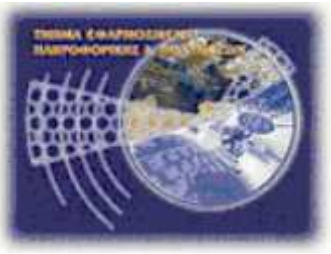
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής και Πολυμέσων



Πτυχιακή εργασία

Υποδομή Δημοσίου Κλειδιού (PKI) σε πλατφόρμα Windows Server 2008 R2

Κοσμαδάκη Μαρία (Α.Μ. 1845)

Μαραγκάκη Αναστασία (Α.Μ. 1902)

Επιβλέπων Καθηγητής: Φυσαράκης Κωνσταντίνος

Επιτροπή αξιολόγησης:

Ημερομηνία Παρουσίασης

Abstract

Cryptography is an integral part of computer science and the secure operation of computer systems and their networks. This Thesis deals with the study of various aspects of cryptography and focuses on public key cryptography and especially the implementation of the necessary infrastructure. In specific, the use of Public Key Infrastructure in Windows Server 2008-based operating environment is detailed, along with observations and conclusions drawn from the above studies.

Σύνοψη

Η κρυπτογραφία αποτελεί αναπόσπαστο μέρος της επιστήμης υπολογιστών και της ασφαλούς λειτουργίας των υπολογιστικών συστημάτων και των δικτύων τους.Αυτή η εργασία ασχολείται με την μελέτη διάφορων στοιχείων της κρυπτογραφίας και επικεντρώνεται στην κρυπτογραφία δημόσιου κλειδιού και ιδιαίτερα στην υλοποίηση των απαραίτητων υποδομών. Έπειτα ασχολείται με την χρήση της υποδομής δημόσιου κλειδιού σε περιβάλλον Windows Server 2008, καταλήγοντας με τις παρατηρήσεις και τα συμπεράσματα που προέκυψαν από τα παραπάνω θέματα.

Περιεχόμενα

1 Εισαγωγή

1.1 Περίληψη

Η ασφάλεια δικτύων είναι απαραίτητη για την σωστή λειτουργίας οποιουδήποτε δικτύου υπολογιστών. Η διασφάλιση της γίνεται με την χρήση μεθόδων κρυπτογραφίας τις οποίες θα μελετήσουμε αναλυτικά, επικεντρώνοντας το ενδιαφέρον μες στην κρυπτογραφία δημόσιου κλειδιού και την τυποποιημένη υλοποίησή της μέσω της υποδομής δημόσιου κλειδιού (Public Key Infrastructure - PKI).

Για την μελέτη της υποδομής δημόσιου κλειδιού θα ασχοληθούμε με την ρύθμιση ενός εξυπηρετητή Windows Server 2008 και πελάτες Windows 7. Καθώς ο Windows Servereίναι ένα λειτουργικό σύστημα που υποστηρίζει εγγενώςPKIθα παρουσιάσουμε αναλυτικά τις δυνατότητες και τις απαιτήσεις του, καθώς και τις απαραίτητες ρυθμίσεις που πρέπει να γίνουν για την απροβλημάτιστη λειτουργία του.

1.2 Κίνητρο για την διεξαγωγή της εργασίας

Η υποδομή δημόσιου κλειδιού είναι μία ολοκληρωμένη λύση ελέγχου των πόρων και των υπηρεσιών ενός δικτύου, με τέτοιο τρόπο ώστε να εγγυάται την πρόσβαση μόνο στους εξουσιοδοτημένους χρήστες και συσκευές. Παρόλα αυτά η χρήση ενός τέτοιου συστήματος είναι αρκετά πιο πολύπλοκη σε σχέση με τα παραδοσιακά συστήματα, καθώς πέρα από βασικές γνώσεις κρυπτογραφίας είναι απαραίτητη η βαθύτερη κατανόηση του ίδιου του συστήματος και έπειτα η σχεδίαση του δικτύου με τέτοιο τρόπο ώστε να ανταποκρίνεται στις απαιτήσεις του περιβάλλοντος στο οποίο θα χρησιμοποιηθεί.

Επιπλέον, αν και ο Windows Server 2008 είναι ένα από τα πιο διαδεδομένα λειτουργικά συστήματα εξυπηρετητή για εταιρικά δίκτυα και προσφέρει την δυνατότητα χρήσης του PKIη ρύθμιση του πρωτοκόλλου και του δικτύου είναι κάθε άλλο παρά απλή.

1.3 Στόχος εργασίας

Στόχος της εργασίας είναι να εξηγήσει τις βασικές έννοιες της κρυπτογραφίας και να εξοικειώσει τον αναγνώστη με τους βασικούς αλγορίθμους και τύπους κρυπτογράφησης, ενώ θα αναλύσει τις έννοιες της κρυπτογραφίας δημόσιου κλειδιού και τις υπηρεσίες που πρέπει να έχει η υποδομή δημόσιου κλειδιού, σε θεωρητικό επίπεδο και σε επίπεδο τεχνικών προτύπων.

Επιπλέον θα παρουσιάζει με λεπτομέρεια την διαδικασία εγκατάστασης του Windows Server 2008 και τις δυνατότητες και τα εργαλεία που προσφέρει για την διαχείριση του εξυπηρετητή και του δικτύου. Τέλος θα εξηγεί τα βήματα που χρειάζονται για την σωστή ρύθμιση της αναγνώρισης χρηστών με το PKI, τις δυνατότητες που προσφέρει αλλά και τους κινδύνους που μπορεί να προκύψουν από λάθη και παραλήψεις στην ρύθμισή του και τα προβλήματα και τους κινδύνους που πρέπει να γνωρίζει ο διαχειριστής ενός συστήματος.

2 Κρυπτογραφία

2.1 Γενικά

Η κρυπτογραφία ασχολείται με την με την μελέτη τεχνικών που διασφαλίζουν την ασφαλή και μυστική επικοινωνία ανάμεσα σε δύο η περισσότερες πλευρές, παρά την πιθανή παρουσία κακόβουλων τρίτων. Συγκεκριμένα ασχολείται με την κατασκευή και την ανάλυση πρωτοκόλλων που διασφαλίζουν την ασφάλεια της επικοινωνίας, συνδυάζοντας μέρη από τις επιστήμες των μαθηματικών, της πληροφορικής και της ηλεκτρονικής.

Σε αυτή την ενότητα θα αναλυθεί περισσότερο η έννοια της ασφάλειας δεδομένων και έπειτα θα παρουσιαστούν οι βασικές έννοιες και αλγόριθμοι κρυπτογράφησης.

2.2 Ασφάλεια

Η ασφάλεια αποτελεί βασικό κομμάτι των σύγχρονων επικοινωνιών. Η βασικότερη απαίτηση ώστε να ισχύει ο όρος «ασφαλής επικοινωνία», είναι η διατήρηση τριών θεμελιωδών χαρακτηριστικών, της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Κάνοντας μια σύντομη αναφορά σε αυτές τις έννοιες, καθώς αναλύονται στα επόμενα κεφάλαια, η ύπαρξη εμπιστευτικότητας μας εξασφαλίζει ότι οι αποθηκευμένες ή προς μετάδοση πληροφορίες είναι προσβάσιμες μόνο από εξουσιοδοτημένες, η ύπαρξη ακεραιότητας μας εξασφαλίζει ότι κάθε σύστημα, πόρος, αρχείο και κάθε πληροφορία μπορεί να τροποποιηθεί μόνο από εξουσιοδοτημένες οντότητες ενώ κάθε άλλη αλλοίωση θα είναι εύκολα ανιχνεύσιμη, και η ύπαρξη διαθεσιμότητας μας εξασφαλίζει ότι ένα σύστημα θα είναι σε λειτουργία και θα εξυπηρετεί τον σκοπό του (π.χ. διάθεση μία υπηρεσίας σε χρήστες) όποτε αυτό απαιτείται. Γενικά τα 3 αυτά χαρακτηριστικά είναι ανεξάρτητα αλλά μπορεί μερικώς να επικαλύπτονται ή ακόμα και να αποκλείει το ένα το άλλο. Στην πράξη, οι διάφορες πολιτικές ασφαλείας απαιτούν να πληρούνται συγκεκριμένες προδιαγραφές - χαρακτηριστικά κάθε φορά, πράγμα που εξαρτάται από τις ανάγκες που εξυπηρετεί η συγκεκριμένη υπηρεσία την οποία προσπαθούμε να προστατεύσουμε.

2.2.1 Αρχές ασφάλειας δεδομένων

Οι τρεις βασικές αρχές που πρέπει να διασφαλίζονται για την ασφάλεια των δεδομένων χαρακτηρίζονται από το ακρωνύμιο CIA (Confidentiality–Integrity - AvailabilityΠαρακάτω παρουσιάζονται σε αναλυτικότερα με βάση το σενάριο της επικοινωνίας μεταξύ δύο οντοτήτων.

2.2.1.1 Ιδιωτική Επικοινωνία – Privacy / Εμπιστευτικότητα - Confidentiality

Μια ασφαλής επικοινωνία πρέπει να είναι ιδιωτική (private). Με άλλα λόγια μόνο ο αποστολέας και ο παραλήπτης πρέπει να είναι στη θέση να «κατανοούν» τα μηνύματα που ανταλλάσσονται κατά τη διάρκεια της επικοινωνίας. Αν κάποιος τρίτος προσπαθήσει να εισχωρήσει στην επικοινωνία, τότε η πολιτική ασφαλείας που έχουμε ακολουθήσει, πρέπει να μας διασφαλίζει ότι δεν θα μπορεί να κατανοήσει το περιεχόμενο των μηνυμάτων αυτών (κρυπτογράφηση).

2.2.1.2 Ακεραιότητα – Integrity

Μια σημαντική απαίτηση, που πρέπει να ικανοποιείται σε μια ασφαλή επικοινωνία αφόρα την ακεραιότητα (integrity) του μηνύματος. Ο παραλήπτης πρέπει να μπορεί να επιβεβαιώσει ότι το μήνυμα που έλαβε είναι ακριβώς το μήνυμα του αποστολέα, ώστε να προστατεύεται από τυχών κακόβουλη και μη μεταβολή των περιεχομένων του από κάποιον τρίτο. Άρα πρέπει να παρέχεται ένας μηχανισμός επαλήθευσης του μηνύματος και απόρριψής του σε περίπτωση που βρεθεί ότι έχει αλλοιωθεί με οποιοδήποτε τρόπο.

2.2.1.3 Διαθεσιμότητα - Availability

Με την πιστοποίηση, διασφαλίζουμε ότι οι οντότητες που λαμβάνουν μέρος σε μια «ασφαλή» επικοινωνία, δηλαδή ο αποστολέας και ο παραλήπτης, είναι σε θέση να αποδείξουν ότι όντως είναι αυτοί που ισχυρίζονται. Πρέπει να μπορούμε να διασφαλίσουμε ότι δεν θα μπορεί κάποιος τρίτος να οικειοποιηθεί την ταυτότητα ενός νόμιμου χρήστη. Το αποτέλεσμα της πιστοποίησης είναι ένα σύνολο πιστοποιητικών, τα οποία περιγράφουν τις ιδιότητες (ταυτότητα, ρόλος, ομάδα, κ.τ.λ.) που είναι άμεσα συνδεδεμένες με την πιστοποίηση.

2.2.2 Υπηρεσίες ασφάλειας

Πέρα από τις τρεις βασικές αρχές της ασφάλειας που παρουσιάστηκαν παραπάνω, ένα πλήρες πρωτόκολλο ασφαλούς επικοινωνίας είναι απαραίτητο να προσφέρει και κάποιες επιπλέον υπηρεσίες.

Παρακάτω παρουσιάζονται συνοπτικά οι κυριότερες υπηρεσίες ασφάλειας που είναι και θεμελιώδεις για την end-to-end ασφάλεια σε multitiereφαρμογές.

2.2.2.1 Εξουσιοδότηση - Authorization

Η έννοια της εξουσιοδότησης είναι παρεμφερής με την πιστοποίηση. Αφού επιβεβαιώσουμε ότι ο πελάτης κάποιας υπηρεσίας είναι αυτός που ισχυρίζεται ότι είναι (authentication), στην συνεχεία θα πρέπει να καθορίσουμε και τα δικαιώματα αυτού του χρήστη και τον ρόλο/ρόλους που θα έχει στο σύστημα. Μόνο εξουσιοδοτημένα άτομα μπορούν να τροποποιούν πόρους του συστήματος.

2.2.2.2 Εμπιστοσύνη - Trust

Η έννοια της εμπιστοσύνης αφορά στην οικοδόμηση εμπιστοσύνης μεταξύ των διαφόρων περιοχών διαχείρισης (administrative domains), οι οποίες είναι πιθανόν να ανήκουν σε διαφορετικούς οργανισμούς. Συνήθως, η εμπιστοσύνη εγκαθιδρύεται με την ανταλλαγή στοιχείων πιστοποίησης (credentials).

2.2.2.3 Single Sign-On

Ο χρήστης πρέπει να έχει τη δυνατότητα, πιστοποιώντας τον εαυτό του μόνο μια φορά στην αρχή, να μπορεί να έχει πρόσβαση και σε άλλες υπηρεσίες χωρίς περαιτέρω πιστοποίηση. Είναι απαραίτητο όταν ένας χρήστης θέλει να έχει πρόσβαση σε πόρους με διαφορετική διαθεσιμότητα και πολιτικές ασφαλείας.

2.2.2.4 Αντιπροσώπευση - Delegation

Με την λειτουργία του delegation, ένας χρήστης μπορεί να εκχωρήσει μέρος των δικαιωμάτων του σε κάποιον, ο οποίος θα δρα εκ μέρους του χρήστη για ένα ορισμένο χρονικό διάστημα.

2.2.2.5 Μη άρνηση της Ευθύνης – Non-repudation

Το non-repudation, αφορά στα μέτρα που παίρνουμε για να διασφαλίσουμε ότι κάποιος χρήστης δεν θα αρνηθεί μια ενέργεια που πράγματι έκανε. Αυτό είναι ιδιαίτερα σημαντικό στο e-commerce.

2.2.2.6 Ανάκληση - Revocation

Η έννοια του revocation αφορά στην ανάκληση μιας οντότητας ασφαλείας, όπως ενός πιστοποιητικού, η οποία δεν είναι πλέον έγκυρη. Σε αυτή την περίπτωση, ο «ιδιοκτήτης» μιας τέτοιας οντότητας θεωρείται εφεξής ως μη έμπιστος.

2.3 Κρυπτογράφηση

Παλαιότερα η κρυπτογραφία ταυτίζονταν με την κρυπτογράφηση. Κρυπτογράφηση είναι η διαδικασία κατά την οποία η πληροφορία μετατρέπεται από την αρχική της, αναγνώσιμη μορφή (plain-text) σε ακατάληπτα δεδομένα, με σκοπό την προστασία από

υποκλοπή. Η αντίστροφη διαδικασία καλείται αποκρυπτογράφηση. Τόσο η κρυπτογράφηση, όσο και η αποκρυπτογράφηση, βασίζονται σε έναν αλγόριθμο, ο οποίος ως είσοδο παίρνει την αρχική πληροφορία και ένα κλειδί (key) και ως έξοδο βγάζει την κρυπτογραφημένη (κρυπτογράφηση) ή την αποκρυπτογραφημένη (αποκρυπτογράφηση) πληροφορία. Σήμερα ο όρος κρυπτογραφία περιλαμβάνει μεταξύ άλλων το σύνολο των πρακτικών κρυπτογράφησης και αποκρυπτογράφησης.

Αν και παραδοσιακά η χρήση της κρυπτογράφησης γινόταν σχεδόν αποκλειστικά από κυβερνήσεις και στρατούς, η μεγάλη διείσδυση του διαδικτύου στην καθημερινή ζωή οδήγησε στην ανάγκη να προστατευτούν οι εμπιστευτικές πληροφορίες εταιρειών και απλών χρηστών που το χειρίζονται. Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί είτε για την προφύλαξη δεδομένων που βρίσκονται σε αποθηκευτικά μέσα είτε για δεδομένα τα οποία αποστέλλονται ανάμεσα σε υπολογιστές μέσω δικτύου ή κάποιου άλλου καναλιού μεταφοράς.

