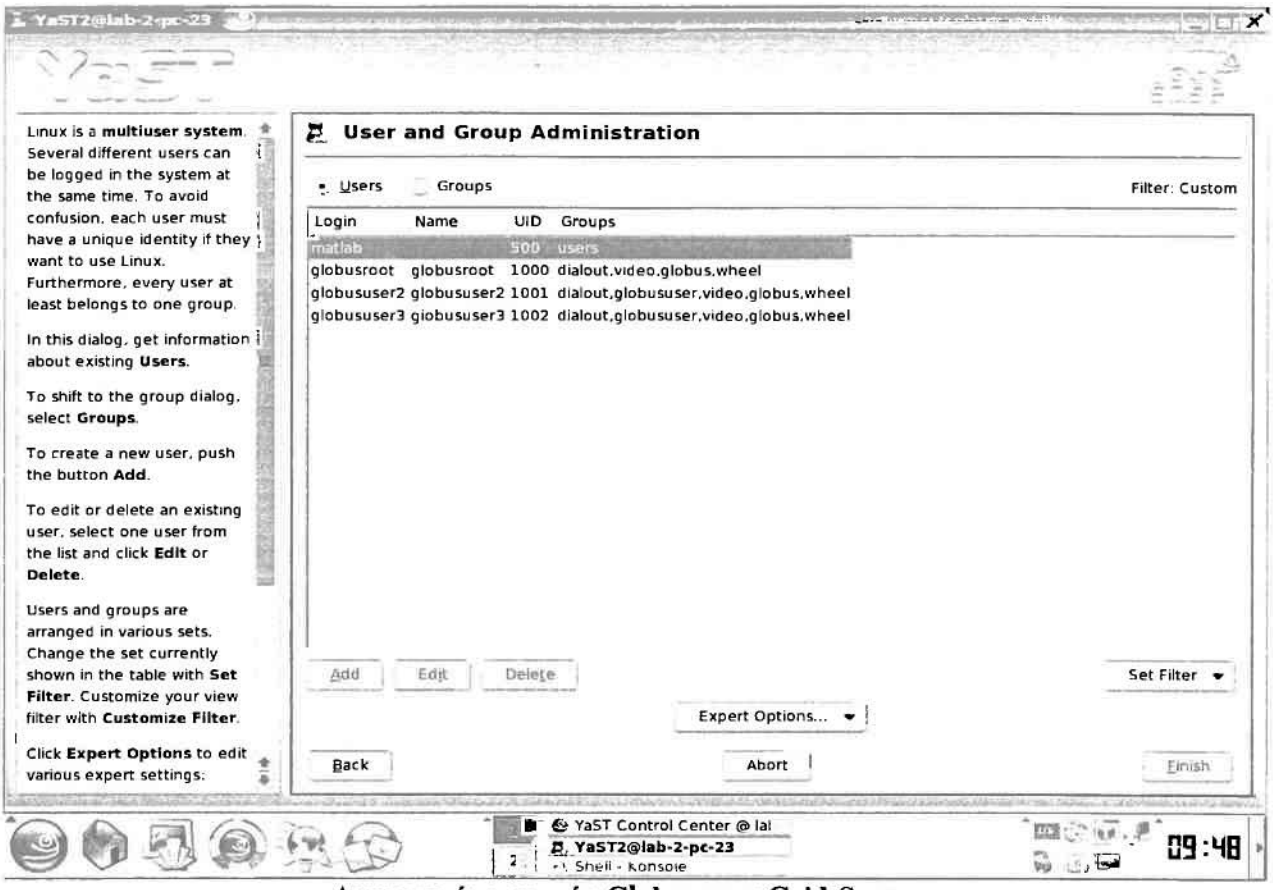
6.4 ΔΙΑΔΙΚΑΣΙΑ ΕΓΚΑΤΑΣΤΑΣΗΣ ΑΣΦΑΛΟΥΣ ΠΛΕΓΜΑΤΟΣ

Τα βήματα που ακολουθήσαμε για να εγκαταστήσουμε το globus στους υπολογιστές του εργαστηρίου είναι τα εξής:

- Δημιουργία, λογαριασμών χρήστη-διαχειριστή του globus (globusroot) και απλού χρήστη του globus (globususer2 , globususer3 για τον client 2, 3 αντίστοιχα)
- Εγκατάσταση του πακέτου Globus Toolkit version 4.0 και στα 3 μηχανήματα
- Εγκατάσταση στο μηχάνημα server (lab-2-pc-23) της αρχής πιστοποίησης του Globus (Simple CA)
- Εγκατάσταση του GSI στο κεντρικό μηχάνημα lab-2-pc-23.inf.uth.gr
- Έκδοση και υπογραφή πιστοποιητικού server (host certificate)
- Εγκατάσταση της ίδιας αρχής πιστοποίησης και στα μηχανήματα-clients
- Εγκατάσταση υπηρεσίας NFS στο πλέγμα
- Έκδοση και υπογραφή πιστοποιητικού χρήστη (user certificate) για τους 2 clients
- Δημιουργία πληρεξούσιου χρήστη (Grid-Proxy-Init)

6.4.1 Δημιουργία λογαριασμών χρηστών για τη χρήση του Globus

Σε κάθε σύστημα δημιουργήσαμε, σύμφωνα και με τις οδηγίες στο [62], ένα λογαριασμό χρήστη που θα διαχειρίζεται το globus (globusroot) και θα μπορεί να ξεκινά το globus container καθώς και άλλες υπηρεσίες (Grid Services).



Δημιουργία χρηστών Globus στον Grid-Server

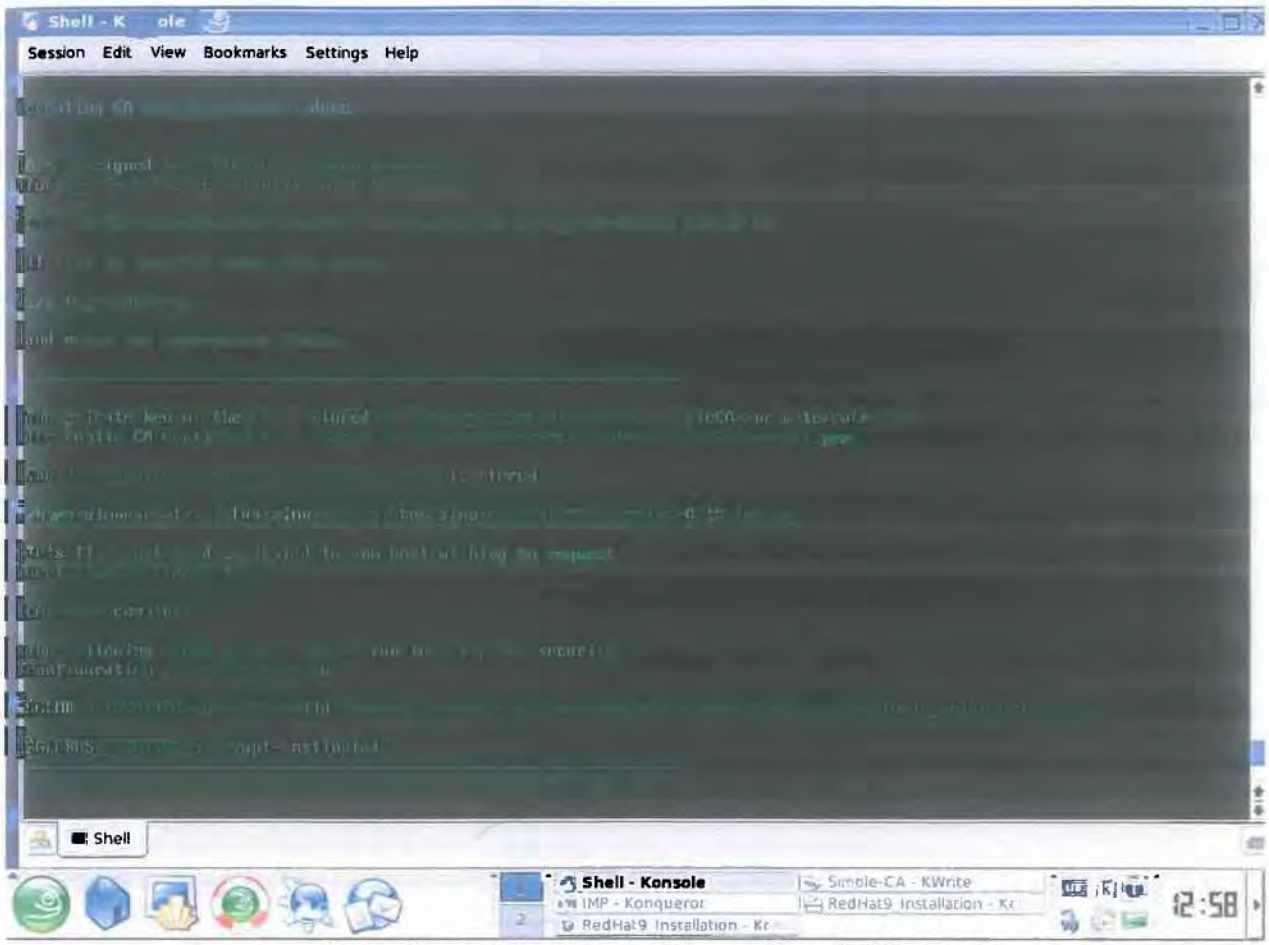
Επίσης, δημιουργήσαμε δύο ακόμη λογαριασμούς (globususer2, globususer3) που αντιστοιχούν σε απλούς χρήστες του πλέγματος, οι οποίοι θα αυθεντικοποιούνται και θα εξουσιοδοτούνται για να χρησιμοποιούν υπηρεσίες στο πλέγμα. Συγκεκριμένα αυτοί οι χρήστες αντιστοιχούν στα δύο μηχανήματα client 2 και 3 της τοπολογίας που είδαμε πιο πάνω.