2.3.1 Κλασσική κρυπτογραφία

Η κρυπτογράφηση μηνυμάτων άρχισε να χρησιμοποιείται από τα αρχαία χρόνια, με τα πρώτα δείγματα να χρονολογούνται περίπου το 2000 π. Χ. στην Αίγυπτο και στην Μεσοποταμία. Εξαιτίας των μέσων της εποχής οι αλγόριθμοι που χρησιμοποιούνταν βασίζονταν σε αλγόριθμους αντικατάστασης και αντιμετάθεσης των γραμμάτων. Κατά την αναγέννηση αναπτύχθηκαν πιο πολύπλοκες τεχνικές κρυπτογραφίας ενώ παρουσιάστηκαν και οι πρώτες (μηχανικές) μηχανές που μπορούσαν να παράγουν ένα κρυπτογραφημένο μήνυμα ή να το αποκρυπτογραφήσουν.

Η κλασσική κρυπτογραφία άρχισε να χάνει έδαφος τον $20^{ο}$ αιώνα όπου και άρχισε να αναπτύσσεται η επιστήμη της μοντέρνας κρυπτογραφίας. Οι βασικοί λόγοι ήτανε η εισαγωγή των μαθηματικών για την μελέτη της κρυπτογραφίας παράλληλα με την δημιουργία υπολογιστικών μηχανών, αρχικά μηχανικών και μετέπειτα ψηφιακών, οι οποίες μπορούσαν να υπολογίσουν μέσα σε εύλογο χρονικό διάστημα τις δυνατές λύσεις για ένα μήνυμα.

2.3.2 Μοντέρνα κρυπτογραφία

Η επιστήμη της κρυπτογραφία όπως την γνωρίζουμε σήμερα άρχισε να αναπτύσσεται κατά την διάρκεια του Δευτέρου Παγκοσμίου Πολέμου. Τα δύο κυριότερα χαρακτηριστικά της είναι η χρήση μαθηματικών για την εκτενή ανάλυση των αλγορίθμων κρυπτογράφησης και η γενικότερη αλλαγή νοοτροπίας ώστε η κρυπτογραφία να μην ασχολείται μόνο με τους αλγορίθμους κρυπτογράφησης αλλά με ολόκληρη την διαδικασία μετάδοσης ενός κρυφού μηνύματος.

Ένα ιδιαίτερο χαρακτηριστικό που ορίζει τον τρόπο δημιουργίας και χρήσης των μοντέρνων αλγορίθμων κρυπτογράφησης είναι η ανάπτυξη των ηλεκτρονικών υπολογιστών. Για κάθε γνωστό αλγόριθμο κρυπτογράφησης ο επιτιθέμενος μπορεί, αποκτώντας πρόσβαση στο κρυπτογράφημα να ξεκινήσει μία επίθεση ωμής δύναμης (brute force), υπολογίζοντας όλα τα αποτελέσματα χρησιμοποιώντας όλα δυνατά κλειδιά ώστε να σπάσει το μήνυμα. Η υπολογιστική δύναμη που παρέχουν οι σύγχρονοι υπολογιστές καθιστούν τέτοιες επιθέσεις εύκολο να πραγματοποιηθούν με σχετικά μικρό κόστος, ενώ οι δυνατότητές τους αυξάνονται εκθετικά.

Κατά συνέπεια πλέον ο υπολογισμός του πόσο αποτελεσματικός είναι ένας αλγόριθμος εξαρτάται από το πόσες δυνατές λύσεις υπάρχουν για να βρεθεί ένα μήνυμα που στέλνει. Επιπλέον, έχοντας σαν δεδομένη την συνεχή αύξηση της υπολογιστικής δύναμης που θεωρητικά υπάρχει στα χέρια του επιτιθέμενου ένα μήνυμα κάποια στιγμή θα σπάσει. Ο στόχος είναι η κωδικοποίησή του με τέτοιο τρόπο ώστε όταν ο επιτιθέμενος θα καταφέρει να το σπάσει το μήνυμα να έχει χάσει την χρησιμότητα του για αυτόν εξαιτίας της παρόδου του χρόνου.

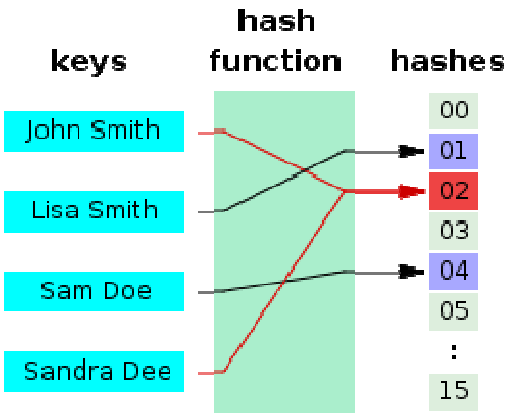
2.3.3 Μηχανισμοί κρυπτογράφησης

2.3.3.1 Συνάρτηση κατατεμαχισμού

Η συνάρτηση κατατεμαχισμού, γνωστή και ως συνάρτηση κατακερματισμού, είναι μια μαθηματική συνάρτηση που έχοντας ως είσοδο μια αυθαίρετου μεγέθους ομάδα δεδομένων δίνει έξοδο μια καθορισμένου μεγέθους συμβολοσειρά (string) (συνήθως ένα ακέραιο αριθμό), πολύ μικρότερη από την είσοδο. Οι τιμές που επιστρέφει η συνάρτηση κατατεμαχισμού ονομάζονται τιμές κατατεμαχισμού (hash values), κώδικες κατατεμαχισμού (hash codes), αθροίσματα κατατεμαχισμού (hash sums) ή απλά τιμές κατατεμαχισμού (hashes).

Μια συνάρτηση κατατεμαχισμού μπορεί να αντιστοιχίζει δύο ή περισσότερους εισόδους στην ίδια τιμή κατατεμαχισμού. Στις περισσότερες εφαρμογές είναι επιθυμητή η ελαχιστοποίηση αυτών συγκρούσεων. Αυτό σημαίνει ότι η συνάρτηση κατατεμαχισμού θα πρέπει να αντιστοιχίζει κάθε είσοδο σε διαφορετική τιμή κατατεμαχισμού. Ανάλογα με την εφαρμογή χρήσης, η συνάρτηση κατατεμαχισμού σχεδιάζεται με διαφορετικές προδιαγραφές. Η ιδέα αυτών των συναρτήσεων εμφανίστηκε το 1950 αλλά ακόμη και σήμερα ο σχεδιασμός μιας καλής συνάρτησης κατατεμαχισμού είναι αντικείμενο έρευνας.

Στην εικόνα 2-1 φαίνεται μία συνάρτηση κατακερματισμού που αναθέτει ακέραιους από 0 έως 15 σε συγκεκριμένες συμβολοσειρές. Στο συγκεκριμένο παράδειγμα υπάρχει σύγκρουση ανάμεσα σε δύο συμβολοσειρές που έχουν τον ίδιο κώδικα. Μία κανονική συνάρτηση κατακερματισμού παράγει αρκετά τυχαίες και διαφορετικές τιμές κατακερματισμού ώστε να μην υπάρχουν συγκρούσεις.



Εικόνα 2-1 Η λειτουργία μίας τυπικής συνάρτηση κατακερματισμού.

Οι συναρτήσεις κατατεμαχισμού χρησιμοποιούνται τυπικά σε δομές δεδομένων, συνήθως για την ομαλή διασπορά των δεδομένων σε ομάδες και την μετέπειτα ανάκτηση τους (πίνακες κατατεμαχισμού – hash tables) ή για την επιτάχυνση της αναζήτησης σε κάποιο πίνακα ή σε εργασίες σύγκρισης δεδομένων (π.χ. εύρεση στοιχείων σε μια βάση δεδομένων, εύρεση παρόμοιων εγγραφών σε ένα μεγάλο αρχείο βάσης κλπ.). Για τις παραπάνω χρήσεις το σημαντικότερο κριτήριο είναι η ταχύτητα εκτέλεσης της συνάρτησης. Παρόλα αυτά στην κρυπτογραφία χρησιμοποιούνται ειδικές συναρτήσεις κατακερματισμού που επιλέγονται με διαφορετικά κριτήρια.

Οι κρυπτογραφικές συναρτήσεις κατακερματισμού έχουν τέσσερα κύρια χαρακτηριστικά:

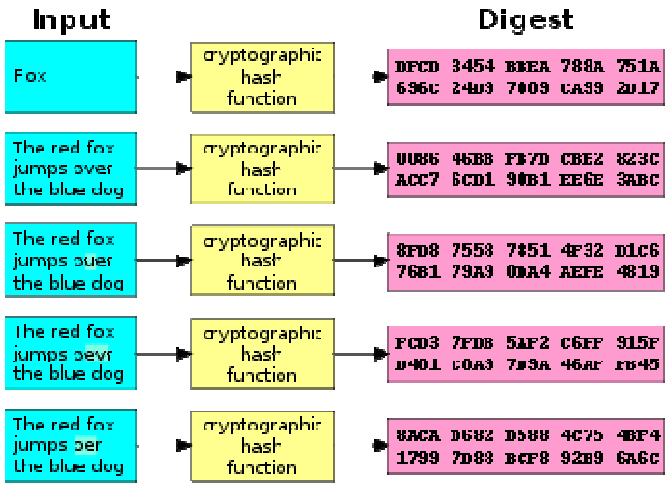
- Η ταχύτητα υπολογισμού της τιμής πρέπει να είναι μικρή άσχετα με το μήκος του μηνύματος.
- Χρειάζεται να μην είναι πρακτικός ο υπολογισμός ενός μηνύματος από την τιμή κατακερματισμού του.
- Είναι απαραίτητο να μην είναι πρακτική η μεταβολή του μηνύματος χωρίς να μεταβληθεί η τιμή κατακερματισμού του.
- Επίσης πρέπει να μην είναι πρακτική η εύρεση δεύτερου μηνύματος με την ίδια τιμή κατακερματισμού.

Αξίζει να σημειωθεί ότι η έννοια της αποδεκτής ταχύτητας εκτέλεσης διαφέρει αρκετά ανάμεσα στις απλές συναρτήσεις κατακερματισμού και τις κρυπτογραφικές. Μία συνάρτηση κατακερματισμού που χρησιμοποιείται για την αποθήκευση δεδομένων (πχ σε ένα hash table)καλείται πολλές φορές για το ίδιο μήνυμα, με σκοπό την αποθήκευση και την ανάκτησή του, οπότε η ταχύτητα παίζει πολύ μεγάλο ρόλο. Αντίθετα, μία κρυπτογραφική συνάρτηση κατακερματισμού καλείται συνήθως μία φορά για τον υπολογισμό της τιμής και για την επαλήθευση, οπότε το κριτήριο δεν είναι η σύντομη ταχύτητα εκτέλεσης αλλά η δυσκολία μίας επίθεσης ωμής δύναμης (brute force), κάνοντας την αργή ταχύτητα εκτέλεσης επιθυμητή.

Παρακάτω θα δούμε κάποιες εφαρμογές των συναρτήσεων κατακερματισμού στην ασφάλεια.

2.3.3.1.1 Επιβεβαίωση ακεραιότητας μηνυμάτων

Μία σημαντική εφαρμογή των συναρτήσεων κατακερματισμού είναι η επιβεβαίωση της ακεραιότητας ενός μηνύματος. Ένας απλός τρόπος είναι ο υπολογισμός των τιμών κατακερματισμού πριν και μετά την αποστολή ενός μηνύματος και η σύγκριση των δύο τιμών. Εξαιτίας αυτού τα κριτήρια με τα οποία επιλέγονται οι κρυπτογραφικές συναρτήσεις κατακερματισμού είναι η μεταβολή του αποτελέσματος άσχετα με το πόσο μικρές είναι οι αλλαγές στο αρχικό μήνυμα και η δυσκολία υπολογισμού δεύτερου μηνύματος με την ίδια τιμή κατακερματισμού.



Εικόνα 2-2 Οι τιμές κατακερματισμού που παράγει για διάφορα μηνύματα ο αλγόριθμος SHA-1.

Οι περισσότεροι αλγόριθμοι ηλεκτρονικής υπογραφής βασίζονται στην επιβεβαίωση της αυθεντικότητας της τιμής κατακερματισμού του μηνύματος και όχι ολόκληρου του μηνύματος, καθώς αυτή θεωρείται αρκετή για να εγγυηθεί της εγκυρότητα της υπογραφής.

2.3.3.1.2 Επιβεβαίωση κωδικού πρόσβασης

Μία άλλη εφαρμογή των συναρτήσεων κατακερματισμού είναι η επιβεβαίωση των κωδικών πρόσβασης σε ένα υπολογιστικό σύστημα. Οι κωδικοί για λόγους ασφαλείας δεν αποθηκεύονται σχεδόν ποτέ σε αναγνώσιμη μορφή, καθώς αυτό θα έδινε σε έναν επιτιθέμενο

την δυνατότητα να έχει άμεσα πρόσβαση σε όλες τις λειτουργίες ενός συστήματος αν αποκτήσει πρόσβαση στα αρχεία που αποθηκεύουν τους κωδικούς. Αντίθετα αυτό που αποθηκεύεται είναι η τιμή κατακερματισμού που παράγει κάθε κωδικός.

Για να γίνει η επαλήθευση ενός χρήστη υπολογίζεται η τιμή κατακερματισμού του κωδικού που δίνει κατά την είσοδό του στο σύστημα και έπειτα συγκρίνεται με την ήδη αποθηκευμένη τιμή. Σε περίπτωση που συμπίπτουν σημαίνει ότι ο χρήστης έχει δώσει τον ίδιο κωδικό με τον αποθηκευμένο. Τυπικά η τιμή κατακερματισμού που αποθηκεύεται είναι η τιμή του κωδικού μαζί με ένα γνωστό αλλά τυχαίο αλφαριθμητικό που είναι διαφορετικό για κάθε χρήστη, ώστε να εξασφαλιστεί ότι ο επιτιθέμενος δεν θα έχει μία ήδη υπολογισμένη λίστα με τιμές κατακερματισμού.

Βέβαια τα παραπάνω σημαίνουν ότι ο κωδικός ενός χρήστη δεν είναι γνωστός και σε περίπτωση απώλειάς του πρέπει να αλλαχθεί, αφού δεν είναι δυνατή η ανάκτηση του. Επιπλέον με αυτόν τον τρόπο παρέχεται προστασία από επιθέσεις ωμής δύναμης, αλλά αν οι ίδιοι οι κωδικοί δεν είναι σωστά επιλεγμένοι συνεχίζουν να είναι ευάλωτοι σε επιθέσεις με χρήση λεξικού, όπου δοκιμάζουν επιλεκτικά τους ποιο συνηθισμένους κωδικούς.

Κάποιες μέθοδοι ενδυνάμωσης κλειδιού (key stretching) όπως η PBKDF2 αποθηκεύουν αναδρομικά υπολογισμένες τιμές κατακερματισμού με στόχο να κάνουν τον υπολογισμό χρονοβόρο και να εμποδίσουν επιθέσεις ωμής δύναμης.

2.3.3.2 Συμμετρική κρυπτογράφηση

Στη συμμετρική κρυπτογράφηση (Symmetric Cryptography) χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, πιο συγκεκριμένα ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα.

Έτσι κατά συνέπεια, το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη την διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού, για αυτό το λόγο απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται, αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία.

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με πιο γνωστό τον Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Τα συστήματα συμμετρικής κρυπτογράφησης προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα έχουν αναπτυχθεί και ήδη χρησιμοποιούνται, με πιο διαδεδομένο το σύστημα Kerberos, του MIT (Massachusetts Institute of Technology).

2.3.3.2.1 Advanced Encryption Standard

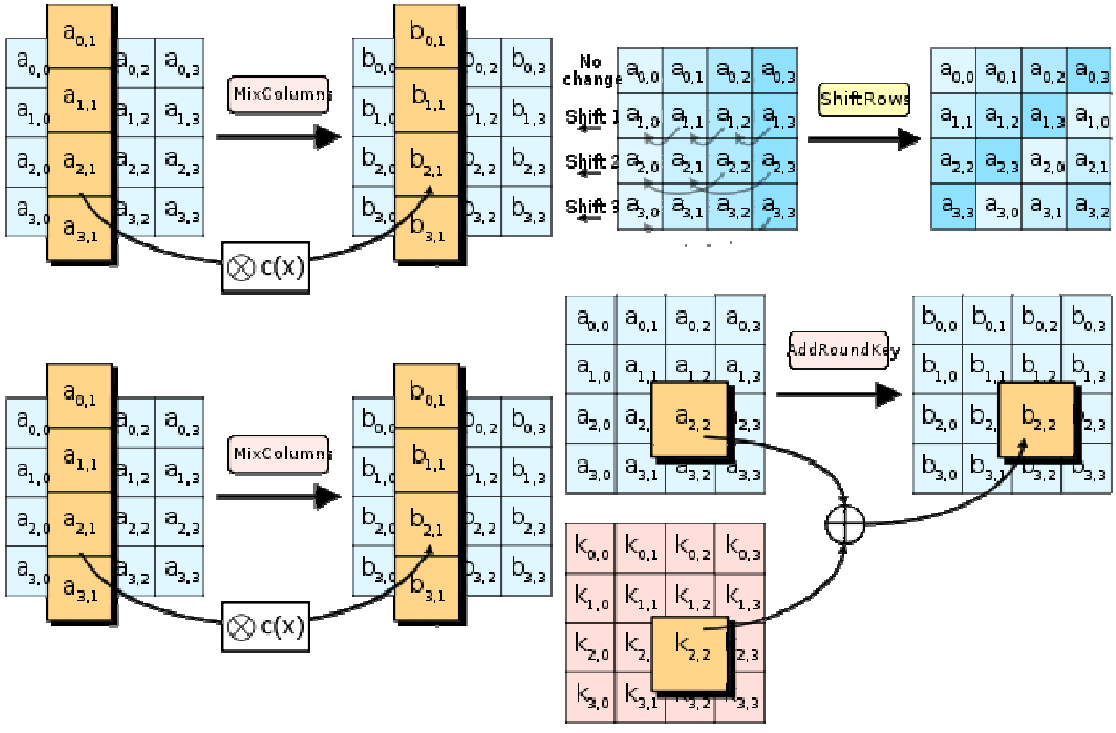
Το πρότυπο κρυπτογράφησης AES (Advanced Encryption Standard) περιγράφει μια διαδικασία κρυπτογράφησης ηλεκτρονικής πληροφορίας βασισμένη στην λογική της κωδικοποίησης ομάδων δεδομένων με κάποιο μυστικό κλειδί. Έχει προτυποποιηθεί από το NIST (National Institute of Technology) τον Νοέμβριο του 2001, αντικαθιστώντας το πρότυπο DES (Data Encryption Standard) και πλέον αποτελεί τον προτεινόμενο αλγόριθμο για εφαρμογές κρυπτογράφησης.

Το πρότυπο AES περιγράφει μια συμμετρική μπλοκ διαδικασία κρυπτογράφησης μυστικού κλειδιού. Το πρότυπο υποστηρίζει την χρήση κλειδιών μήκους 128, 192 και 256 bits. Ανάλογα με το ποιο μήκος κλειδιού χρησιμοποιείται, συνήθως χρησιμοποιείται η συντόμευση AES-128, AES-192 και AES-256 αντίστοιχα. Ανεξάρτητα από το μήκος κλειδιού, ο αλγόριθμος επενεργεί πάνω σε μπλοκ δεδομένων μήκους 128 bits. Η διαδικασία κρυπτογράφησης είναι επαναληπτική. Αυτό σημαίνει ότι σε κάθε μπλοκ δεδομένων γίνεται μια επεξεργασία η οποία επαναλαμβάνεται έναν αριθμό από φορές ανάλογα με το μήκος κλειδιού. Κάθε επανάληψη ονομάζεται γύρος (round). Στον πρώτο γύρο επεξεργασίας ως είσοδος είναι ένα plaintext μπλοκ και το αρχικό κλειδί, ενώ στους γύρους που ακολουθούν ως είσοδος είναι το μπλοκ που έχει προκύψει από τον προηγούμενο γύρο καθώς και ένα κλειδί που έχει παραχθεί από το αρχικό με βάση κάποια διαδικασία που ορίζει ο αλγόριθμος. Το τελικό προϊόν της επεξεργασίας είναι το κρυπτογραφημένο μπλοκ (cipher text). Το μπλοκ αυτό πρέπει να σημειωθεί ότι έχει ακριβώς το ίδιο μέγεθος (128 bits) με το plaintext μπλοκ.

Ο AES τροφοδοτείται με ακολουθίες από bits των 128 bits (μπλοκ) καθώς και από κλειδιά, που μπορεί να έχουν μέγεθος 128, 192 ή 256 bits. Τα κλειδιά αυτά ονομάζονται κλειδιά κρυπτογράφησης (cipher keys) για να διαχωριστούν από τα κλειδιά που παράγονται κατά την λειτουργία του αλγορίθμου.

Τόσο κατά την διάρκεια της διαδικασίας κρυπτογράφησης όσο και αποκρυπτογράφησης, κάθε γύρος επεξεργασίας αποτελείται από μια σειρά μετασχηματισμών σε επίπεδο byte. Για την ακρίβεια, χρησιμοποιούνται 4 τύποι μετασχηματισμών :

- Ένας μετασχηματισμός αντικατάστασης bytes χρησιμοποιώντας κάποιον σχετικό πίνακα αντικατάστασης.
- Ένας μηχανισμός ολίσθησης των bytes του block κατά διαφορετικά offsets.
- Μια διαδικασία ανάμειξης των bytes του block.
- Μια πρόσθεση ενός κλειδιού στου block.



Εικόνα 2-3 Τα τέσσερα στάδια του AES όπως εφαρμόζονται σε ένα block bytes.

Ο αλγόριθμος χαρακτηρίζεται από ιδιαίτερα υψηλή ταχύτητα εκτέλεσης και μικρές απαιτήσεις μνήμης, καθιστώντας τον κατάλληλο για χρήση σε έξυπνες συσκευές με περιορισμένους πόρους. Αν και έχουν βρεθεί κάποιες αποτελεσματικές κρυπτογραφικές επιθέσεις αυτές βασίζονται σε αδυναμίες συγκεκριμένων υλοποιήσεων του και όχι σε κάποια αδυναμία του ίδιου του αλγορίθμου.

2.3.3.3 Ασύμμετρη κρυπτογράφηση

Στην ασύμμετρη κρυπτογράφηση (Public-Key Cryptography), χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

- Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.
- Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.

Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού.

Προκειμένου να επιτευχθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά. Κάθε χρήστης, λοιπόν έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα καλείται δημόσιο κλειδί και το άλλο καλείται ιδιωτικό κλειδί. Το δημόσιο κλειδί δημοσιοποιείται, ενώ το ιδιωτικό κλειδί κρατείται μυστικό και δεν μεταδίδεται ποτέ στο δίκτυο, ενώ όλες οι επικοινωνίες βασίζονται στο δημόσιο κλειδί. Η ανάγκη ο αποστολέας και ο παραλήπτης να μοιράζονται το ίδιο κλειδί εξαφανίζεται και μαζί και πολλά προβλήματα που θα δούμε παρακάτω. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η έμπιστη και επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία, συνεπώς μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δεν μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από ότι η συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποιεί είναι πολύ πιο αργοί από τους αντίστοιχους της συμμετρικής. Το ιδιωτικό κλειδί είναι μαθηματικά συνδεδεμένο με το δημόσιο κλειδί. Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένας τέτοιος αλγόριθμος κρυπτογράφησης ανακτώντας το ιδιωτικό κλειδί από το δημόσιο. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την εύρεση ενός πολύ μεγάλου πρώτου αριθμού.

Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί το δημόσιο κλειδί του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση του ιδιωτικού του κλειδιού για να το αποκρυπτογραφήσει. Κανένας μη εξουσιοδοτημένος τρίτος που υποκλέπτει την σύνδεση δεν

μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει το δημόσιο κλειδί του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το διαβάσει γιατί είναι ο μόνο που γνωρίζει το ιδιωτικό κλειδί. Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί το ιδιωτικό του κλειδί και το ίδιο το μήνυμα. Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας το δημόσιο κλειδί του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.

2.3.3.3.1 RSA

Ο RSA είναι ένας κρυπταλγόριθμος που προτάθηκε το 1977, το όνομα του οποίου προέρχεται από τους δημιουργούς του, Ron Rivest, Adi Shamir και Len Adleman. Είναι ένας κρυπταλγόριθμος ασύμμετρου κλειδιού και κατά συνέπεια επιτρέπει όχι μόνο την κωδικοποίηση μηνυμάτων αλλά μπορεί επίσης να χρησιμοποιηθεί και ως ψηφιακή υπογραφή.

Ο RSA βασίζεται στη δυσκολία παραγοντοποίησης μεγάλων αριθμών. Ένας χρήστης του αλγορίθμου υπολογίζει δύο μεγάλους πρώτους αριθμούς, οι οποίοι αποτελούν το ιδιωτικό κλειδί, και κρατούνται μυστικοί. Έπειτα υπολογίζει και μοιράζεται το γινόμενό τους, μαζί μία βοηθητική τιμή, το οποίο είναι το δημόσιο κλειδί. Οποιοσδήποτε γνωρίζει το δημόσιο κλειδί μπορεί να κρυπτογραφήσει ένα μήνυμα αλλά για να είναι πρακτική η αποκρυπτογράφησή του είναι απαραίτητη η γνώση του ιδιωτικού κλειδιού.

Η ασφάλεια του αλγορίθμου βασίζεται στην δυσκολία υπολογισμού μεγάλων πρώτων αριθμών, με το μέγεθος του κλειδιού να αυξάνει εκθετικά τον θεωρητικό χρόνο εύρεσης μίας λύσης. Μέχρι στιγμής το μεγαλύτερο κλειδί για το οποίο έχει υπολογιστεί μία λύση έχει μέγεθος 768 bit, δηλαδή 232 δεκαδικά ψηφία, το οποίο έχει υπολογιστεί το 2010. Αυτή τη στιγμή το τυπικό μέγεθος ενός κλειδιού RSA είναι 1024 bit ενώ το προτεινόμενο μέγεθος κλειδιού είναι πλέον 2048 bit. Εκτός και αν κάποιος νέος αλγόριθμος εύρεσης πρώτων αριθμών μειώσει δραματικά τον απαιτούμενο χρόνο υπολογισμού, δεν διαφαίνεται κάποιος άμεσος κίνδυνος για την ασφάλεια του αλγορίθμου, ενώ όλες οι γνωστές επιθέσεις βασίζονται σε προβληματικές υλοποιήσεις του.

Το μεγαλύτερο μειονέκτημα του αλγορίθμου είναι πως όλες οι ενέργειες που σχετίζονται με αυτόν (δημιουργία κλειδιών, κρυπτογράφηση, αποκρυπτογράφηση και υπογραφή) είναι εξαιρετικά απαιτητικές σε επεξεργαστική ισχύ. Επίσης όπως και σε όλους τους ασύμμετρους αλγόριθμους κρυπτογραφίας χρειάζεται προσεκτική διαχείριση των κλειδιών ώστε να μην διαρρεύσουν.

2.3.3.4 Μειονεκτήματα και Πλεονεκτήματα την Συμμετρικής και Ασύμμετρης Κρυπτογραφίας.

Το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας, όπως αναφέρθηκε περιληπτικά προηγουμένως, είναι η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής γιατί οποιοσδήποτε γνωρίζει για την συναλλαγή και έχει τα κατάλληλα μέσα μπορεί να καταγράψει όλη την επικοινωνία μεταξύ αποστολέα και παραλήπτη και να αποκτήσει το κλειδί. Έπειτα, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Βέβαια, μπορούν να βασισθούν σε άλλο μέσο επικοινωνίας για την μετάδοση του κλειδιού (π.χ. τηλεφωνία), αλλά ακόμα και έτσι δεν μπορεί να εξασφαλιστεί ότι κανείς δεν παρεμβάλλεται μεταξύ της γραμμής επικοινωνίας των χρηστών.

Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" στο δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.

Άλλο ένα ακόμα πλεονέκτημα των ασύμμετρων κρυπτοσυστημάτων είναι ότι μπορούν να παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους. Η πιστοποίηση ταυτότητας μέσω συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Σαν αποτέλεσμα, ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν επιτρέπεται κάτι τέτοιο αφού κάθε χρήστης έχει αποκλειστική γνώση τού ιδιωτικού του κλειδιού και είναι δικιά του ευθύνη η φύλαξη του.

Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, η διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής (non-repudiation).

Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς (Certificate Authority) ώστε να διασφαλίζεται η κατοχή τους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη.

Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλονται κλειστά, που δεν έχουν σύνδεση με το Διαδίκτυο. Ένας υπολογιστής μπορεί να κρατά τα μυστικά κλειδιά των χρηστών που επιθυμούν να εξυπηρετηθούν από αυτόν, μια και δεν υπάρχει ο φόβος για κατάληψη της μηχανής από εξωτερικούς παράγοντες. Επίσης, στην περίπτωση που η κρυπτογράφηση χρησιμοποιείται για τοπική αποθήκευση κάποιων αρχείων, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη.

Τα δύο κρυπτοσυστήματα μπορούν να εφαρμοστούν μαζί, συνδυάζοντας τα καλά τους χαρακτηριστικά και εξαλείφοντας τα μειονεκτήματα τους. Ένα παράδειγμα τέτοιου συνδυασμού είναι οι ψηφιακοί φάκελοι, οι οποίοι θα αναλυθούν διεξοδικά παρακάτω.

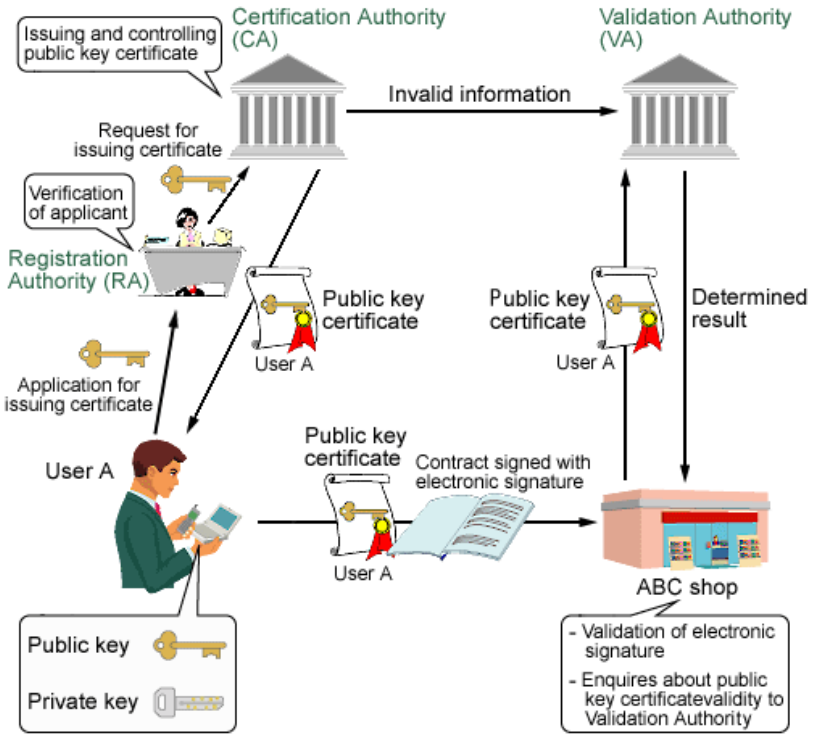
3 Υποδομή δημόσιου κλειδιού

3.1 Γενικά

Η Κρυπτογραφία Δημόσιου Κλειδιού εγγυάται την ασφαλή μεταφορά δεδομένων ανάμεσα σε δύο αποδέκτες, εφόσον ο καθένας γνωρίζει το δημόσιο κλειδί του άλλου και έχει μυστικό το ιδιωτικό του κλειδί. Όμως μόνο με αυτή δεν διασφαλίζεται ότι το δημόσιο κλειδί του άλλου μέρους αντιστοιχεί πραγματικά στο πρόσωπο το οποίο ισχυρίζεται ότι είναι. Η λύση σε αυτό το πρόβλημα δίνεται με την Υποδομή Δημόσιου Κλειδιού.

Η Υποδομή Δημόσιου Κλειδιού (PKI – Public Key Infrastructure) είναι ένας συνδυασμός από προγράμματα, τεχνολογίες κρυπτογράφησης διαδικασίες και υπηρεσίες οι οποίες χρησιμοποιούνται για την δημιουργία, διαχείριση, διανομή, χρήση και ανάκληση ψηφιακών πιστοποιητικών. Συγκεκριμένα πρόκειται για έναν τρόπο αντιστοίχησης δημοσίων κλειδιών με χρήστες, κάθε ένας εκ των οποίων έχει έναν συγκεκριμένο ρόλο και μία μοναδική ταυτότητα.