6.4.2 Εγκατάσταση του Globus Toolkit 4.0

Για να εγκαταστήσουμε το Globus στα 3 μηχανήματα, ακολουθήσαμε τις οδηγίες του [62]. Συγκεκριμένα χρησιμοποιήσαμε την έκδοση του Globus για διανομές Redhat 9 Binary Installer (gt4.0.0-ia32-redhat9-binary-installer.tar.gz) η οποία λειτούργησε πολύ καλά με τη διανομή SuSe9.2, που χρησιμοποιήσαμε στα μηχανήματα του εργαστηρίου.

6.4.3 Εγκατάσταση της αρχής πιστοποίησης (Simple CA installation) στο κεντρικό μηχάνημα.

Αφού ολοκληρώθηκε επιτυχώς η εγκατάσταση του Globus στα 3 μηχανήματα, εγκαταστήσαμε στο κεντρικό μηχάνημα-Grid-Server την αρχή πιστοποίησης (Simple-CA) που ενσωματώνει το Globus , όπως φαίνεται στην παρακάτω εικόνα:



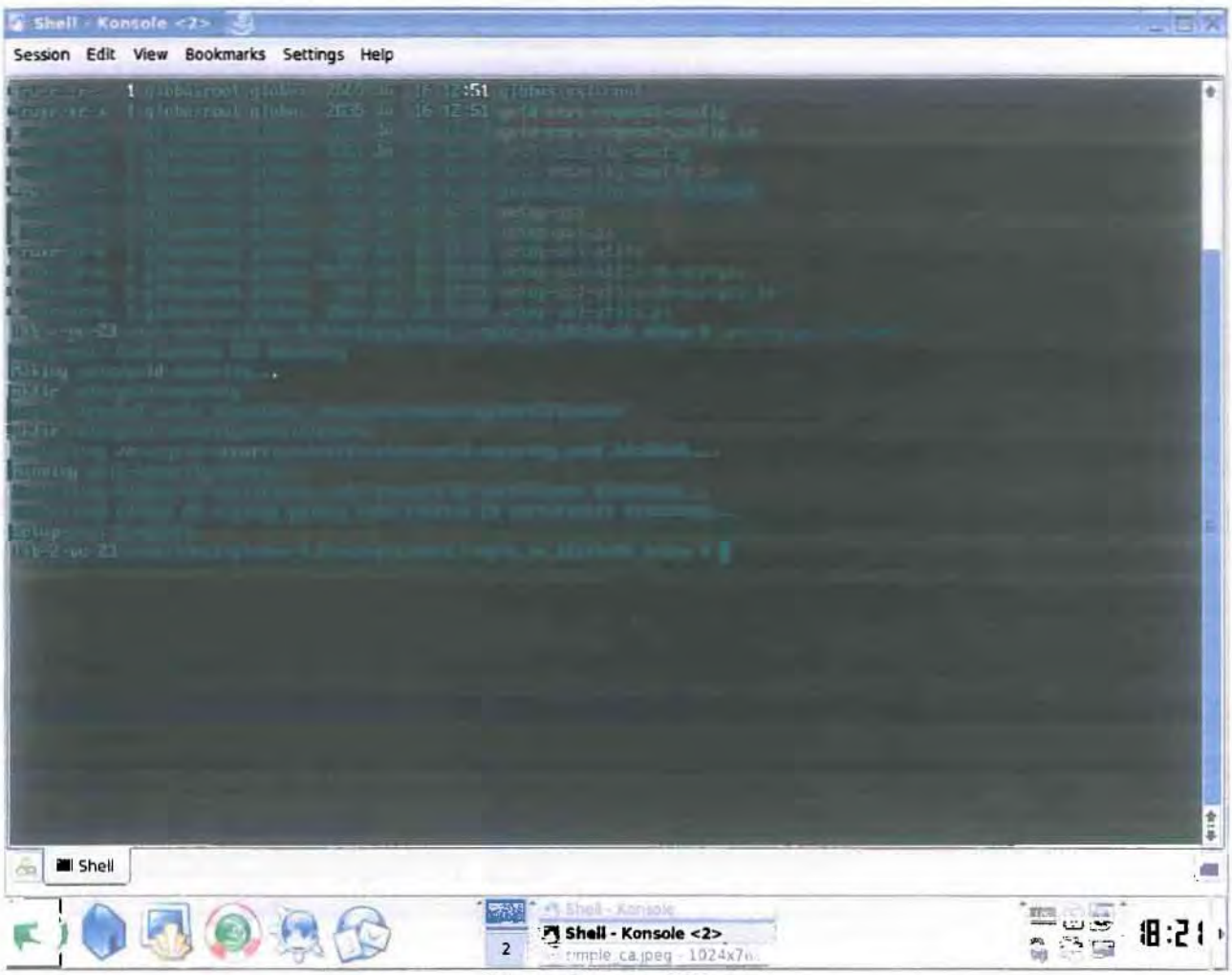
Εγκατάσταση Αρχή πιστοποίησης (Simple CA setup)

Συνεπώς, δημιουργήθηκε το πιστοποιητικό της αρχής πιστοποίησης, έχοντας σαν όνομα **simple-CA-lab-2-pc-23.inf.uth.gr**.Με αυτό το όνομα, η συγκεκριμένη αρχή πιστοποίησης θα είναι ξεχωριστή από οποιαδήποτε άλλη Simple CA , ενώ έτσι θα μπορούν να την αναγνωρίζουν οι χρήστες του πλέγματος που εγκαταστήσαμε.

Επίσης, γνωρίζουμε τον κατάλογο στον οποίο αποθηκεύτηκε το ιδιωτικό κλειδί της CA καθώς και το όλο πακέτο της CA (στο αρχείο tar.gz), το οποίο χρησιμοποιήσαμε αργότερα για να στήσουμε την simpleCA και στα άλλα μηχανήματα.

6.4.4 Εγκατάσταση του GSI στο κεντρικό μηχάνημα

Στο τέλος της εγκατάστασης της SimpleCA, εμφανίζεται μήνυμα που μας δίνει οδηγίες για την τελική διαμόρφωση και εγκατάσταση του GSI . Εκτελούμε σύμφωνα με το [62] την εντολή setup-gsi για να εγκαταστήσουμε το GSI στο κεντρικό μηχάνημα, όπως φαίνεται στην παρακάτω εικόνα:



Εγκατάσταση GSI

6.4.5 Έκδοση και υπογραφή πιστοποιητικού server (host certificate)