Ο ρόλος που έχει κάθε χρήστης καθορίζει τους πόρους του δικτύου και των υπολογιστών του στους οποίους έχει πρόσβαση, ενώ σαν ταυτότητα εννοείται το φυσικό πρόσωπο στο οποίο αντιστοιχεί κάθε τέτοιο κλειδί. Παρακάτω όταν αναφερόμαστε σε έναν χρήστη του δικτύου θα εννοούμε τον συνδυασμό των δύο παραπάνω. Σε κάθε χρήστη χορηγείται ένα μοναδικό πιστοποιητικό το οποίο επιβεβαιώνει ότι ένα συγκεκριμένο δημόσιο κλειδί αντιστοιχεί σε αυτόν.



Εικόνα 3-1 Ένα βασικό διάγραμμα ροής που ακολουθείται σε ένα σύστημα Υποδομής Δημόσιου Κλειδιού.

Τα κύρια μέρη που απαρτίζουν ένα σύστημα Υποδομής Δημόσιου Κλειδιού είναι τα παρακάτω:

- Η αρχή Πιστοποιητικών (CA – Certificate Authority) είναι υπεύθυνη για την έκδοση και την επαλήθευση της εγκυρότητας των πιστοποιητικών κάθε χρήστη.

- Η Αρχή Εγγραφών (RA – Registration Authority) είναι υπεύθυνη για την επιβεβαίωση της ταυτότητας κάθε χρήστη που εγγράφεται στο σύστημα (πριν την έκδοση του πιστοποιητικού του από την Αρχή Πιστοποιητικών).
- Η Αρχή Επιβεβαίωσης (VA – Validation Authority) η οποία είναι προαιρετική και δεν υπάρχει σε αρκετά συστήματα. Πρόκειται για μία Τρίτη αρχή που μπορεί να παρέχει στην Αρχή Πιστοποιητικών κάποιες επιπλέον πληροφορίες με τις οποίες θα επιβεβαιώνεται η μοναδική ταυτότητα του χρήστη.
- Ένας ασφαλής κεντρικός κατάλογος πιστοποιητικών στον οποίο κρατούνται και αποθηκεύονται τα κλειδιά κάθε χρήστη.

Στην εικόνα 3-1 φαίνεται ένα βασικό διάγραμμα ροής που ακολουθείται σε ένα σύστημα Υποδομής Δημόσιου Κλειδιού. Ο χρήστης επικοινωνεί με την Αρχή Εγγραφών καταθέτοντας μία αίτηση για έκδοση ενός πιστοποιητικού. Αυτή ελέγχει την εγκυρότητα της αίτησης και εφόσον είναι ορθή την προωθεί στην Αρχή Πιστοποιητικών, η οποία δημιουργεί ένα δημόσιο κλειδί και εκδίδει ένα πιστοποιητικό που το αντιστοιχίζει σε αυτόν. Όταν ο χρήστης δοκιμάζει να χρησιμοποιήσει μία υπηρεσία χρησιμοποιεί αυτό το πιστοποιητικό. Η υπηρεσία ελέγχει την ηλεκτρονική υπογραφή του χρήστη και μέσω της αρχής επιβεβαίωσης ελέγχει την εγκυρότητα του πιστοποιητικού.

Αρκετά σημαντικό ρόλο παίζει το σύστημα διαχείριση πιστοποιητικών που χρησιμοποιείται, δηλαδή οι τεχνολογίες και οι διαδικασίες που χρησιμοποιείται για την διαχείριση και την χρήση των πιστοποιητικών. Παρακάτω θα εξετάσουμε με λεπτομέρεια τα βασικά σημεία της τεχνολογίας καθώς και κάποια συγκεκριμένα πρότυπα που καθορίζουν τον τρόπο λειτουργίας της Υποδομής Δημόσιου κλειδιού.

3.2 Το πρότυπο X.509

Το X.509 είναι ένα διεθνές πρότυπο που καθορίζει τον τρόπο λειτουργίας των Υποδομών Δημοσίου Κλειδιού (Public Key Infrastructure / PKI). Προδιαγράφει τις μορφές διάθεσης της σχετικής πληροφορίας (κλειδιά, πιστοποιητικά, λίστες ανάκλησης), καθώς και τους αλγορίθμους επαλήθευσης του κύρους ενός πιστοποιητικού.

Θα δώσουμε ιδιαίτερο βάρος σε αυτή την προδιαγραφή γιατί καθορίζει τον τρόπο λειτουργίας του συστήματος που χρησιμοποιείται στον Windows Server 2008.

3.3 Ηλεκτρονικά πιστοποιητικά

Τα ηλεκτρονικά πιστοποιητικά είναι η βάση της Υποδομής Δημόσιου κλειδιού. Πρόκειται για ένα έγγραφο το οποίο χρησιμοποιεί μία ηλεκτρονική υπογραφή για να αντιστοιχίσει με μοναδικό τρόπο ένα δημόσιο κλειδί με έναν συγκεκριμένο χρήστη. Τυπικά ένα ηλεκτρονικό πιστοποιητικό περιέχει τις παρακάτω πληροφορίες:

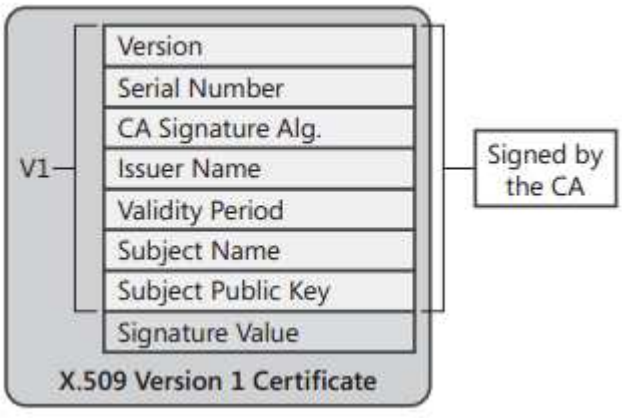
- Την ταυτότητα του χρήστη που χρησιμοποιεί το πιστοποιητικό. Δεν πρόκειται απαραίτητα για ένα φυσικό πρόσωπο, καθώς ένα πιστοποιητικό μπορεί να αντιστοιχεί σε έναν υπολογιστή, μία συσκευή που συνδέεται στο δίκτυο ή μία υπηρεσία του.
- Πληροφορίες σχετικά με την Αρχή πιστοποίησης που εξέδωσε το πιστοποιητικό.
- Το δημόσιο κλειδί που είναι συνδεδεμένο με αυτό το πιστοποιητικό. Προφανώς ο κάτοχος του πιστοποιητικού έχει και το αντίστοιχο ιδιωτικό κλειδί από το οποίο δημιουργήθηκε.
- Τα ονόματα των αλγορίθμων κρυπτογράφησης και υπογραφής που υποστηρίζονται από αυτό το πιστοποιητικό.
- Πληροφορίες σχετικά με το πώς μπορεί να ελεγχθεί η εγκυρότητα του πιστοποιητικού και το αν έχει ανακληθεί ή όχι.

Το πρότυπο X.509 καθορίζει με ακρίβεια τα στοιχεία που περιέχει ένα πιστοποιητικό. Υπάρχουν τρεις εκδόσεις, με την παλιότερη να είναι η Version1, ενώ με το πέρασμα του χρόνου παρουσιάστηκαν οι Version 2 και 3, για να καλύψουν τις νέες ανάγκες που παρουσιάστηκαν.

3.3.1 X.509 Version 1

Η πρώτη έκδοση του ορισμού του πιστοποιητικού παρουσιάστηκε το 1988 και πλέον δεν χρησιμοποιείται με εξαίρεση κάποια παλιότερα συστήματα. Περιέχει τα παρακάτω πεδία:

- **Έκδοση:** Περιέχει την τιμή που υποδεικνύει την έκδοση του πιστοποιητικού.
- **Σειριακός αριθμός:** Ένας ακέραιος που είναι μοναδικός για κάθε πιστοποιητικό και δίνεται από την Αρχή Πιστοποιητικών.
- **Αλγόριθμος υπογραφής:** Ο αλγόριθμος που χρησιμοποιήθηκε από την Αρχή Πιστοποιητικών για να δημιουργήσει την υπογραφή. Περιλαμβάνει τα πεδία που χρησιμοποιήθηκαν για την δημιουργία της υπογραφής, τα οποία είναι όλα τα πεδία του πιστοποιητικού.
- **Όνομα εκδότη:** Το όνομα της Αρχής Πιστοποίησης που εξέδωσε το συγκεκριμένο πιστοποιητικό. Πρόκειται για το διακεκριμένο όνομα της αρχής όπως προσδιορίζεται από το έγγραφο RFC3280.
- **Περίοδος εγκυρότητας:** Το χρονικό διάστημα για το οποίο το πιστοποιητικό είναι έγκυρο. Μπορεί να πρόκειται είτε για έναν προσδιορισμό του πόσο καιρό μετά την έκδοσή του το πιστοποιητικό είναι έγκυρο είτε να περιέχει δύο πεδία που προσδιορίζουν την ημερομηνία έναρξης και λήξης αυτής της περιόδου.
- **Όνομα κατόχου:** Το όνομα του χρήστη του πιστοποιητικού, είτε πρόκειται για φυσικό πρόσωπο είτε για μία συσκευή ή υπηρεσία του δικτύου. Αποθηκεύεται το διακεκριμένο όνομα του κατόχου όπως προσδιορίζεται είτε από το πρότυπο X.500 ή από το έγγραφο RFC822.
- **Δημόσιο κλειδί:** Το δημόσιο του εκδότη, το οποίο θα σταλεί στην Αρχή Πιστοποιητικών για την επιβεβαίωση των στοιχείων. Σε αυτό το πεδίο περιέχεται επίσης το αναγνωριστικό του αλγορίθμου δημιουργίας του κλειδιού (όχι αυτός της υπογραφής του κλειδιού που αναφέρθηκε παραπάνω).
- **Ηλεκτρονική υπογραφή:** Η ηλεκτρονική υπογραφή που επιβεβαιώνει την εγκυρότητα των παραπάνω.

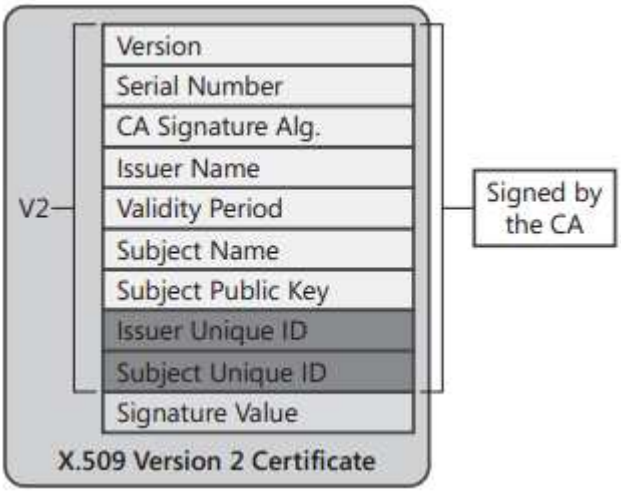


Εικόνα 3-2 Τα πεδία που περιέχονται σε ένα πιστοποιητικό X.509 Version1.

Στα πιστοποιητικά της πρώτης έκδοσης επιτρέπεται να αναφέρονται σε άλλα πιστοποιητικά που παραπέμπουν σε μία αλυσίδα Αρχών Πιστοποίησης ιεραρχικά διατεταγμένων.

3.3.2 X.509 Version 2

Αν και η πρώτη έκδοση του πιστοποιητικού περιέχει βασικές πληροφορίες σχετικά με τον κάτοχο του πιστοποιητικού, λείπουν πληροφορίες σχετικά με τον εκδότη του. Περιέχοντας τις πληροφορίες που προσδιορίζουν μόνο το όνομα του και τους αλγορίθμους δημιουργίας του κλειδιού και της υπογραφής δεν προβλέπεται κάποιος τρόπος για την ανανέωση του κλειδιού της Αρχής Πιστοποιητικών.



Εικόνα 3-3Τα πεδία που περιέχονται σε ένα πιστοποιητικό X.509 Version2.

Όταν το πιστοποιητικό της αρχής πιστοποιητικών ανανεώνεται, δύο πιστοποιητικά περιέχουν την ίδια τιμή στο πεδίο του ονόματος εκδότη. Επιπλέον είναι δυνατών να δημιουργηθεί μία Αρχή Πιστοποιητικών με το ίδιο όνομα από έναν άλλο οργανισμό, ενώ δεν υπάρχει καμία εγγύηση ότι και τα ονόματα των κατόχων θα είναι διαφορετικά.

Για την αντιμετώπιση των παραπάνω μειονεκτημάτων η δεύτερη έκδοση του πρωτοκόλλου εισήγαγε δύο νέα πεδία:

- **Μοναδικό αναγνωριστικό εκδότη:** Ένα προαιρετικό πεδίο που περιέχει ένα μοναδικό αναγνωριστικό, συνήθως ένα αλφαριθμητικό που περιέχει έναν δεκαεξαδικό αριθμό, το οποίο προσδιορίζεται από την Αρχή ανανέωσης κατά την έκδοση του πιστοποιητικού. Αυτό το πεδίο αναφέρεται στο πιστοποιητικό, και με την επανέκδοσή του ανανεώνεται.
- **Μοναδικό χαρακτηριστικό κατόχου:** Ένα μοναδικό πεδίο που περιέχει ένα μοναδικό χαρακτηριστικό, οποίο είναι πάλι ένα δεκαεξαδικό αλφαριθμητικό. Αν ο κάτοχος είναι και αυτός μία Αρχή Πιστοποίησης τότε η τιμή αυτού του πεδίου περιέχεται στο παραπάνω.

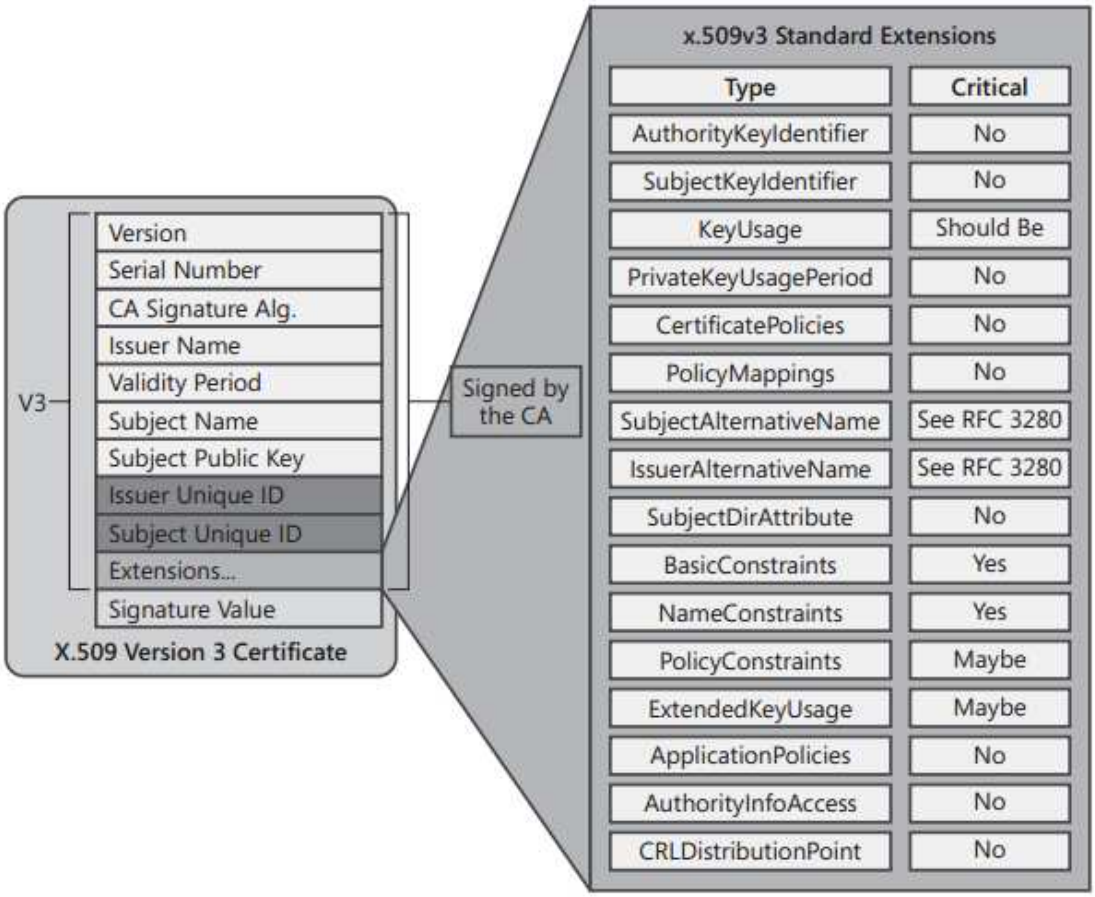
3.3.3 X.509 Version3

Η τρίτη έκδοση του πιστοποιητικού εισήγαγε επεκτάσεις που παρέχουν επιπλέον λεπτομέρειες σχετικά με τον κάτοχο το πιστοποιητικού και τον εκδότη του, καθώς και άλλες πληροφορίες. Κάθε επέκταση προσδιορίζεται από τρία πεδία:

- **Αναγνωριστικό επέκτασης:** Ένα μοναδικό πιστοποιητικό αντικειμένου που υποδεικνύει το είδος και την μορφή της επέκτασης.
- **Σημαφόρος κρισιμότητας:** Μία τιμή που υποδεικνύει αν η συγκεκριμένη επέκταση είναι σημαντική ή όχι. Αν η εφαρμογή που δοκιμάζει να πιστοποιήσει την εγκυρότητα του πιστοποιητικού δεν μπορεί να αναγνωρίσει τον ρόλο της συγκεκριμένης επέκτασης και ή αν η επέκταση δεν περιέχει τιμή τότε η εφαρμογή αρνείται να αποδεχθεί και να χρησιμοποιήσει το πιστοποιητικό. Στην περίπτωση που μία επέκταση δεν είναι χαρακτηρισμένη σαν κρίσιμη τότε η

εφαρμογή μπορεί να αποδεχθεί το πιστοποιητικό (αφού επιβεβαιώσει την χρησιμότητά του).

- **Τιμή επέκτασης:** Η τιμή της συγκεκριμένης επέκτασης. Αυτή μπορεί να διαφέρει ανάλογα με το είδος της επέκτασης.



Εικόνα 3-4 Η τρίτη έκδοση του πιστοποιητικού X.509 με όλες τις επιτρεπόμενες επεκτάσεις.

Σε ένα πιστοποιητικό X.509 Version 3 μπορούν να υπάρχουν αρκετές επεκτάσεις, αλλά η εξέταση κάθε μίας από αυτές ξεφεύγει από τα πλαίσια αυτής της εργασίας.

3.4 Αρχή Πιστοποίησης

Η Αρχή Πιστοποίησης είναι η κοινώς έμπιστη αρχή που εκδίδει τα ψηφιακά πιστοποιητικά. Μία Αρχή Πιστοποίησης η οποία υπογράφει το πιστοποιητικό της ονομάζεται Κεντρική Αρχή Πιστοποίησης. Μία Αρχή Πιστοποίησης της οποίας το πιστοποιητικό έχει υπογραφεί από άλλη Αρχή Πιστοποίησης ονομάζεται υφιστάμενη Αρχή Πιστοποίησης. Οι Αρχές Πιστοποίησης είναι υπεύθυνες για την έκδοση, την ανάκληση πιστοποιητικών και την δημοσιοποίηση των ψηφιακών πιστοποιητικών.

3.5 Υπηρεσίες Δημόσιου Κλειδιού

Για την σωστή λειτουργία της υποδομής δημόσιου κλειδιού είναι απαραίτητο να υλοποιούνται μία σειρά από υπηρεσίες. Παρακάτω εξετάζουμε κάποιες από αυτές:

3.5.1 Ανάκληση Πιστοποιητικού (Certificate Revocation)

Πολλές φορές κρίνεται απαραίτητη η ακύρωση ενός ψηφιακού πιστοποιητικού πριν την καθορισμένη ημερομηνία λήξης του. Υπάρχουν διάφοροι λόγοι που θα μπορούσαν να οδηγήσουν στην ακύρωση ενός πιστοποιητικού, όπως για παράδειγμα:

- Διαρροή του ιδιωτικού κλειδιού του κατόχου του πιστοποιητικού.
- Αλλαγή των πληροφοριών που χαρακτηρίζουν την οντότητα, όπως για παράδειγμα αλλαγή επωνύμου.
- Διαρροή του ιδιωτικού κλειδιού της Αρχής Πιστοποίησης.

Όταν λοιπόν για οποιοδήποτε λόγο κριθεί απαραίτητη η ακύρωση του πιστοποιητικού ενός χρήστη του δικτύου, θα πρέπει να υπάρχει ένας μηχανισμός που να ειδοποιεί τους υπόλοιπους ότι δεν μπορούν πλέον να χρησιμοποιούν το δημόσιο κλειδί αυτής της οντότητας. Αυτόν τον μηχανισμό εξυπηρετεί η υπηρεσία δημοσίου κλειδιού που ονομάζεται Ανάκληση Πιστοποιητικού (Certificate Revocation). Σε περιπτώσεις ανάκλησης πιστοποιητικού η Αρχή Καταχώρησης (RA) θα πρέπει να ενημερώσει την Αρχή Πιστοποίησης για το ποια πιστοποιητικά θα πρέπει να ακυρωθούν.

Οι μηχανισμοί που χρησιμοποιούνται από την Αρχή Πιστοποίησης για το σκοπό αυτό είναι:

- Περιοδικοί Μηχανισμοί Δημοσίευσης (Periodic Publication Mechanisms): ο μηχανισμός αυτός περιλαμβάνει τη χρήση λιστών ανάκλησης πιστοποιητικών (Certificate Revocation Lists - CRL) και τη χρήση δέντρων ανάκλησης πιστοποιητικών (Certificate Revocation Trees - CRT). Μία λίστα ανάκλησης πιστοποιητικών (CRL) είναι μία υπογεγραμμένη λίστα που περιέχει τα πιστοποιητικά που έχουν ανακληθεί. Η λίστα αυτή μπορεί να ανανεώνεται κάθε 1 ως 24 ώρες. Το δέντρο ανάκλησης πιστοποιητικών (CRT) βασίζεται στα δέντρα κατακερματισμού Merkle. Στην περίπτωση ενός CRT, το δέντρο περιέχει όλες τις γνωστές πληροφορίες που αφορούν ανακληθέντα πιστοποιητικά μέσα σε ένα γνωστό σύνολο δικτύων PKI.
- Online Μηχανισμοί Αναζήτησης (Online Query Mechanisms): ο μηχανισμός αυτός προσφέρει στο σύστημα πραγματικού χρόνου ενημέρωση ως προς τα πιστοποιητικά που έχουν ανακληθεί. Αυτού του είδους ο μηχανισμός είναι κατάλληλος για συναλλαγές υψηλής προτεραιότητας, όπως για παράδειγμα οι οικονομικές συναλλαγές. Στην περίπτωση της ενημέρωση πραγματικού χρόνου γίνεται χρήση του πρωτοκόλλου OCSP (Online Certificate Status Protocol) ή των Online Transaction Validation Protocols. Το OCSP ορίζει ένα μηχανισμό ενημέρωσης σχετικά με την εγκυρότητα πιστοποιητικών δημόσιου κλειδιού. Τα Online Transaction Validation Protocols χρησιμοποιούνται για on-line έλεγχο της εγκυρότητας συναλλαγών όπως είναι οι εμπορικές συναλλαγές μέσω πιστωτικής κάρτας.

Θα πρέπει να σημειωθεί ότι υπάρχει μία έμμεση σχέση ανάμεσα στις πληροφορίες που περιέχει ένα πιστοποιητικό και το χρήσιμο χρόνο ζωής του. Χονδρικά ισχύει ο κανόνας όσο πιο πολλές οι πληροφορίες σε ένα πιστοποιητικό, τόσο μικρότερη η χρησιμότητά του. Αυτό συμβαίνει γιατί είναι πολύ πιθανό οι πληροφορίες που περιέχονται στο πιστοποιητικό να αλλάξουν. Έτσι ένα παλιό πιστοποιητικό μπορεί να ανακληθεί και ένα νέο πιστοποιητικό να εκδοθεί πριν τη λήξη του προηγούμενου.

Ένα από τα πιο σημαντικά ζητήματα στο θέμα της ανάκλησης των πιστοποιητικών είναι η συχνότητα με την οποία οι πληροφορίες της ανάκλησης ανανεώνονται και δημοσιεύονται. Αν οι χρήστες δεν ενημερωθούν έγκαιρα για την ακύρωση κάποιου πιστοποιητικού μπορεί να εμπιστευθούν ένα άκυρο πιστοποιητικό. Η καθυστέρηση μεταξύ του χρόνου που η Αρχή Πιστοποίησης λαμβάνει την πληροφορία ότι ένα πιστοποιητικό πρέπει να ανακληθεί και του χρόνου που τελικά η Αρχή Πιστοποίησης ανακοινώνει και δημοσιεύει την ανάκληση ονομάζεται καθυστέρηση ανάκλησης (revocation delay).

Η καθυστέρηση ανάκλησης θα πρέπει να είναι όσο το δυνατόν μικρότερη και θα πρέπει να προσδιορίζεται στην πολιτική των πιστοποιητικών (certificate policy). Η πολιτική

των πιστοποιητικών είναι ένα έγγραφο που προσδιορίζει την πολιτική ασφαλείας κατά την διαχείριση των πιστοποιητικών. Η σύνταξη ενός τέτοιου εγγράφου είναι αρμοδιότητα της Αρχή Πιστοποίησης.

3.5.2 Δημιουργία εφεδρικού κλειδιού και ανάκτηση κλειδιού (Key backup and recovery)

Σε ένα περιβάλλον Υποδομής Δημοσίου Κλειδιού υπάρχουν πολλοί λόγοι που μπορούν να οδηγήσουν στην απώλεια του ιδιωτικού κλειδιού ενός ή περισσοτέρων χρηστών. Τέτοιοι λόγοι μπορεί να είναι η απώλεια ενός κωδικού που ξεκλειδώνει το κωδικοποιημένο ιδιωτικό κλειδί, η καταστροφή ή η αντικατάσταση ενός αποθηκευτικού μέσου (π.χ. ενός σκληρού δίσκου ή μιας έξυπνης κάρτας) που περιέχει το ιδιωτικό κλειδί κ.α. Η απώλεια τέτοιου είδους δεδομένων μπορεί να αποβεί καταστροφική.

Η λύση στο πρόβλημα της απώλειας ενός ιδιωτικού κλειδιού δίνεται με την *δημιουργία εφεδρικού κλειδιού και ανάκτηση κλειδιού* (*key backup and recovery*). Το εφεδρικό κλειδί είναι στην ουσία ένα αντίγραφο ασφαλείας του ιδιωτικού κλειδιού και συνήθως δημιουργείται από την Αρχή Πιστοποίησης κατά την δημιουργία του πιστοποιητικού. Ας σημειωθεί ότι η δημιουργία εφεδρικού κλειδιού δεν είναι απαραίτητη στην περίπτωση που το κλειδί χρησιμοποιείται για ψηφιακή υπογραφή.

3.5.3 Αυτόματη ανανέωση κλειδιού (Automatic Key Update)

Κάθε πιστοποιητικό από την στιγμή της έκδοσης του έχει περιορισμένη διάρκεια ζωής. Καθώς το πιστοποιητικό πλησιάζει στη λήξη του, θα πρέπει να δημιουργηθεί ένα νέο ζεύγος δημοσίου και ιδιωτικού κλειδιού καθώς και ένα νέο πιστοποιητικό. Η διαδικασία αυτή είναι γνωστή ως *ανανέωση κλειδιού* (*key update*). Οι περισσότεροι χρήστες ενός δικτύου όμως δεν μπορούν να θυμούνται την ημερομηνία λήξης των πιστοποιητικών τους με αποτέλεσμα να μην τα ανανεώνουν έγκαιρα.

Το πρόβλημα αυτό μπορεί να ξεπεραστεί αν η ανανέωση του κλειδιού γίνεται αυτόματα από την ίδια την Υποδομή Δημοσίου Κλειδιού και χωρίς την παρέμβαση κάποιου χρήστη. Η διαδικασία αυτή ονομάζεται αυτόματη ανανέωση κλειδιού (Automatic Key Update). Κάθε φορά που ένα πιστοποιητικό χρησιμοποιείται, ελέγχεται η περίοδος ισχύος του. Στην περίπτωση που πλησιάζει η ημερομηνία λήξης του δημιουργείται ένα νέο πιστοποιητικό που αντικαθιστά το παλιό. Τα νέα κλειδιά χρησιμοποιούνται για τις μελλοντικές διαδικασίες ψηφιακής υπογραφής και κρυπτογράφησης. Το παλιό πιστοποιητικό διατηρείται σε περίπτωση που χρειαστεί για επαλήθευση ψηφιακής υπογραφής και αποκρυπτογράφηση δεδομένων με το παλιό ιδιωτικό κλειδί.

3.5.4 Ιστορικό κλειδιών (Key history)

Είδαμε παραπάνω ότι καθώς ένα πιστοποιητικό πλησιάζει την ημερομηνία λήξης του, αντικαθίσταται από ένα καινούριο που περιέχει νέα κλειδιά κρυπτογράφησης. Αυτό δε σημαίνει ότι τα δεδομένα που κρυπτογραφήθηκαν με τα παλιά κλειδιά δε θα μπορούν πλέον να ανακτηθούν. Για αυτό το λόγο είναι σημαντική η ασφαλής αποθήκευση των παλιών ιδιωτικών κλειδιών ακόμη και αν το πιστοποιητικό τους έχει λήξει.

Η αποθήκευση των παλιών κλειδιών έχει ως αποτέλεσμα την δημιουργία ενός *ιστορικού κλειδιών (key history)*, στο οποίο μπορεί εύκολα να ανατρέξει ο χρήστης όποτε χρειαστεί. Οι πληροφορίες του ιστορικού κλειδιών συνήθως αποθηκεύονται τοπικά στο χρήστη, μπορούν όμως να αποθηκευτούν και στην Αρχή Πιστοποίησης ή σε κάποια έμπιστη αρχή, εφόσον βέβαια είναι δυνατή η ασφαλής ανάκτηση τους.

3.5.5 Δια-πιστοποίηση (Cross certification)

Η *δια-πιστοποίηση* είναι ένας χρήσιμος μηχανισμός για την δημιουργία μιας αμφίδρομης σχέσης εμπιστοσύνης μεταξύ δύο Αρχών Πιστοποίησης. Κατά τη διαδικασία της δια-πιστοποίησης συγκρίνονται οι πολιτικές ασφαλείας και οι πρακτικές που εφαρμόζει κάθε

αρχή και αν βρεθούν κοινά σημεία τότε κάθε μία αρχή εκδίδει ένα πιστοποιητικό για την άλλη. Η δια-πιστοποίηση χρησιμοποιείται για να επεκτείνει τις σχέσεις εμπιστοσύνης ανάμεσα σε περιβάλλοντα Υποδομής Δημοσίου Κλειδιού που αρχικά ήταν ασύνδετα μεταξύ τους.

3.5.6 Μη αποκήρυξη (non - repudiation)

Μη αποκήρυξη είναι η υπηρεσία εκείνη που διασφαλίζει ότι μία οντότητα δε θα μπορεί να αρνηθεί μελλοντικά τη συμμετοχή της σε κάποια δράση. Η βασική ιδέα είναι ότι η οντότητα δεσμεύεται κρυπτογραφικά με κάθε συγκεκριμένη πράξη, με τέτοιο τρόπο, ώστε πιθανή άρνησή της να αποτελεί παραδοχή αμέλειας ή κακεντρέχειας. Τέτοια πράξη μπορεί να είναι κάποια οικονομική συναλλαγή στο Διαδίκτυο, η δημιουργία και η αποστολή ή λήψη ενός εγγράφου κ.α. Έτσι συχνά γίνεται λόγος για μη αποκήρυξη της προέλευσης, της παραλαβής, και της αποδοχής.