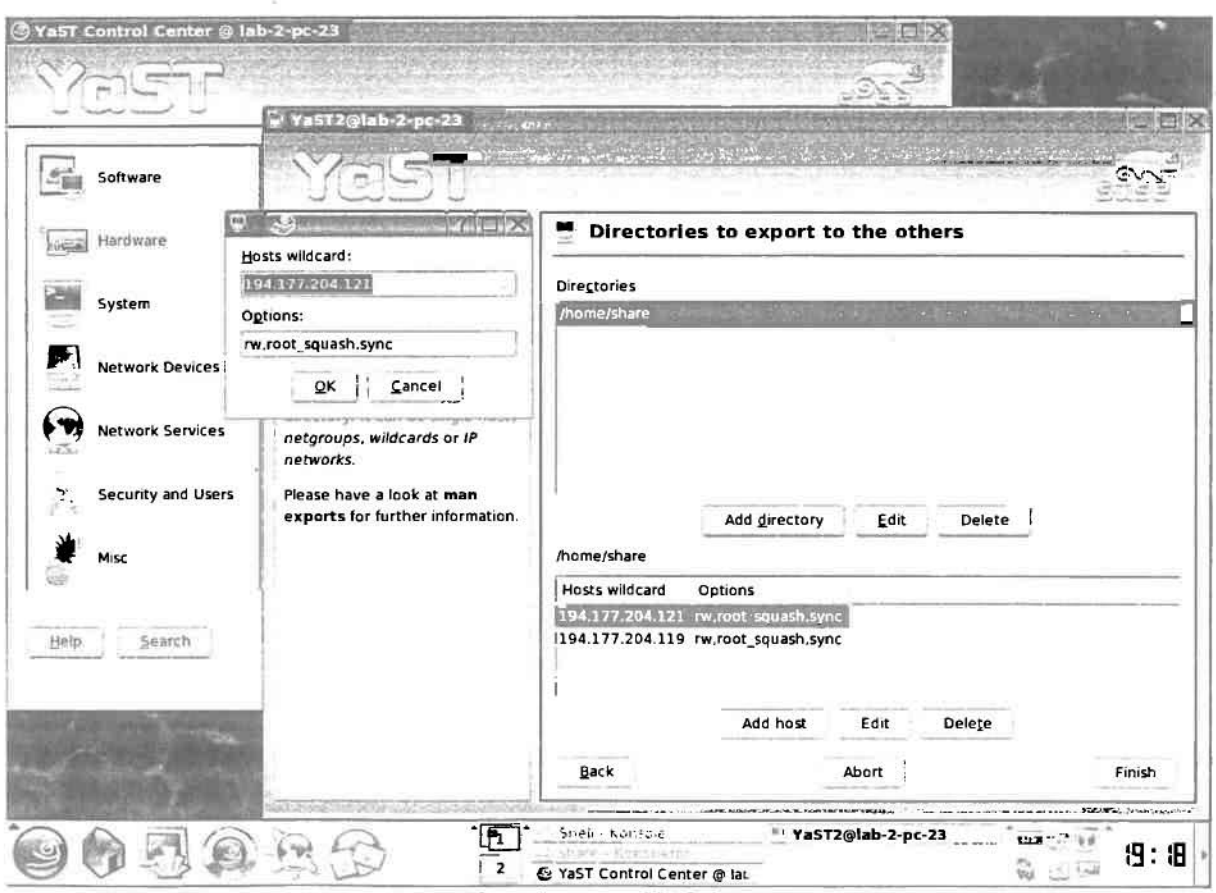
Προκειμένου το μηχάνημα-server να αποκτήσει πιστοποιητικό host, εκτελέσαμε από τη γραμμή εντολών του Linux, με δικαιώματα root την εντολή
grid-cert-request –host 194.177.204.120 (ή αντίστοιχα το domain-name στην περίπτωση μας το lab-2-pc-23.inf.uth.gr).
Έπειτα η αρμόδια αρχή πιστοποίησης (στην περίπτωσή μας η Simple-CA) υπογράφει το πιστοποιητικό που μόλις δημιουργήσαμε με την εντολή (με δικαιώματα **globusroot)**
cd /etc/grid-security/
./**grid-ca-sign** –in hostcert_request.pem –out hostsigned.pem
Έτσι δημιουργήθηκε ένα υπογεγραμμένο πιστοποιητικό για το host, με subject
/O=Grid/OU=GlobusTest/OU=simpleCA-lab-2-pc-23.inf.uth.gr/CN=host/ 194.177.204.120 .

6.4.6 Εγκατάσταση simpleCA στους Grid-clients

Προκειμένου να μπορέσουν τα 3 μηχανήματα, να επικοινωνήσουν μεταξύ τους μέσω του Globus , χρειάστηκε να γίνει μια συγκεκριμένη διαδικασία ([64]), κατά την οποία εγκαταστήσαμε στα μηχανήματα που είναι Grid-Clients το αρχείο **/globususer2/.globus/simpleCA/globus_simple_ca_HASH_setup-0.18.tar.gz** (στην περίπτωσή μας **hash=bfcf6cd6**) ώστε να αποδέχονται τα πιστοποιητικά που εκδίδει η συγκεκριμένη αρχή πιστοποίησης (SimpleCA) του κεντρικού μηχανήματος.
Αντιγράψαμε το αρχείο tar.gz στα μηχανήματα client και εκτελέσαμε την εντολή **$GLOBUS_location/sbin/gpt-build globus_simple_ca_HASH_setup-0.18.tar.gz gcc32dbg** για να εγκατασταθεί πλήρως η simpleCA.

6.4.7 Εγκατάσταση υπηρεσίας NFS στο πλέγμα

Για την αποστολή των αιτήσεων έκδοσης πιστοποιητικών (certificate requests) από τους clients και την υπογραφή τους από την αρχή πιστοποίησης (simple-CA) στο κεντρικό μηχάνημα, που παίζει το ρόλο του Grid-Server, κρίθηκε αναγκαίο να στηθεί μια υπηρεσία NFS προκειμένου να αποφευχθεί η αποστολή και λήψη άσκοπων email στη διεύθυνση της αρχής πιστοποίησης που τύχαινε να συμπίπτει με την προσωπική μου διεύθυνση email.
Έτσι στο κεντρικό μηχάνημα (lab-2-pc-23), μέσω του εργαλείου YAST που παρέχεται από τη διανομή SuSe για την διαμόρφωση του συστήματος , εκκινήσαμε την υπηρεσία NFS Server ,δημιουργώντας ένα κοινόχρηστο φάκελο (/home/share) τον οποίο μπορούν να βλέπουν οι 2 clients και στον οποίο με ίσα δικαιώματα χρήσης, θα μπορούν να αποθηκεύουν τα αρχεία αίτησης πιστοποιητικών και οποιοδήποτε άλλο αρχείο, προκειμένου να λαμβάνονται από το κεντρικό μηχάνημα στο οποίο εγκαταστάθηκε η αρχή πιστοποίησης.



Διαμόρφωση NFS Server

Όπως φαίνεται και στην εικόνα, η δήλωση των NFS-clients γίνεται μέσω των διευθύνσεων IP στους οποίους δίνονται δικαιώματα read-write.

Την ίδια διαδικασία ακολουθήσαμε και στα 2 Grid clients μηχανήματα όπου εκκινήσαμε την υπηρεσία NFS Client , δηλώσαμε την IP του NFS Server (στην περίπτωση μας η IP του Grid Server 194.177.204.120) , καθώς και το όνομα του φακέλου στο οποίο θα κάνουμε mount τον κοινόχρηστο φάκελο .
Μετά από αυτήν την διαδικασία είναι δυνατή η διαμοίραση αρχείων (κυρίως των πιστοποιητικών και των αντίστοιχων αιτημάτων τους) μεταξύ των κόμβων του πλέγματος μέσω δικτύου .

Δημιουργία NFS-Client

6.4.8 Έκδοση και υπογραφή πιστοποιητικού χρήστη (user certificate)

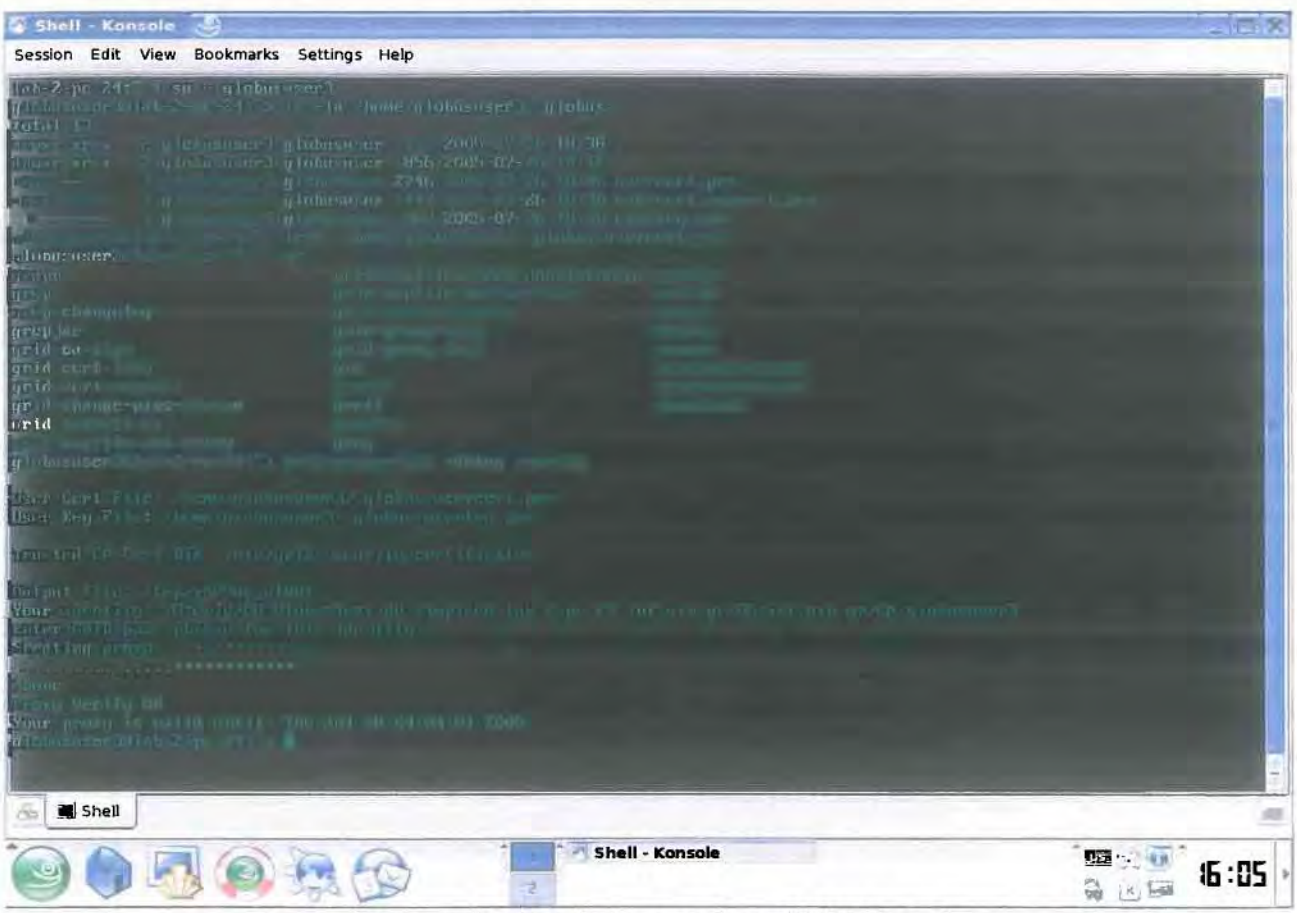
Αφού εγκαταστήσαμε την αρχή πιστοποίησης και στα 2 μηχανήματα-clients προχωρήσαμε στην αίτηση έκδοσης και υπογραφής πιστοποιητικού χρήστη από την αρμόδια αρχή πιστοποίησης (simple-CA). Χρησιμοποιήσαμε τον client-2 μέσω του λογαριασμού (globususer2) και ακολουθήσαμε τις οδηγίες που αναφέρονται στο [62] προκειμένου να παραχθεί στον τοπικό client ένα αρχείο αίτησης πιστοποιητικού χρήστη (user certificate request) .
Εκτελέσαμε τις εντολές που αναφέρονται στο [62] και εκδόθηκε τοπικά από το globus ένα πιστοποιητικό χρήστη με subject

/O=Grid/OU=GlobusTest/OU=simpleCA-lab-2-pc-23.inf.uth.gr/OU=inf.uth.gr/CN=globususer2

το οποίο και αποθηκεύσαμε στον κοινόχρηστο φάκελο /home/share .Έπειτα μέσω της υπηρεσίας NFS , το λάβαμε σαν globusroot χρήστες (στο κεντρικό μηχάνημα –server) για να το υπογράψουμε και να το ξαναστείλουμε μέσω NFS στον Grid-Client ,ώστε να το έχει υπογεγραμμένο από την αρμόδια αρχή πιστοποίησης.
Η ίδια ακριβώς διαδικασία ακολουθήθηκε και για το 3° μηχάνημα client του πλέγματος.

6.4.9 Δημιουργία πληρεξούσιου χρήστη (Grid-Proxy-Init)

Προκειμένου να ελεγχθεί η εγκυρότητα των πιστοποιητικών χρήστη, εκτελέσαμε σύμφωνα με το [62] την εντολή grid-proxy-init –debug –verify.
Η συγκεκριμένη εντολή εκτός από τον έλεγχο της εγκυρότητας των πιστοποιητικών, δημιουργεί proxy certificate το οποίο δρα εκ μέρους του χρήστη (delegation).



Δημιουργία πληρεξούσιου χρήστη (Grid- Proxy)

Δίνοντας διαδοχικά τις εντολές grid-cert-info –subject , και grid-proxy-info πήραμε τα παρακάτω στοιχεία:

```
/O=Grid/OU=GlobusTest/OU=simpleCA-lab-2-pc-
23.inf.uth.gr/OU=inf.uth.gr/CN=globususer3
subject  : /O=Grid/OU=GlobusTest/OU=simpleCA-lab-2-pc-
23.inf.uth.gr/OU=inf.uth.gr/CN=globususer3/CN=249882151
issuer   : /O=Grid/OU=GlobusTest/OU=simpleCA-lab-2-pc-
23.inf.uth.gr/OU=inf.uth.gr/CN=globususer3
identity : /O=Grid/OU=GlobusTest/OU=simpleCA-lab-2-pc-
23.inf.uth.gr/OU=inf.uth.gr/CN=globususer3
```

```
type      : Proxy draft (pre-RFC) compliant impersonation proxy
strength  : 512 bits
path      : /tmp/x509up_u1001
timeleft  : 11:23:50
```

Πράγματι τα πιστοποιητικά χρήστη που υπογράφηκαν από την SimpleCA στην πειραματική μας εφαρμογή ήταν απολύτως έγκυρα και η δημιουργία πληρεξούσιου χρήστη ήταν επιτυχημένη.

6.5 ΕΦΑΡΜΟΓΗ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ ΣΤΟ ΠΛΕΓΜΑ ΣΥΣΤΗΜΑΤΩΝ

Η εξουσιοδότηση στο Globus γίνεται μέσω αντιστοιχήσεως (mapping) του distinguished name(DN-με το οποίο ο χρήστης είναι ευρύτερα γνωστός στο πλέγμα), σε κάποιο τοπικό λογαριασμό στο μηχάνημα στο οποίο θα ήθελε ο χρήστης να εκτελέσει απομακρυσμένα κάποια εργασία.
Ενδεικτικά, στην περίπτωσή μας, για να εκτελέσει ο χρήστης globususer2 απομακρυσμένα μια εργασία στο κεντρικό μηχάνημα (Grid-Server), πρέπει να του απονέμουμε εξουσιοδότηση, με την εξής διαδικασία:

Στο αρχείο /etc/grid-security/grid-mapfile, δηλώνουμε την αντιστοίχιση μεταξύ του DN του globususer2 και του τοπικού(στο μηχάνημα που θα εκτελεστεί η εργασία) λογαριασμού εισάγοντας την παρακάτω σειρά:

"/O=Grid/OU=GlobusTest/OU=simpleCA-lab-2-pc-23.inf.uth.gr/OU=inf.uth.gr/ CN=globususer2 " globususer2

Η αντιστοίχηση (mapping) γίνεται από το DN που βρίσκεται μέσα στα εισαγωγικά στον τοπικό χρήστη globususer2, που δημιουργήσαμε στο κεντρικό μηχάνημα(§ 6.4.1).

Έπειτα στο απομακρυσμένο μηχάνημα Grid Client , που έχει ήδη ένα πιστοποιητικό χρήστη για τον globususer2 (§6.4.8), δημιουργούμε ένα προσωρινό πιστοποιητικό πληρεξουσιότητας (proxy certificate) μέσω της εντολής grid-proxy-init. Δεδομένου ,ότι αυτά έχουν μικρή διάρκεια ζωής (12 ώρες συνήθως-για λόγους ασφαλείας) θα πρέπει να ελέγχουμε ανά τακτά χρονικά διαστήματα την διάρκεια 'ζωής' τους μέσω της εντολής grid-proxy-info , η οποία όταν εκτελεστεί αναφέρει για πόσες ακόμη ώρες θα είναι έγκυρο το proxy –certificate(§6.4.9)

Αυτό το proxy certificate περιέχει το κατάλληλο DN ώστε να γίνει η εξουσιοδότηση και αντιστοίχηση μέσα στο grid-map file. Δίνοντας έπειτα την εντολή
globusrun-ws –submit https://194.177.204.120:8443/ -c /bin/date στο client-μηχάνημα, εκτελείται η εργασία μέσω Globus, στο μηχάνημα που του υποδεικνύουμε (IP) και τα αποτελέσματά εμφανίζονται και πάλι στο client
Όλα αυτά ισχύουν με την προϋπόθεση ότι θα γίνει σωστή εγκατάσταση , και το κυριότερο σωστή διαμόρφωση του globus ώστε να τρέχουν τα web services του.
Το Globus, εκτελώντας την εντολή globus-start-container, φορτώνει τα web services στον soap server (στην περίπτωσή μας τρέχει στο 194.177.204.120 και port 8443) τα οποία είναι απαραίτητα για τη σωστή λειτουργία του διαχειριστή ανάθεσης πόρων GRAM αλλά και του μηχανισμού MDS (Monitor Discovery Service) που είναι υπεύθυνος για την παρακολούθηση της κατάστασης των πόρων του πλέγματος.