Η μη αποκήρυξη είναι από τις πιο σημαντικές αλλά ταυτόχρονα και πιο πολύπλοκες υπηρεσίες μιας Υποδομής Δημοσίου κλειδιού. Η σωστή λειτουργία της βασίζεται στην ύπαρξη και άλλων υπηρεσιών όπως είναι η ασφαλής χρονοσφράγιση και η ασφαλής συμβολαιογραφία. Σημαντική είναι επίσης και η δυνατότητα ασφαλούς αποθήκευσης πληροφοριών χρήσιμων για την επίλυση διαφωνιών, όπως είναι ψηφιακά πιστοποιητικά μετά τα λήξη τους, παλιές λίστες πιστοποιητικών, σφραγίδες χρόνου κ.α. Σε αυτή την περίπτωση η δυσκολία έγκειται στο να βρεθεί μία ισορροπία ανάμεσα στο πλήθος και το είδος των πληροφοριών που θα αποθηκευτούν και θα θεωρηθούν επαρκής για την επίλυση οποιασδήποτε διαμάχης. Η διατήρηση, λοιπόν, της μη αποκήρυξης σε μία Υποδομή Δημόσιου Κλειδιού είναι πολύπλοκη και επικεντρώνεται στην προστασία του ιδιωτικού κλειδιού.

Η μεγαλύτερη αδυναμία ενός συστήματος με Υποδομή Δημοσίου Κλειδιού είναι η ικανότητά του να προστατεύει και να αποδεικνύει ότι έχει στην κατοχή του το ιδιωτικό κλειδί που χρησιμοποιείται για τις ψηφιακές συναλλαγές.

3.5.7 Χρονοσφράγιση (Time stamping)

Μία από τις πιο σημαντικές υπηρεσίες για την υποστήριξη της μη-αποκήρυξης σε μια Υποδομή Δημοσίου Κλειδιού, είναι αυτή της *ασφαλούς* χρονοσφράγισης (secure time stamping). Η ασφαλής χρονοσφράγιση χρησιμοποιείται για να αποδείξει ότι ένα ορισμένο δεδομένο υπήρξε πριν από κάποια συγκεκριμένη χρονική στιγμή. Κάτι τέτοιο είναι πολύ σημαντικό όταν πρόκειται για δεδομένα που αφορούν οικονομικές ή νομικές συναλλαγές, ιατρικά αρχεία κ.α. Η συσχέτιση μίας πληροφορίας με κάποια συγκεκριμένη χρονική στιγμή γίνεται από μία έμπιστη Τρίτη αρχή, την *Αρχή Χρονοσφράγισης* (Time Stamping Authority - TSA).

Η τεχνική της δημιουργία μιας σφραγίδας χρόνου (timestamp) βασίζεται στις ψηφιακές υπογραφές και στις συναρτήσεις κατακερματισμού . Ο χρήστης της υπηρεσίας στέλνει στην Αρχή Χρονοσφράγισης ένα αίτημα για ασφαλή χρονοσφράγιση, το οποίο αποτελείται από μια σύνοψη της πληροφορίας. Η σύνοψη της πληροφορίας έχει προκύψει από τη χρήση μιας συνάρτησης κατακερματισμού. Όταν η Αρχή Χρονοσφράγισης λάβει το αίτημα του πελάτη, επισυνάπτει στη σύνοψη της πληροφορίας τον χρόνο στον οποίο την έλαβε. Το μήνυμα που προκύπτει υπογράφεται ψηφιακά με το ιδιωτικό κλειδί της Αρχής Χρονοσφράγισης και αποτελεί πλέον την σφραγίδα χρόνου η οποία αποστέλλεται στον πελάτη.

3.5.8 Συμβολαιογραφία (Notarization)

Η υπηρεσία ασφαλούς *ψηφιακής συμβολαιογραφίας* είναι για τις ανάγκες μιας Υποδομής Δημοσίου Κλειδιού συνώνυμη με την έννοια της πιστοποίησης δεδομένων. Αυτό σημαίνει ότι η συγκεκριμένη υπηρεσία πιστοποιεί την εγκυρότητα ή την ορθότητα

δεδομένων. Για παράδειγμα, ένα ηλεκτρονικό συμβολαιογραφείο μπορεί να θεωρήσει έγκυρη μία ψηφιακή υπογραφή αφού κάνει τους εξής ελέγχους:

- Η υπογραφή επαληθεύεται με τη χρήση του αντίστοιχου δημοσίου κλειδιού
- Το δημόσιο κλειδί ανήκει πράγματι στην οντότητα που ισχυρίζεται ότι έχει δημιουργήσει την ψηφιακή υπογραφή.
- Όλα τα υπόλοιπα στοιχεία που χρειάζονται για την επαλήθευση της υπογραφής (όπως πρόσθετα πιστοποιητικά για τον έλεγχο μονοπατιών πιστοποίησης) είναι διαθέσιμα και αξιόπιστα .

Το συμβολαιογραφείο μιας ΥΔΚ είναι μια οντότητα την οποία εμπιστεύεται ένα σύνολο άλλων οντοτήτων ΥΔΚ ως προς το ότι διεκπεραιώνει σωστά την υπηρεσία συμβολαιογραφίας. Μετά την επαλήθευσή τους, τα δεδομένα υπογράφονται ψηφιακά και χρονοσφραγίζονται.

3.5.9 Διαχείριση προνομίων (Privilege management)

Ο όρος *διαχείριση προνομίων* είναι ένα γενικός όρος που περιλαμβάνει έννοιες όπως η εξουσιοδότηση, ο έλεγχος πρόσβασης, η διαχείριση δικαιωμάτων, η διαχείριση άδειας κοκ. Η υπηρεσία μέσα από κάποιους κανόνες καθορίζει τι μπορεί και τι δεν μπορεί να κάνει μια οντότητα ή μια ομάδα οντοτήτων μέσα σε ένα συγκεκριμένο περιβάλλον. Η διαχείριση προνομίων δημιουργεί και ενισχύει αυτούς τους κανόνες διατηρώντας με αυτόν τον τρόπο ένα επιθυμητό επίπεδο ασφάλειας.

3.6 Προϋποθέσεις Χρήσης Υποδομής PKI

Για να μπορέσει να αξιοποιηθεί η Υποδομή Δημοσίου Κλειδιού PKI και οι εφαρμογές που αυτή παρέχει θα πρέπει να γίνουν και οι ακόλουθες ενέργειες που περιγράφουν τη γενικότερη κατεύθυνση αλλαγής του.

Ενέργειες που θα πρέπει να γίνουν:

- Κατηγοριοποίηση των υπηρεσιών που παρέχονται ώστε να δημιουργηθούν οι κατάλληλες υποδομές για την ταυτοποίηση των χρηστών με χρήση PKI όπου αυτό απαιτείται (3ου και 4ου επιπέδου υπηρεσίες).
- Επιμόρφωση των υπαλλήλων που εμπλέκονται στις διαδικασίες που υλοποιούν τις προσφερόμενες υπηρεσίες Ηλεκτρονικής Διακυβέρνησης όσον αφορά τη χρήση και εφαρμογή του PKI, την αναγνώριση της ταυτότητας των χρηστών, την κρυπτογράφηση αλλά και υπογραφή εγγράφων.
- Αναβάθμιση των εφαρμογών που υπάρχουν σήμερα και δεν υποστηρίζουν τη δυνατότητα χρήσης Ψηφιακών Πιστοποιητικών.
- Δημιουργία πολιτικής ασφαλείας και πολιτικής διαχείρισης δικαιωμάτων χρηστών στις εφαρμογές αλλά και διαχείριση αυτών.
- Δημιουργία λίστας εργαζομένων που θα πρέπει να αποκτήσουν ψηφιακό πιστοποιητικό από την Υποδομή PKI ώστε να μπορούν να κάνουν χρήση των δυνατοτήτων που προσφέρονται όπου αυτή απαιτείται.
- Αναγνώριση των σταθμών εργασίας που απαιτούν την υποστήριξη Ψηφιακών Πιστοποιητικών ώστε να γίνει προμήθεια των απαραίτητων αναγνωστών καρτών αλλά και του αντίστοιχου λογισμικού για τη χρήση της Ψηφιακής Υπογραφής όπου δεν διατίθεται.
- Παροχή λογαριασμών e-mail σε όλα τα στελέχη που απαιτείται να ανταλλάξουν πληροφορίες με τρίτους φορείς ώστε να μπορεί να γίνει η επικοινωνία αυτή γρηγορότερη αλλά και να υποστηρίζει τη χρήση Ψηφιακών Πιστοποιητικών.

4 Παρουσίαση Windows Server 2008

4.1 Γενικά

Ο Windows Server 2008 είναι ένα λειτουργικό σύστημα της εταιρείας Microsoft το οποίο, όπως λέει το όνομά του, κυκλοφόρησε το 2008. Ήταν ο διάδοχος του Windows Server 2003 και βασίζεται στον πυρήνα Windows NT 6.0, όπως και τα Windows Vista που είχαν κυκλοφορήσει νωρίτερα. Πρόκειται για ένα από τα ποιο διαδεδομένα λειτουργικά συστήματα για διακομιστές και είναι εγκαταστημένο σε οργανισμούς διαφόρων μεγεθών, από μικρές εταιρείες μέχρι μεγάλους οργανισμούς.

Παρόλο που έχει κυκλοφορήσει εδώ και τέσσερα χρόνια, η φύση των εργασιών που επιτελεί ένας διακομιστής καθιστά την αντικατάστασή του λειτουργικού του συστήματος μία επίπονη και χρονοβόρα διαδικασία, ενώ λόγοι για την αναβάθμισή του είναι μόνο η έλλειψη κάποιων δυνατοτήτων που υπάρχουν σε μία μεταγενέστερη έκδοση ή η λήξη της επίσημης υποστήριξής του. Αν και πλέον δεν πωλείται αφού έχει αντικατασταθεί από την έκδοση 2012, έχει αποδειχθεί πως είναι ένα αξιόπιστο σύστημα το οποίο συνεχίζεται να χρησιμοποιείται. Οι περισσότεροι χρήστες του θα συνεχίσουν να το χρησιμοποιούν τουλάχιστον μέχρι το 2015 οπότε και η Microsoft έχει ανακοινώσει πως θα σταματήσει την υποστήριξή του ή μέχρι το 2020 για τους χρήστες που κάνουν χρήση της υπηρεσίας εκτεταμένης υποστήριξης.

Τον Νοέμβριο του 2009 κυκλοφόρησε η δεύτερη έκδοση Windows Server 2008 R2, οποία είναι και η τρέχουσα έκδοση του λειτουργικού, ενώ τον Σεπτέμβριο του 2012 κυκλοφόρησε ο Windows Server 2012.

4.2 Εκδόσεις

Το λειτουργικό σύστημα έχει κυκλοφορήσει σε διαφορετικές εκδόσεις και για διάφορες αρχιτεκτονικές. Υποστηρίζονται πλατφόρμες 32 και 64 bit με τις αρχιτεκτονικές IA-32 και x86-64 αντίστοιχα, ενώ υποστηρίζονται και επεξεργαστές Itanium με αρχιτεκτονική IA-64.

Επιπλέον υπάρχουν αρκετές εκδόσεις του λειτουργικού για διαφορετικά σενάρια χρήσης. Αυτές είναι:

- Windows Server 2008 Standard (για συστήματα με αρχιτεκτονική IA-32 και x86-64)η οποία είναι η βασική έκδοση.
- Windows Server 2008 Enterprise (για συστήματα με αρχιτεκτονική IA-32 και x86-64) που απευθύνεται σε μεγάλους οργανισμούς.
- Windows Server 2008 Datacenter (για συστήματα με αρχιτεκτονική IA-32 και x86-64) που δίνει έμφαση στην ομαλή εκτέλεση εφαρμογών διαχείρισης βάσεων δεδομένων.
- Windows HPC Server 2008 που στοχεύει σε υπολογιστές υψηλής απόδοσης.
- Windows Web Server 2008 (για συστήματα με αρχιτεκτονικήIA-32 και x86-64) με έμφαση στην χρήση σαν διακομιστής διαδικτύου.
- Windows Storage Server 2008 (για συστήματα με αρχιτεκτονική IA-32 και x86-64) που στοχεύει στην χρήση σαν διακομιστής αποθήκευσης.
- Windows Small Business Server 2008 (για συστήματα με αρχιτεκτονική x86-64) που απευθύνεται σε μικρές επιχειρήσεις.
- Windows Essential Business Server 2008 (για συστήματα με αρχιτεκτονική x86-64) για επιχειρήσεις μεσαίου μεγέθους.
- Windows Server 2008 for Itanium-based Systems για συστήματα με αρχιτεκτονική IA-64.

Η πληθώρα εκδόσεων είχε προκαλέσει αρκετά αρνητικά σχόλια, καθώς αρκετές εκδόσεις έχουν παρόμοιες δυνατότητες και διαφέρουν σε ελάχιστα σημεία, κάνοντας την επιλογή μίας έκδοσης δύσκολη.

4.2.1 Windows Server 2008 R2

Τον Νοέμβριο του 2009 κυκλοφόρησε η δεύτερη έκδοση του Windows Server, με όνομα Windows Server 2008 R2 (release 2). Η νέα έκδοση είχε αρκετές βελτιώσεις και επιπλέον δυνατότητες. Χαρακτηριστικά προστέθηκαν αρκετές επιλογές διαχείρισης εικονικών συστημάτων και βελτιώθηκε σημαντικά η απόδοση των αποθηκευτικών συστημάτων. Βασίζεται στον πυρήνα των Windows NT 6.1, όπως και τα Windows 7.

Πρέπει να σημειωθεί πως οι εκδόσεις του Windows Server R2 διαφέρουν από αυτές της πρώτης έκδοσης:

- Windows Server2008 R2Foundation (για συστήματα με αρχιτεκτονική x86-64), που είναι η πιο οικονομική έκδοση για γενική χρήση, χωρίς δυνατότητα χρήσης σαν εικονική μηχανή.
- Windows Server 2008 R2 Essentials (για συστήματα με αρχιτεκτονική x86-64), που απευθύνεται σε μικρές επιχειρήσεις, Έχει αρκετές εφαρμογές ήδη ρυθμισμένες και έτοιμες για χρήση.
- Windows Server 2008 R2 Standard (για συστήματα με αρχιτεκτονική x86-64) που απευθύνεται σε επιχειρήσεις μεσαίου μεγέθους. Έχει όλη την λειτουργικότητα ενώ δίνει και την δυνατότητα χρήσης με δύο εικονικές μηχανές.
- Windows Server 2008 R2 Datacenter (για συστήματα με αρχιτεκτονική x86-64) με στόχο την χρήση του σε datacenters.
- Windows Server 2008 R2 HPC (για συστήματα με αρχιτεκτονική x86-64) για χρήση σε συστήματα υψηλών επιδόσεων.
- Windows Server 2008 R2 Web (για συστήματα με αρχιτεκτονική x86-64) που παρέχεται σαν εικονική μηχανή για χρήση σαν διακομιστής διαδικτύου.
- Windows Server 2008 R2 Itanium για χρήση σε συστήματα αρχιτεκτονικής IA-64. Έχει περίπου τις ίδιες δυνατότητες με την έκδοση datacenter.

4.3 Απαιτήσεις συστήματος

Οι απαιτήσεις των Windows Server 2008 φαίνονται στον παρακάτω πίνακα.

	Ελάχιστες απαιτήσεις	**Προτεινόμενες απαιτήσεις**
Επεξεργαστής	1 GHz (IA-32) ή 1.4 GHz (x86-64) ή Intel Itanium 2	2 GHz ή μεγαλύτερος
Μνήμη	512 MBRAM (μπορεί να περιορίσει τις επιδόσεις και την διαθεσιμότητα κάποιων δυνατοτήτων)	2 GB RAM ή παραπάνω Μέγιστη (συστήματα32-bit): 4 GB RAM (Standard) ή 64 GB RAM (Enterprise, Datacenter) Μέγιστη (συστήματα64-bit): 8 GB (Foundation) ή 32 GB RAM (Standard) ή 2 TB RAM (Enterprise, Datacenter και Itanium)

Κάρτα γραφικών	Super VGA (800 × 600)	
Σκληρός	ΈκδοσηFoundation: 10 GBή περισσότερο. Άλλες εκδόσεις: Συστήματα 32-bit: 20 GBή περισσότερο. Συστήματα 64-bit: 32 GBή περισσότερο.	40 GB ή περισσότερο.
Οπτικά μέσα	DVD-ROM	
Άλλες	Οθόνη Super VGA (800 × 600)ή με μεγαλύτερη ανάλυση, πληκτρολόγιο και ποντίκι	

Αξίζει να σημειωθεί ότι οι παραπάνω απαιτήσεις αφορούν μόνο την εκτέλεση του λειτουργικού συστήματος, ενώ στα περισσότερα σενάρια χρήσης χρειάζονται αρκετά περισσότεροι πόροι για την εκτέλεση των υπόλοιπων εφαρμογών που θα τρέχει ο διακομιστής.