Κεφάλαιο 7: ΣΥΜΠΕΡΑΣΜΑΤΑ- ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ

7.1 ΤΟ ΜΕΛΛΟΝ ΚΑΙ Η ΔΥΝΑΜΙΚΗ ΤΗΣ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ (Grid Computing)

Η υπολογιστική πλέγματος , και γενικότερα τα πλέγματα υπολογιστικών συστημάτων, αποτελούν μια ραγδαία αναπτυσσόμενη τεχνολογία κτίζοντας την υποδομή για την επόμενη γενιά υπολογιστικής . Σε τέτοια περιβάλλοντα , οι πόροι είναι ετερογενείς και γεωγραφικά κατανεμημένοι με διαφορετική διαθεσιμότητα και ποικίλες πολιτικές κοστολόγησης για διάφορους χρήστες.
Το εύρος των εφαρμογών της υπολογιστικής πλέγματος, αυξάνει καθημερινά, γεγονός που εν πολλοίς οφείλεται και στα ποικίλα χαρακτηριστικά της υπολογιστικής πλέγματος. (βλ. κεφ. 2)

Η διαχείριση των πόρων και η οργανωμένη λειτουργία των εφαρμογών σε ένα τέτοιο μεγάλο και κατανεμημένο περιβάλλουν κρύβει σίγουρα μεγάλη δυσκολία, καθώς η διαθεσιμότητα των πόρων και οι απαιτήσεις των χρηστών αλλάζουν δυναμικά. Ωστόσο τα πλεονεκτήματα που μπορούν να αποκομίσουν οι διάφορες εταιρείες και οργανισμοί, από τη χρήση αυτής της τεχνολογίας, είναι πραγματικά σπουδαία.

7.2 ΤΟ ΠΑΡΩΝ ΚΑΙ ΤΟ ΜΕΛΛΟΝ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΠΛΕΓΜΑΤΟΣ (Grid System Security)

Παρ' όλα αυτά , δεν αρκεί απλώς και μόνο η χρήση κάποιου εργαλείου δημιουργίας υπολογιστικού πλέγματος . Το μείζων ζήτημα, κατά τη διαμοίραση των πόρων μεταξύ των διάφορων οργανισμών (εικονικών και μη) , είναι η διατήρηση της ακεραιότητας των πόρων και η ασφαλής μεταφορά δεδομένων από κόμβο σε κόμβο.
Η ασφάλεια, κατά συνέπεια, υπήρξε βασικό ζήτημα έρευνας μέσα στην επιστημονική κοινότητα του Grid Computing, και ιδιαίτερα από τα μέσα της δεκαετίας του '90 όταν εθνικοί υπερ-υπολογιστικοί πόροι στις ΗΠΑ, συνδέθηκαν , δομώντας έτσι το πρώτο υπολογιστικό πλέγμα.

Οι μηχανισμοί ασφάλειας και τα πρωτόκολλα που έχουν αναπτυχθεί έρχονται αντιμέτωπα με διάφορες προκλήσεις που αφορούν την ασφάλεια του πλέγματος.
Σήμερα κεντρικό ρόλο στην ασφάλεια υπολογιστικής πλέγματος παίζουν τα ψηφιακά πιστοποιητικά, τα πιστοποιητικά πληρεξουσιότητας (proxy) και φυσικά τα εργαλεία αυθεντικοποίησης όπως είναι το GridFTP.
Ωστόσο καθώς οι έρευνες πάνω στο συγκεκριμένο τομέα, συνεχίζονται, οι Web υπηρεσίες συμμετέχουν ολοένα και περισσότερο σε Grid αρχιτεκτονικές ασφάλειας όπως είναι η OGSA (βλ. κεφ.3), η οποία θεωρείται το μέλλον του Grid Computing.

Η έρευνα πάνω στην ασφάλεια, αντιμετωπίζει τα βασικά λειτουργικά προβλήματα που συναντούν τα στελέχη εταιρειών πληροφορικής (και όχι μόνο), και τα οποία σχετίζονται με θέματα αυθεντικοποίησης, εξουσιοδότησης και πολιτικών ασφάλειας.

Τα αποτελέσματα από αυτές τις έρευνες είχαν ως αποτέλεσμα το GSI.
Όπως είδαμε στο 4° κεφάλαιο, το εκάστοτε μοντέλο ασφάλειας πλέγματος, βασίζεται σε ένα θεμελιώδες συστατικό την υποδομή ασφάλειας πλέγματος (ή πιο απλά GSI).
Το GSI λοιπόν παρέχει κάποιες πολύ σημαντικές δυνατότητες όπως είναι η εκχώρηση δικαιωμάτων που ανεβάζει το επίπεδο ασφάλειας, χωρίς να απαιτείται η συνεχής παρουσία του χρήστη.

Η έρευνα που πραγματοποιήθηκε στην παρούσα διπλωματική εργασία, δεν περιορίστηκε μόνο στη θεωρητική μελέτη όλων των παραπάνω , αλλά και στην ανάλυση, μελέτη (κεφ.5) και εγκατάσταση (κεφ.6) ενός από τα πιο γνωστά εργαλεία ανάπτυξης πλέγματος συστημάτων, του Globus.

Γενικά πρόκειται για ένα εργαλείο η τεχνολογία του οποίου βασίζεται σε υπηρεσίες (GRAM,GridFTP) ενώ η αρχιτεκτονική του στην έκδοση 4 (OGSA) στηρίζεται και αυτή με τη σειρά της σε υπηρεσίες Web. Στόχος του Globus είναι η εύκολη χρήση, αξιοπιστία, κλιμακωσιμότητα και η εύρυθμη λειτουργία του με πολλά διαφορετικά περιβάλλοντα, ανεξάρτητα της πλατφόρμας λειτουργικού συστήματος.
Αναμφισβήτητα, έχει πολλές δυνατότητες, για αυτό το χρησιμοποιούν πολλοί χρήστες, φορείς, οργανισμοί κτλ. Κάτι που φαίνεται άλλωστε και από τις πολλές υλοποιήσεις Grid Project (βλ. κεφ.5).

Συνοπτικά η έρευνα της διπλωματικής εργασίας ανέδειξε τις απαιτήσεις ασφάλειας των συστημάτων υπολογιστικής πλέγματος και με βάση τα αποτελέσματα της διπλωματικής εργασίας μας :

- Καθορίστηκαν τα **αντικείμενα ασφάλειας των Grid Systems**. Οι πόροι πρέπει να προστατεύονται με μηχανισμούς αυθεντικοποίησης και εξουσιοδότησης, όπως επίσης τα δεδομένα ,οι υπολογισμοί και τα πιστοποιητικά των χρηστών. Αυτό γίνεται και μέσω της κατάλληλης δομής της αρχιτεκτονικής πλέγματος που χωρίζεται σε διάφορα επίπεδα και βοηθά σε αυτόν τον τομέα.
  (βλ. Κεφ.2,3)

- Μελετήθηκαν συγκεκριμένες αρχιτεκτονικές πλέγματος όπως η **SOA, WSA** και ιδιαίτερα η αρχιτεκτονική **OGSA**. Τα χαρακτηριστικά της και οι μηχανισμοί που έχουν αναπτυχθεί για αυτήν , συμβάλλουν στην καλύτερη συνεργασία των ήδη υπαρχόντων τεχνολογιών ασφάλειας όπως η τεχνολογία ws-security με τεχνολογίες πλέγματος (βλ.κεφ 3).

- Διερευνήθηκε η χρήση των **πιστοποιητικών πληρεξουσιότητας** (proxy certificates). Μελετήσαμε πως λειτουργούν και πως επιτρέπουν στις οντότητες που συμμετέχουν στο υπολογιστικό πλέγμα, να εξουσιοδοτούν άλλες οντότητες έτσι ώστε να ενεργούν εκ μέρους τους (**delegation**), και είδαμε πράγματι πως συμβάλλει στην όλη εφαρμογή της ασφάλειας σε περιβάλλοντα πλέγματος.(βλ. Κεφ.4)

- Μελετήθηκαν οι μηχανισμοί **καθολικής πιστοποίησης (single sign-on)** και πολιτικές **ελέγχου πρόσβασης** σε συγκεκριμένους κόμβους του πλέγματος. Οι μηχανισμοί αυτοί πράγματι είναι αναγκαίοι για την εφαρμογή ασφάλειας σε υπολογιστικό πλέγμα , προστατεύοντας πόρους και δεδομένα. Ιδιαίτερη έμφαση δόθηκε στην μελέτη του GSI σαν βασική υποδομή ασφάλειας πλέγματος, καθώς και στον μηχανισμών του που έχουν να κάνουν με έλεγχο πρόσβασης βάσει των πιστοποιητικών των χρηστών και των ιδιοτήτων που αυτοί έχουν.

Επιπροσθέτως , η πειραματική μελέτη του 6ου κεφαλαίου, ανέδειξε μερικές μόνο από τις πολλές δυνατότητες του Globus, όπως η ασφαλής επικοινωνία των κόμβων, η εφαρμογή μηχανισμών εξουσιοδότησης και η εκχώρηση δικαιωμάτων (proxy delegation), αποδεικνύοντας ότι η χρήση του μπορεί πράγματι να συμβάλλει στην εξάπλωση της τεχνολογίας του Grid Computing, παρέχοντας παράλληλα μηχανισμούς ασφάλειας πλέγματος.

Όσο αφορά στις μελλοντικές εξελίξεις στο συγκεκριμένο χώρο της ασφάλειας πλέγματος, ήδη έχουν δρομολογηθεί από το παγκόσμιο φόρουμ πλέγματος (Global Grid Forum) ερευνητικές προσπάθειες που θα αφορούν στην ενσωμάτωση της ασφάλειας σε περιβάλλον πλέγματος που θα βασίζεται σε υπηρεσίες web. (grid-based Web services environment)
Υπάρχει στις μέρες μας, μια φυσική σύγκλιση μεταξύ υπηρεσιών πλέγματος και Web υπηρεσιών. Αυτή η σύγκλιση ολοένα και εντείνεται.
Συνεπώς και η ασφάλεια της αρχιτεκτονικής OGSA βασίζεται στην ασφάλεια των Web υπηρεσιών. Ωστόσο για να καλυφθούν πλήρως και οι απαιτήσεις των εικονικών οργανισμών απαιτούνται κάποιες μελλοντικές επεκτάσεις στους ήδη υπάρχοντας μηχανισμούς.

Μέλη της ομάδας ασφάλειας OGSA σχεδιάζουν να υλοποιήσουν μηχανισμούς ασφάλειας κάνοντας χρήση της ασφάλειας υπηρεσιών Web (WS-Security), η οποία με τη σειρά της υποστηρίζει μηχανισμούς που στηρίζονται στο πρωτόκολλο SOAP και μηχανισμούς κωδικοποίησης πιστοποιητικών X.509 .
Γενικά, είναι δύσκολο να προβλέψει κάποιος το μέλλον σε ένα επιστημονικό πεδίο όπως αυτό της πληροφορικής, όπου η τεχνολογικές πρόοδοι είναι ραγδαίες. Επίσης δεν είναι εύκολο να προβλέψεις ακριβώς τι θα συμβεί στο χώρο της ασφάλειας υπολογιστικής πλέγματος καθώς συνεχώς παρουσιάζονται καινούργιες ιδέες.

Όμως, διαφαίνονται ήδη κάποιες τάσεις όπως είναι η χρήση της Java, και φυσική η σύγκλιση υπηρεσιών Grid-Web.
Όσο αφορά στη χρήση της γλώσσας Java, αυτή συμβάλλει στην αντιμετώπιση διάφορων θεμάτων και ιδιαίτερα κάποιων απαιτήσεων των πλεγμάτων υπολογιστικής όπως είναι η ετερογένεια και η ασφάλεια.
Η χρήση υπηρεσιών που θα βασίζονται στο πρωτόκολλο CORBA θα βοηθήσει σημαντικά στην σχεδίαση και ανάπτυξη των μελλοντικών πλεγμάτων υπολογιστικής.

Συμπερασματικά, οτιδήποτε και αν συμβεί στο χώρο της πληροφορικής , είναι σχεδόν βέβαιο ότι η τεχνολογία υπολογιστικής πλέγματος, θα παίζει όλο και πιο σημαντικό ρόλο στα τεχνολογικά δρώμενα στον κόσμο. Πολλοί μάλιστα πιστεύουν ότι οι μελλοντικές υπολογιστικές ανάγκες του ανθρώπου θα ικανοποιούνται με τον ίδιο τρόπο που ικανοποιούνται οι αντίστοιχες για την ηλεκτρική ενέργεια.

Στην πραγματικότητα, το πλέγμα-Grid είναι ανάλογο με το ηλεκτρικό ρεύμα και αυτό που οραματίζονται οι ερευνητές για το πλέγμα είναι να παρέχει συνεπή, **ασφαλή** και χωρίς μεγάλο κόστος πρόσβαση στους πόρους ανεξαρτήτως που βρίσκονται αυτοί γεωγραφικά.

7.3 ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ ΤΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η παρούσα διπλωματική εργασία, ανέδειξε τις απαιτήσεις ασφάλειας των συστημάτων υπολογιστικού πλέγματος, δίνοντας ιδιαίτερη έμφαση σε μηχανισμούς αυθεντικοποίησης εξουσιοδότησης και ελέγχου πρόσβασης.
Λαμβάνοντας υπόψη την δυναμική που προκύπτει από τη χρήση και την μελλοντική εξάπλωση της τεχνολογίας Grid Computing, εκτιμούμε ότι διαγράφονται ορισμένες προοπτικές για περαιτέρω έρευνα πάνω στο θέμα της συγκεκριμένης διπλωματικής εργασίας:

7.3.1 HealthGrids

Ενδιαφέρον ζήτημα που χρήζει επιπλέον έρευνας, και ήδη παγκοσμίως γίνονται πολλές προσπάθειες , είναι αυτός της ανάπτυξης «**ασφαλών** πλεγμάτων συστημάτων Υγείας» ή αλλιώς health Grids.
Τα ιατρικά πληροφοριακά συστήματα αποθηκεύουν ,επεξεργάζονται και μεταδίδουν ευαίσθητα προσωπικά δεδομένα. Αυτό δημιουργεί την ανάγκη για 'αυστηρή' εμπιστευτικότητα και εφαρμογή πολιτικής προστασίας τους. Αυτές οι απαιτήσεις δεν έχουν ικανοποιηθεί πλήρως από τις υπάρχουσες ως τώρα λύσεις της τεχνολογίας πλέγματος.

Σε τομείς όπως αυτόν της φυσικής υψηλής ενέργειας, τα στοιχειώδη σωματίδια που μελετώνται, δεν έχουν ανάγκη από ιδιωτικότητα. Το ίδιο συμβαίνει και με τους φυσικούς επιστήμονες που δεν απαιτούν προστασία της πληροφορίας τους από άλλους συναδέλφους τους.

Γίνεται λοιπόν αντιληπτή η ανάγκη για έρευνα σε μηχανισμούς ασφάλειας που θα περιφρουρήσουν το περιβάλλον ενός πλέγματος συστημάτων Υγείας. Και αυτό γιατί τα ιατρικά δεδομένα είναι πολύ ευαίσθητα και η μετάδοσή τους είναι επιρρεπής σε καταστροφή, κλοπή και αλλοίωση. Μάλιστα πολλές φορές έχουν έρθει στη δημοσιότητα τέτοια περιστατικά, αποδεικνύοντας το υπαρκτό του κινδύνου. Ήδη υπάρχουν μηχανισμοί αυθεντικοποίησης και εξουσιοδότησης που όμως βρίσκονται σε πρώιμο στάδιο ανάπτυξης και αποτελεσματικότητας. Είναι σημαντικό να κατανοήσουμε ότι η περαιτέρω ανάπτυξη της τεχνολογίας ασφάλειας, είναι το κλειδί για την αποδοχή στην τεχνολογική (και όχι μόνο) κοινωνία ,της έννοιας του HealthGrid.

Ο συγκεκριμένος 'επιστημονικός' χώρος παρέχει πολλά πεδία έρευνας όπως έρευνα σε πρωτόκολλα ασφάλειας Web Security, πολιτικές πρόσβασης και γλώσσες εξουσιοδότησης κατάλληλες για τέτοια περιβάλλοντα. Επίσης μηχανισμοί ασφάλειας όπως αποθήκευσης αντιγράφων δεδομένων (data replication).

Τέτοιοι μηχανισμοί , αντιγράφουν τα δεδομένα σε ένα πόρο (μνήμη, δίσκο κτλ) προκειμένου να αποφύγουν καθυστερήσεις σε αναγκαίες μελλοντικές μεταδόσεις τους. Ωστόσο κάτι τέτοιο δεν επιτρέπεται σε περιπτώσεις ιατρικών δεδομένων, και έτσι απαιτείται προσαρμογή του συγκεκριμένου μηχανισμού σε ιατρικά περιβάλλοντα healthGrid.

7.3.2 Έρευνα και ανάπτυξη μηχανισμών δημιουργίας ασφαλών Web-based Grid Portals

Στο κεφάλαιο 4 είδαμε μια νέα τεχνολογία MyProxy που έχει αναπτυχθεί για περιβάλλοντα πλεγμάτων συστημάτων. Σκοπός αυτής της τεχνολογίας, , είναι η ασφαλής αποθήκευση πιστοποιητικών αλλά και η δυναμική ανάκλησή τους από απομακρυσμένους υπολογιστές . Οπωσδήποτε τέτοιοι μηχανισμοί συμβάλλουν στη δημιουργία ασφαλών πλεγμάτων υπολογιστικής, αλλά όπως είδαμε και παραπάνω, τα health Grids έχουν πολύ υψηλότερες απαιτήσεις ασφάλειας από τα άλλα είδη πλεγμάτων.