4.4 Παρουσίαση δυνατοτήτων

Σε αυτή την ενότητα θα παρουσιάσουμε κάποια βασικά στοιχεία του λειτουργικού συστήματος. Καθώς τα Windows Server 2008 είναι ένα πλήρες λειτουργικό σύστημα εξυπηρετητή που μπορεί να καλύψει μία πληθώρα αναγκών και ρόλων η απαρίθμηση όλων των δυνατοτήτων και των στοιχείων του δεν είναι πρακτική και υπερβαίνει τους στόχους της παρουσίασής μας.

Αντίθετα θα δοθεί βάρος στα στοιχεία και τα εργαλεία που είναι απαραίτητα για την ρύθμιση ενός δικτύου και την προετοιμασία του ώστε να υποστηρίξει την υποδομή δημόσιου κλειδιού.

4.4.1 Windows domain

Στα πλαίσια ενός δικτύου ένα Windows domain είναι μία ομάδα ελεγκτών δικτύου που μοιράζονται κοινές πληροφορίες ασφαλείας μέσω μίας κεντρικής βάσης δεδομένων. Η κεντρική βάση δεδομένων βασίζεται στην τεχνολογία Active Directory της εταιρείας Microsoft. Κάθε χρήστης που χρησιμοποιεί οποιονδήποτε υπολογιστή στο δίκτυο έχει έναν προσωπικό λογαριασμό που χαρακτηρίζεται από το όνομα χρήστη του (username).

Ένας υπολογιστή μπορεί να συνδεθεί σε ένα domain μέσω τοπικού δικτύου LAN, απομακρυσμένου δικτύου (WAN) ή εικονικού ιδιωτικού δικτύου (VPN).Οι servers που αναλαμβάνουν την διαπίστευση των χρηστών σε ένα Windows domainονομάζονται domain controllers.

4.4.2 Active Directory

Το Active Directory (Ενεργός Κατάλογος) είναι μία υπηρεσία καταλόγου που δημιουργήθηκε από την Microsoft και χρησιμοποιείται από όλες τις εκδόσεις των Windows Server.

Η τεχνολογία παρέχει μία κεντρική υπηρεσία που αναλαμβάνει την διαχείριση και την ασφάλεια του δικτύου. Ένας serverπου λειτούργει σαν domain controller, δηλαδή που

τρέχει αυτή την υπηρεσία αναλαμβάνει να πιστοποιήσει την ταυτότητα των χρηστών και να τους δώσει πρόσβαση στο δίκτυο που ανήκει σε αυτό το domain, επιβάλλοντας τους κανόνες ασφάλειας και τα δικαιώματα πρόσβασης που έχουν καθοριστεί για κάθε χρήστη.

Η δομή ενός καταλόγου Active Directory είναι μία ιεραρχική δομή αντικειμένων, με κάθε αντικείμενο να ανήκει σε μία από δύο κατηγορίες: Είτε πρόκειται για πόρους του δικτύου, όπως για παράδειγμα εκτυπωτές, είτε πρόκειται για οντότητες οι οποίες πρέπει να πιστοποιηθούν πριν αποκτήσουν πρόσβαση στους πόρους του δικτύου (χρήστες, ομάδες χρηστών, προγράμματα). Αυτές οι οντότητες ονομάζονται security principals. Σε κάθε μία από αυτές δίνεται ένας μοναδικό αναγνωριστικό ασφάλειας (security identifier - SID).

Κάθε αντικείμενο μέσα σε έναν τέτοιο κατάλογο αναπαριστά μία από τις προηγούμενες οντότητες και τις ιδιότητές της. Οι ιδιότητες που μπορεί να έχει κάθε αντικείμενο ορίζονται από ένα σχήμα (schema object), το οποίο καθορίζει και τα είδη των αντικειμένων που μπορεί να περιέχει ο κατάλογος. Οι διαχειριστές του δικτύου μπορούν να τροποποιήσουν το σχήμα των αντικειμένων τροποποιώντας τις υπάρχουσες ιδιότητες ή εισάγοντας νέες. Όμως επειδή το σχήμα καθορίζει τον τρόπο με τον οποίο αποθηκεύονται τα αντικείμενα στον κατάλογο οποιαδήποτε αλλαγή στο σχήμα μπορεί να δημιουργήσει προβλήματα στην χρήση των αντικειμένων που είναι ήδη αποθηκευμένα. Η δημιουργία του σχήματος γίνεται μετά από μεγάλη προεργασία και η τροποποίηση του χρειάζεται να γίνεται με μεγάλη προσοχή ώστε να μην δημιουργήσει προβλήματα στο δίκτυο.

4.4.2.1 Sites

Ένα sitεσε ένα domainαναφέρεται σε μία γεωγραφική τοποθεσία. Χρησιμοποιείται για την καλύτερη οργάνωση των πόρων του δικτύου και δεν έχει επίπτωση στους κανόνες που ισχύουν για τα αντικείμενα που ανήκουν σε αυτό, εκτός και αν οριστούν ειδικοί κανόνες.

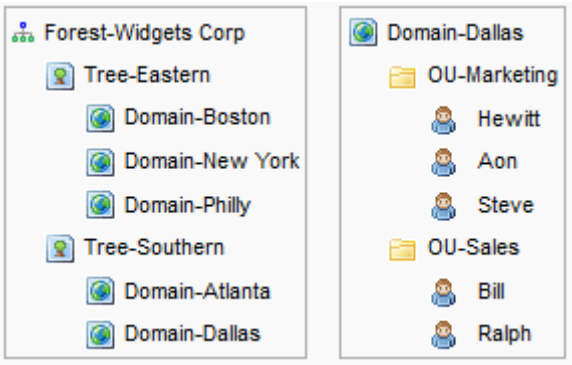
4.4.2.2 Δάση και δέντρα

Ο κατάλογος ενός Active Directory χωρίζεται σε τρία λογικά επίπεδα, τα δάση, τα δέντρα και τα domains.

Σε κάθε δίκτυο τα αντικείμενα που το αποτελούν ανήκουν σε συγκεκριμένα domains. Οι πληροφορίες για όλα τα αντικείμενα ενός domain αποθηκεύονται σε μία συγκεκριμένη βάση δεδομένων, ενώ κάθε domain έχει ένα όνομα που ανήκει σε έναν συγκεκριμένο χώρο ονομάτων. Ένα δέντρο είναι μία ομάδα από domainsτα οποία ανήκουν και αυτά σε έναν συγκεκριμένο χώρο ονομάτων.

Ένα δάσος με τη σειρά του αποτελείται από πολλά δέντρα τα οποία μοιράζονται ένα κοινό σχήμα Active Directory. Το δάσος είναι το όριο μέσα στο οποίο καθορίζονται τα δικαιώματα ενός αντικειμένου που βρίσκεται στο Active Directory.

Στην εικόνα 4-3 φαίνεται ένα τυπικό παράδειγμα των τριών επιπέδων ενός Active Directory. Αριστερά φαίνεται το δάσος, το οποίο αναφέρεται στα γραφεία μίας υποθετικής εταιρείες. Αυτό χωρίζεται σε δύο δέντρα βάση της γεωγραφικής θέσης τους, με τα domain να αναφέρονται σε κάθε πόλη.



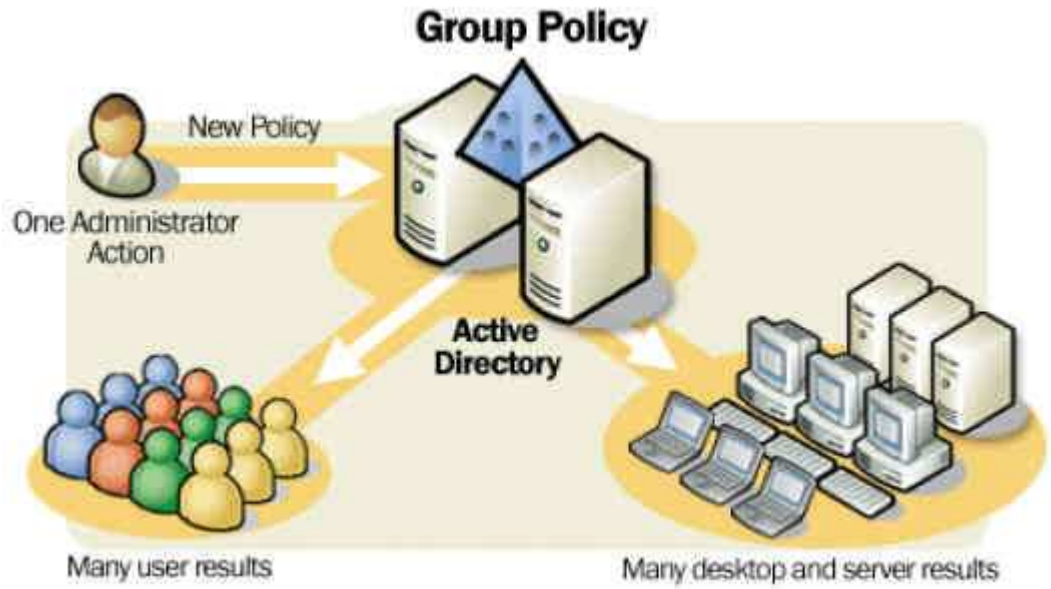
Εικόνα 4-1 Τα τρία επίπεδα ενός Active Directory.

Ένα Organizational Unit (OU – Μονάδα οργάνωσης) είναι μία ομάδα αντικειμένων ενός domain. Η οργάνωση μπορεί να γίνει για λόγους ευκολίας διαχείρισης ή αναπαράστασης μίας λογικής ιεραρχίας, καθώς κάθε Organizational Unit μπορεί να περιέχει άλλα Organizational Unit.

4.4.3 Group policy

Το Group Policy (Πολιτική Ομάδας) είναι μία δυνατότητα που παρέχεται από το λειτουργικό σύστημα Windows Server για την ρύθμιση των παραμέτρων των λογαριασμών των χρηστών σε κάθε υπολογιστή του δικτύου. Προσφέρουν την δυνατότητα συγκεντρωτικής διαχείρισης και ρύθμισης των συστημάτων που ανήκουν στο δίκτυο.

Ο ρόλος των Group Policies είναι να καθορίσουν ακριβώς τα δικαιώματα κάθε χρήστη που έχει πρόσβαση σε έναν υπολογιστή του δικτύου θέτοντας συγκεκριμένους κανόνες. Αποτελούνται από κανόνες που καθορίζουν και επιβάλλουν συγκεκριμένες πολιτικές στους χρήστες, οι οποίοι μπορεί να εκτείνονται από το μέγεθος του κωδικού που επιτρέπεται να χρησιμοποιήσουν μέχρι να επιτρέψουν ή να απαγορεύσουν την δυνατότητα πρόσβασης ενός χρήστη σε κάποιους φακέλους του μηχανήματος του ή στους πόρους του δικτύου. Ένα σύνολο τέτοιων κανόνων ονομάζεται Group Policy Object.



Εικόνα 4-2 Η πολιτική αυτόματης ανανέωσης των group policies μέσω του Active Directory.

Ένα Group Policy Object μπορεί να βρίσκεται σε έναν υπολογιστή ή να βρίσκεται στο Active Directory ενός domain. Τα μηχανήματα που ανήκουν σε αυτό το

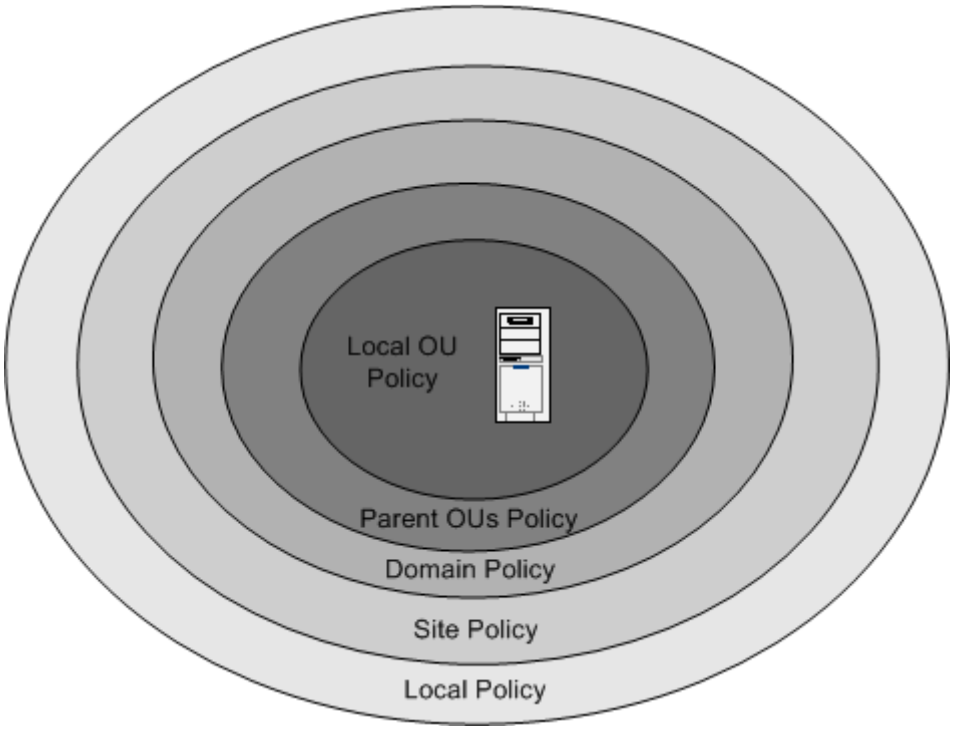
domainανανεώνουν αυτόματα ανά τακτά χρονικά διαστήματα τα Group Policy Objects ζητώντας από τον domain controller να ενημερωθούν για αλλαγές στα υπάρχοντα ή για προσθήκη νέων. Όπως δείχνει το σχήμα 4-2 μέσω των group policies και της αυτόματης ανανέωσής τους με το Active Directory ο διαχειριστής ενός δικτύου μπορεί να κάνει αλλαγές που να εφαρμοστούν αυτόματα σε πολλούς χρήστες ή υπολογιστές του δικτύου.

4.4.3.1 Ιεραρχία

Ένα Group Policy Object δεν αναφέρεται απαραίτητα σε έναν υπολογιστή, αλλά μπορεί να έχει διαφορετικό εύρος εφαρμογής. Ο τύπος και η σειρά με την οποία επεξεργάζονται φαίνεται παρακάτω:

- Local: Αρχικά επεξεργάζονται οι κανόνες που αναφέρονται στον υπολογιστή υπολογιστή. Αυτοί οι κανόνες μπορούν να διαφέρουν ανάλογα με τον λογαριασμό του χρήστη που χρησιμοποιεί τον υπολογιστή.
- Site: Έπειτα επεξεργάζονται οι κανόνες που είναι συσχετισμένοι στο Active Directory με την τοποθεσία στην οποία ανήκει ο υπολογιστής.
- Domain: Μετά επεξεργάζονται οι κανόνες που ισχύουν για todomainστο οποίο ανήκει ο υπολογιστής.
- Organizational Unit: Τέλος επεξεργάζονται οι κανόνες που ισχύουν για την μονάδα οργάνωσης του υπολογιστή.

Αν βρεθούν δύο αντικρουόμενοι κανόνες τότε υπερισχύει αυτός που επεξεργάστηκε τελευταίος, οπότε για παράδειγμα ένας κανόνας για ένα domainθα υπερισχύσει σε σχέση με έναν αντικρουόμενο κανόνα που βρίσκεται σε έναν υπολογιστή.



Εικόνα 4-3 Η ιεραρχία με την οποία επιβάλλονται τα Group Policies.

4.4.3.2 Κληρονομικότητα

Εξ' ορισμού ένα Group Policy που έχει οριστεί μέσα στα πλαίσια μίας ιεραρχικής δομής ισχύει και για όλα τα παιδιά της εκτός και αν περιέχουν ρητά κάποιον κανόνα που το αντικρούει. Αν αυτό δεν είναι επιθυμητό μπορεί να απενεργοποιηθεί.