Εκεί που πιστεύουμε ότι μπορεί και πρέπει να γίνει περαιτέρω έρευνα στο συγκεκριμένο ή σε ανάλογα με το MyProxy συστήματα, είναι στους μηχανισμούς εκχώρησης –αποθήκευσης του πιστοποιητικού (credential delegation to repository), όπου οι μηχανισμοί αυτοί πρέπει να διασφαλίζουν στον μέγιστο βαθμό ότι η ανάκληση ή αποθήκευση γίνεται από νόμιμους χρήστες και όχι από παράνομους. Η συγκεκριμένη τεχνολογία χρησιμοποιεί ευρέως web-based grid portals προκειμένου ο χρήστης να μπορεί να μπαίνει από οπουδήποτε και να επεξεργάζεται τα πιστοποιητικά του.

Τα Grid-Portals επιτρέπουν (βλ. Κεφ. 4- MyProxy) στο χρήστη να πραγματοποιεί τις εργασίες στο πλέγμα και απομακρυσμένα μέσω standard web browser της αγοράς.
Υπάρχουν ωστόσο απαιτήσεις για την λειτουργία των συγκεκριμένων portals τόσο για τη λειτουργικότητά τους όσο και για το επίπεδο της ασφάλειας, στο οποίο εστιάζουμε περισσότερο την προσοχή μας.

Ενδεικτικά μερικές απαιτήσεις που απαιτούν περαιτέρω έρευνα είναι οι παρακάτω:

- Οι χρήστες πρέπει να μπορούν να χρησιμοποιούν οποιοδήποτε web browser της αγοράς χωρίς κάποιο πρόβλημα προκειμένου να μπορούν να έχουν πρόσβαση στο πλέγμα.
- Οι χρήστες πρέπει να μπορούν να χρησιμοποιούν τα πιστοποιητικά τους όπως θέλουν οι ίδιοι κατά νόμιμο φυσικά τρόπο, ακόμα και αν είναι σε απομακρυσμένο υπολογιστή.
- Οι web browsers από μόνοι τους δεν υποστηρίζουν εξουσιοδότηση μέσω πιστοποιητικών. Έτσι πρέπει να αναπτυχθούν μηχανισμοί που θα μπορούν να ικανοποιούν την συγκεκριμένη απαίτηση , χωρίς κατ'ανάγκη να αποθηκεύεται προσωρινά ένα γνήσιο πιστοποιητικό του χρήστη στον απομακρυσμένο υπολογιστή κάτι το οποίο πιθανώς να έκρυβε κινδύνους ασφάλειας για το πιστοποιητικό.
- Έρευνας χρήζει και η διαδικασία συνεχόμενης πρόσβασης για αυθεντικοποίηση (log in) , καθώς θα ήταν επιθυμητό αντί ο χρήστης συνεχώς να αυθεντικοποιεί τον εαυτό του από όπου και αν συνδέεται, να μπορούσαν τα πιστοποιητικά να ήταν διαθέσιμα παντού και με ασφάλεια.

- Τα portal πρέπει να χρησιμοποιούν το ίδιο πιστοποιητικό χρήστη χωρίς να αναγκάζεται το σύστημα να εκδίδει νέες ταυτότητες (identities) για τον ίδιο χρήστη.
- Πολλαπλά Grid portals πρέπει να μπορούν να χρησιμοποιούν ένα σύστημα αποθήκευσης πιστοποιητικών (π.χ MyProxy) και το αντίθετο δηλαδή ένα portal να μπορεί να συνδέεται με πολλαπλά συστήματα τύπου MyProxy

Σημαντικό ρόλο μπορεί να παίξει και **η χρήση της Java** η οποία από τη φύση της είναι ανεξάρτητη πλατφόρμας λογισμικού και πιστεύουμε ότι μπορεί να χρησιμεύσει στην ανάπτυξη τέτοιων portals
Δεδομένης λοιπόν της χρησιμότητας των web-based Grid portals, η αυξανόμενη ανάγκη για ασφαλή πρόσβαση και επεξεργασία των πιστοποιητικών του χρήστη, καθιστά αναγκαία την έρευνα σε αυτό το τομέα.

7.3.3 G-Commerce: Ανάπτυξη grid μηχανισμών με εφαρμογή σε εταιρείες E-commerce

Οι εταιρείες συνεχώς ψάχνουν τρόπους για να μειώσουν τα έξοδά τους, τα οποία περιλαμβάνουν και τα έξοδα για αγορά καινούργιου hardware (servers, clusters). Θέλοντας να αποφύγουν την αγορά γρηγορότερων συστημάτων, κάθε χρόνο, στρέφονται σιγά –σιγά στην τεχνολογία Grid Computing.
Η συγκεκριμένη τεχνολογία μπορεί να εκμεταλλευτεί τα συστήματα των εταιρειών που δεν χρησιμοποιούνται πολύ. Είναι γεγονός ότι πολλές εταιρείες αγοράζουν υπολογιστές για συγκεκριμένες εφαρμογές όπως συστήματα διαχείρισης σχέσεων πελατών (γνωστά και σαν CRM), ERP, κτλ. Σε μερικές περιπτώσεις ωστόσο , αυτές οι εφαρμογές έχουν κάποιες εναλλαγές στις απαιτήσεις τους σε επεξεργαστική ισχύ χρησιμοποιώντας άλλοτε την CPU του συστήματος πολύ και άλλοτε λίγο. Σαν αποτέλεσμα τα συστήματα αυτά μπορούν να λειτουργήσουν μόνο στο 5% των πραγματικών τους δυνατοτήτων, καθώς στον υπόλοιπο χρόνο παραμένουν 'ανενεργά'.
Πρέπει να γίνουν λοιπόν έρευνες που θα εστιάζουν στην **σχεδίαση ασφαλών εφαρμογών Grid Computing** που θα εκμεταλλεύονται αυτά τα 'αχρησιμοποίητα κενά' των παραπάνω συστημάτων και να μετακινήσουν υπολογιστικό φόρτο άλλων υπερ-χρησιμοποιήσιμων συστημάτων σε αυτά . Εφαρμογές που θα μπορούν να διαιρούν τον υπολογιστικό φόρτο σε μικρότερα κομμάτια να τα αναθέτουν σε κατάλληλους πόρους και έπειτα να ανασυνθέτουν τα αποτελέσματα. Στο συγκεκριμένο τομέα έρευνας υπεισέρχονται διάφορα ζητήματα και ένα από αυτά έχει να κάνει με το γεγονός ότι την δεδομένη χρονική στιγμή οι εφαρμογές Grid Computing δεν είναι σε θέση να αποφασίζουν από μόνες τους πότε και αν πρέπει να εκτελέσουν μια εργασία τα αποτελέσματα της οποίας σχετίζονται με άλλους υπολογισμούς άλλων εργασιών.
Ένα χαρακτηριστικό παράδειγμα είναι το εξής:
Μια εταιρεία έχει ένα web site και εμπορεύεται ολοκληρωμένα συστήματα Η/Υ. Έχει διάφορους συνεργάτες π.χ για την CPU, την motherboard και γενικά όλα τα τμήματα του Η/Υ. Ο χρήστης θα μπορεί να μπαίνει στο Internet και να επιλέγει την σύνθεση του Η/Υ με τα δικά του χαρακτηριστικά, συγκεκριμένη μάρκα CPU που θα μπορεί να δουλεύει με συγκεκριμένη motherboard . Οι επιλογές του χρήστη θα μπορούν να διαμοιράζονται μέσω της τεχνολογίας Grid Computing στους συνεργάτες .
Τα αποτελέσματα που θα επιστρέφουν στο κεντρικό site πρέπει μέσω κατάλληλης εφαρμογής να ελέγχονται για τη συμβατότητα των επιμέρους τμημάτων του υπολογιστή και έπειτα να δίνεται η δυνατότητα στο χρήστη να προβεί σε αγορά του συστήματος.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] **Fundamentals of Grid Computing.** IBM redbooks 2002 V. Berstis.

[2] **The Anatomy of the Grid : Enabling Scalable Virtual Organizations**. 2000 I. Foster;C. Kesselman;S. Tuecke.

[3] http://www.byteandswitch.com Architecture of Grid

[4] http://www.grid.org/about/gc/evolution.htm

[5] **Grids:The Top 10 Questions.ppt** Jeniffer M. Schopf, Jan 14, 2005

[6] **The Top 10 Questions.ppt, Possibilities & Limitations of Using Grid Computing in Collaborative Environments**, Rami Madhoun Systems and Computer Engineering Dept.Carleton University

[7] http://gridcafe.web.cern.ch/gridcafe/index.html

[8] **Distributed Computing Research Issues in Grid Computing**, Henri Casanova, Dept. of Computer Science, ACM SIGACT, July 29, 2002

[9] **The Physiology of the Grid**, Ian Foster, Carl Kesselman , Jeffrey M., Nick Steven Tuecke

[10] **Computational Grids** , Ian Foster,

[11] **What is the Grid** – A three point checklist, Ian Foster, July 20, 2002

[12] **Grids and Grid technology for wide area distributed computing**, Mark Baker, Rajkumar Buyya , Domenico Laforentza , 2002

[13] http://www.ibm.com/developerworks/grid/

[14] http://www.grid.org/

[15] **middleware** , Ian Foster, Argonne National Laboratory The University of Chicago

[16] **The evolution of Grid Computing, architecture and grid adoption models,** Joseph, M. Ernest, C. Fellenstein

[17] http://setiathome.berkelev.edu/learnmore.html

[18] **Grid Security.ppt :issues, challenges, approaches**, Li Tievan, Institute for InfoComm, 2003

[19] **Grid Computing , Possibilities & Limitations of Using Grid Computing in Collaborative Environments**, Rami Madhoun Systems and Computer Engineering Dept. Carleton University

[20] **Security for Grid based Computing Systems Issues and Challenges**, Elisa Bertino, Bruno Crispo, James Joshi, Wengliang Du, Ravi Sandhu

[21] **A Security Architecture for Computational Grids**, Ian Foster, Carl Kesselman, Gene tsudik, Steven Tuecke

[22] **Security for Grid Services,** Von Welch Frank Siebenlist Ian Foster John Bresnahan Karl Czajkowski Jarek Gawor Carl Kesselman Sam Meder Laura Pearlman Steven Tuecke

[23] **Security Challenges in Supporting Grid Computing and Collaboration** Mary R. Thompson, Keith R. Jackson Distributed Systems Department – LBNL

[24] **Grid security**: state of the art, IBM, Anne Zieger Chief analyst,

PeerToPeerSource.comAugust 2003

[25] **Security Architecture for Open Grid Services**. OGSASec-ggf.pdf

[26] **OGSA Security Roadmap,**Siebenlist F, Von Welch, Steven Tuecke, Ian Foster, Nataraj Nagaratnam, IBM, Philippe Janson, IBM, John Dayka, IBM, Anthony Nadalin, IBM July, 2002

[27] **Research on Security Architecture and Security Policy of grid Computing System.ppt** , Wang Yufeng, Yang Shoubao, Zhao.Xiaochun, CHEN, Xin University of Science and technology of China

[28] **Fine-Grain Authorization Policies in the GRID**: Design and Implementation.pdf, K. Keahey Argonne National Lab, Argonne, IL, USA V. Welch University of Chicago, Chicago, IL, USA S. Lang Argonne National Lab, Argonne, IL, USA B. Liu University of Houston, Houston, TX, USA S. Meder University of Chicago, Chicago, IL, USA

[29] **Toward Exlpicit Policy Management for Virtual Organizations**, Glenn Wasson, Marty Humphrey

[30] **Security Mechanisms in Grid Environment**, Adrian Bagala, Roland Bott

[31] **Grid Security Infrastructure The Globus project**, Argonne National Laboratory USC Information Sciences Instutute http://www.globus.org/, 04 –Security.ppt

[32] **Introduction to Grid Computing with Globus**, IBM redbooks 2003

[33] **Security in GRID**, gct11.ppt

[34] **X.509 Proxy Certificates for Dynamic Delegation**, Ian Foster, Jarek Gawor, Carl Kesselman, Sam Meder, Olle Mulmo, Laura Perlman, Frank Siebenlist, Steven Tuecke, Von Welch, proxy_certs-present.ppt, pdf

[35] **Globus Toolkit keys concepts &overview**, Rayak Igor, 20.03.2005

[36] **The Globus Toolkit: A System Manager's Perspective**, globus-system-manager-perspective.ppt

[37] **CA-based trust issues for Grid authentication**, Mary R. Thompson, LBNL

Doug Olson, LBNL, Robert Cowles, SLAC, Shawn Mullen, IBM ,Mike Helm, ESnet

June 2003 Grid Certificate Policy Working Group

[38] **Ασφάλεια Πληροφοριακών Συστημάτων και δικτύων**, Γ. Πάγκαλου, Ι. Μαυρίδη, 2002

[39]http://www-fp.mcs.anl.gov/dsl/GridFTP-Protocol-RFC-Draft.pdf

[40] **An Online Credential Repository for the Grid:My Proxy**, Jason Novotny, Steven Tuecke, Von Welch

[41] **The Globus Toolkit: A System Manager's Perspective**.ppt, Bruce Beckles, Systems Manager Cambridge eScience Centre

[42] **Globus: A Core Grid Middleware**, Source: The Globus Project Argonne National Laboratory, University of Southern California / ISI www.globus.org Localised by: Rajkumar Buyya

[43] **The Globus Project: A Status Report**, Ian Foster Carl Kesselman

[44] **Grid Security Infrastructure, The globus project.ppt,** Argonne National Laboratory

[45] **An Analysis of the UNICORE Security Model.pdf**, T. Goss-Walter, Deutscher WetterdienstR. Letz, Deutscher WetterdienstDr. T. Kentemich, Pallas GmbH

H.-C. Hoppe, Pallas GmbHP. Wieder, Forschungszentrum Julich Grid Certificate Policy WG July 2003

[46] **UNICORE at SourceForge**: Detailed Client description.htm

[47]**OPEN SOURCE unicore.sourceforge**.net, OpenSourceFlyer.pdf

[48] **Grids as Production Computing Environments**: The Engineering Aspects of NASA's Information Power Grid, William E. Johnston1, Dennis Gannon2, and Bill Nitzberg3Numerical Aerospace Simulation Division, NASA Ames Research Center, Moffett Field, CA

[49] http://www.ipg.nasa.gov/ipgflat , Credentials on the IPG

[50] **Security GridPP6 30 Jan 2003** Coseners House, David Kelsey CLRC/RAL, UK d.p.kelsey@rl.ac.uk

[51] **DataGrid Security Wrapup**, Linda Cornwall 4th March 2004

[52] **Security, WP7: Security Coordination Group (SCG),** David Kelsey (CCLRC-RAL, UK) d.p.kelsey@rl.ac.uk

[53] **The Earth System Grid (ESG),** Ian Foster (ANL), Dean Williams (PCMDI), &

Don Middleton (presenting), NCAR/SCD On Behalf of the ESG Team

[54] **Registering Users for ESG** - System Architecture, www.globus.org/solution.htm

[55] **The EGEE project: the new Grid Infrastructure**, Fabrizio Gagliardi EGEE Project Director, gagliardi.pdf

[56] **EGEE Global Security Architecture** FOR WEB AND LEGACY SERVICES

EU Deliverable DJRA3.1, **https://edms.cern.ch/document/487004/**

[57] **HEALTHGRID – A SUMMARY**, A joint White Paper from the Healthgrid Association, and Cisco Systems, 30260HealthgridWPv5.pdf

[58] **Authorization on the μgrid for medical data management**, managementLudwig Seitz, Jean-Marc Pierson, Didier OriolLIRIS, CNRS/INSA-LyonJohan Montagnat, Diane Lingrand

[59] **The vision of a HealthGrid**, Sofie NØRAGER European Commission DG INFSO, eHealth unit

[60] **GEMSS:Privacy and Security for a Medical Grid**, Jean A.M Herveg, Federico Crazzolara, Stuart E. Middleton, Darren Marvin, Y. Poullet

[61] **Objectives of the GEMSS project**, http://www.ccrl-nece.de/gemss/index.html

[62] **Globus Toolkit Installation, ISOC, Institute of Technology , University of Washington Tacoma**

[63] **GT4 Admin Guide, www.globus.org, admin.pdf**

[64]http://www.globus.org/toolkit/docs/4.0/security/simpleca/admin-index.html#simpleca-multiplemachines

[65] **Security in the Grid**, by Dr Steven Newhouse, LeSC - London e-Science Centre - Grid Security

[66] **Lessons Learned and Future Directions for Grid Computing,** Samuel D. Gasster, Craig A. Lee, Brooks Davis Computer Systems Research Department, M1–102 The Aerospace Corporation.mgcc_gasster_V1_7.ppt

[67] **Grid Security: Present and Future** , Alan Robiette. JISC Development Group a.robiette@jisc.ac.uk, session2_2.ppt

[68] **Conclusions and Future Directions**, Chapter 8, conclusions.pdf

[69] Enterprises Move to the Computing Grid, Paul Korzeniowski, http://www.ecommercetimes.com/story/45294.html

[70] Grid Computing in Business & Commerce, grid Consortium Memorial Symposium GridWorld Expo 2005