4.4.3.3 Επιλεκτική επιβολή

Το εύρος εφαρμογής ενός Group Policy μπορεί να περιοριστεί ή να περιοριστεί συσχετίζοντας το με συγκεκριμένες συνθήκες εφαρμογής, όπως για παράδειγμα το λογισμικό που είναι εγκαταστημένο σε ένα μηχάνημα ή τις τεχνικές προδιαγραφές του.

5 Ρύθμιση της υποδομής δημοσίου κλειδιού

5.1 Γενικά

Σε αυτό το κεφάλαιο θα αναλύσουμε την διαδικασία ρύθμισης του συστήματος Windows Server 2008. Όπως αναφέρθηκε παραπάνω χρησιμοποιήσαμε ένα σύστημα που έτρεχε λειτουργικό Windows Server 2008 R2 σαν server, ενώ ο client ήταν ένα σύστημα με Windows 7 Professional.

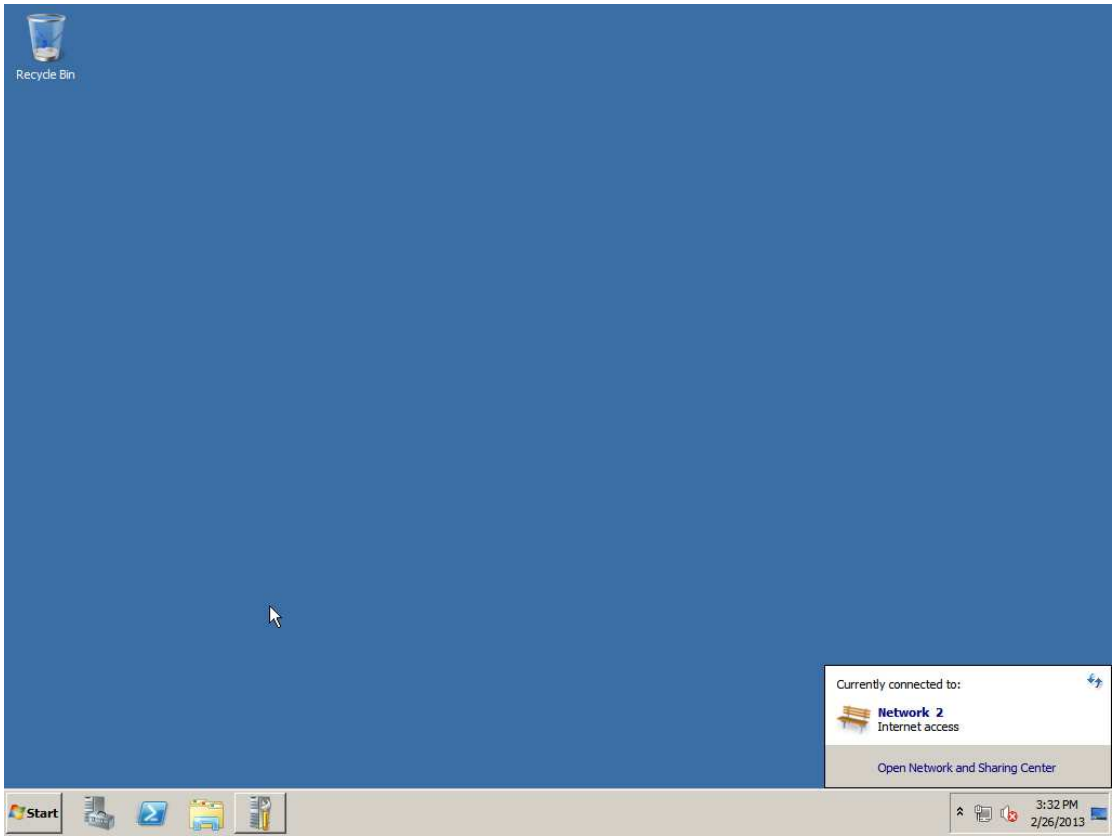
Η εγκατάσταση του Windows Server 2008 είναι εξαιρετικά απλή. Κατά την διάρκειά της γίνονται ερωτήσεις μόνο για τον σκληρό δίσκο που θα εγκατασταθούν και για τον κωδικό του διαχειριστή.

Η εγκατάσταση των Windows 7 πέρα από τα παραπάνω ζητάει κάποιες βασικές πληροφορίες για το είδος του δικτύου στο οποίο είναι συνδεδεμένος ο υπολογιστής και τις ρυθμίσεις λήψης των αναβαθμίσεων. Αυτές οι επιλογές δεν παίζουν ιδιαίτερο ρόλο, καθώς από την στιγμή που ο υπολογιστής θα γίνει μέρος ενός domain, θα αντικατασταθούν από τα group policies που στέλνονται από τον domain controller.

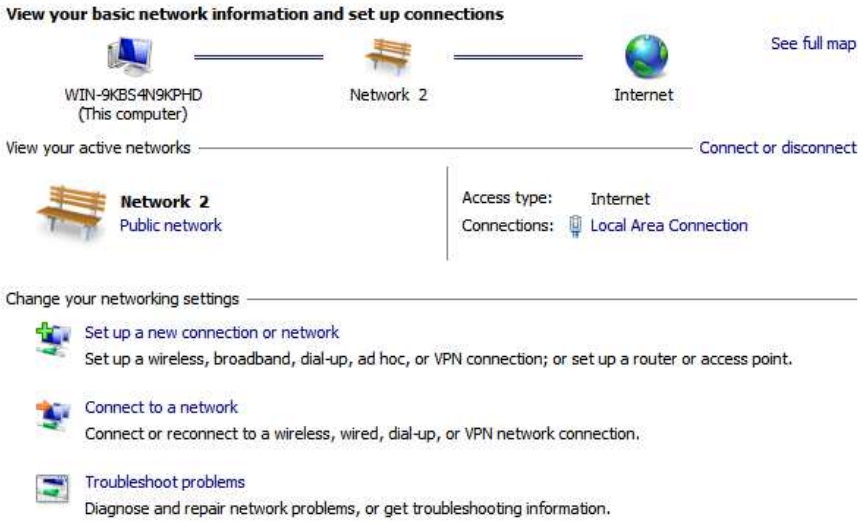
5.2 Απόδοση σταθερής διεύθυνσης IP

Κάθε υπολογιστής σε ένα τοπικό δίκτυο χρειάζεται να έχει μία μοναδική διεύθυνση IP. Σε ένα τυπικό οικιακό δίκτυο αυτές οι ρυθμίσεις αποδίδονται αυτόματα από το DSL modem / router με χρήση του πρωτοκόλλου DHCP. Με αυτόν τον τρόπο κάθε φορά που ένας υπολογιστής συνδέεται στο δίκτυο παίρνει αυτόματα μία ελεύθερη διεύθυνση IP. Το μειονέκτημα αυτής της διαδικασίας είναι πως ο υπολογιστής δεν έχει πάντα την ίδια διεύθυνση, γεγονός που μπορεί να δημιουργήσει προβλήματα ασφαλείας όταν πρόκειται για έναν server.

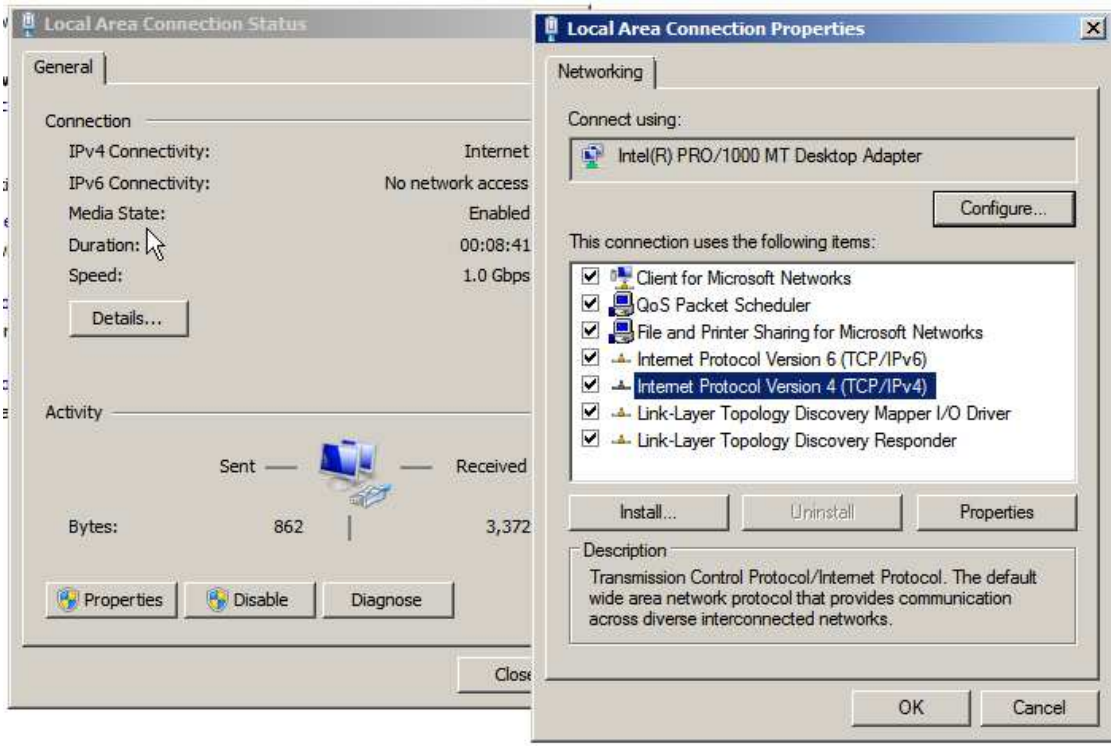
Καθώς κατά την ρύθμιση του PKI μπορούν να παρουσιαστούν προβλήματα με την χρήση του DHCP, χρειάζεται να εισάγουμε μία σταθερή διεύθυνση IP στον server. Αυτό γίνεται κάνοντας κλικ στο εικονίδιο της σύνδεσης δικτύου και επιλέγοντας το Open network and sharing center.



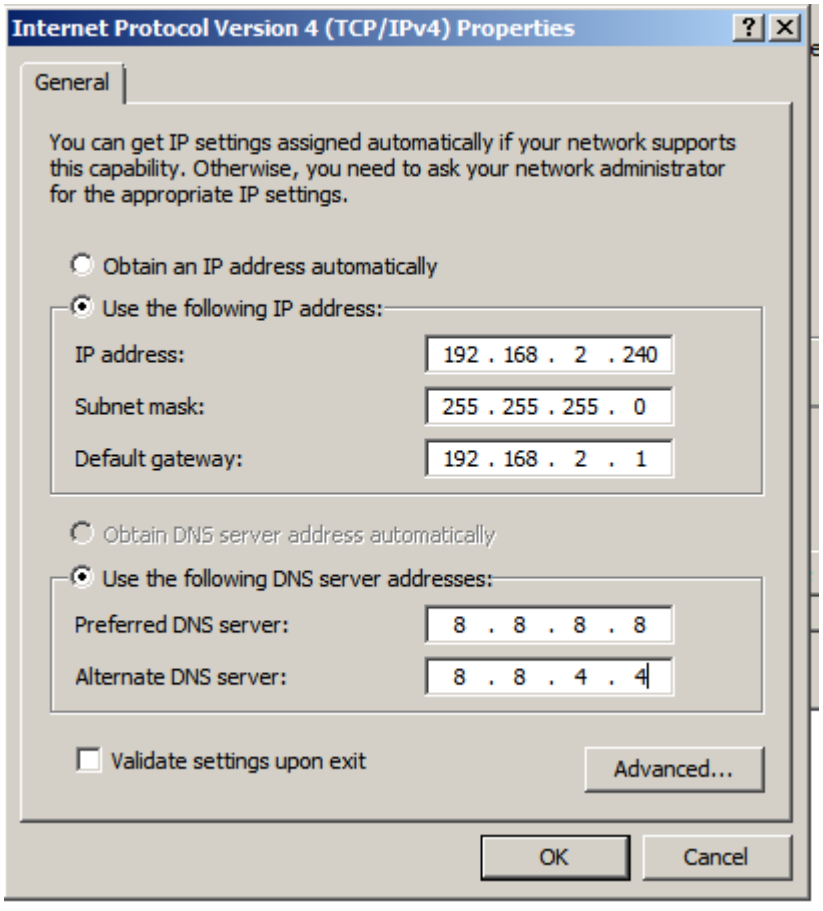
Έπειτα κάνουμε κλικ στην σύνδεση Local Area Connection.



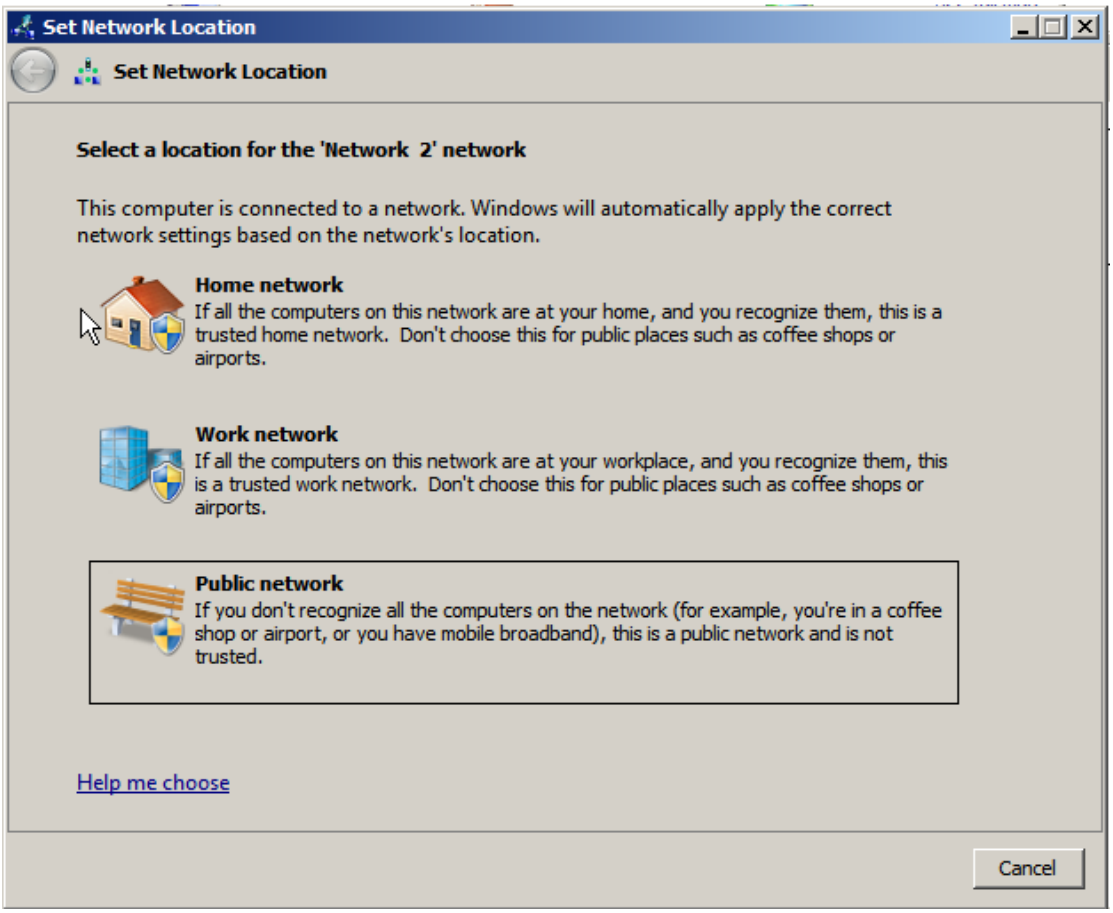
Από το παράθυρο των επιλογών διαλέγουμε το Properties και από την λίστα των συνδέσεων το Internet Protocol Version 4 και ξανά το Properties.



Τέλος εισάγουμε τις επιθυμητές διευθύνσεις δικτύου, οι οποίες εξαρτώνται από το εκάστοτε δίκτυο.



Με το πέρας της διαδικασίας είναι απαραίτητο από το Network and Sharing Center να αλλάξουμε τον χαρακτηρισμό του τρέχοντος δικτύου σε Private Network.

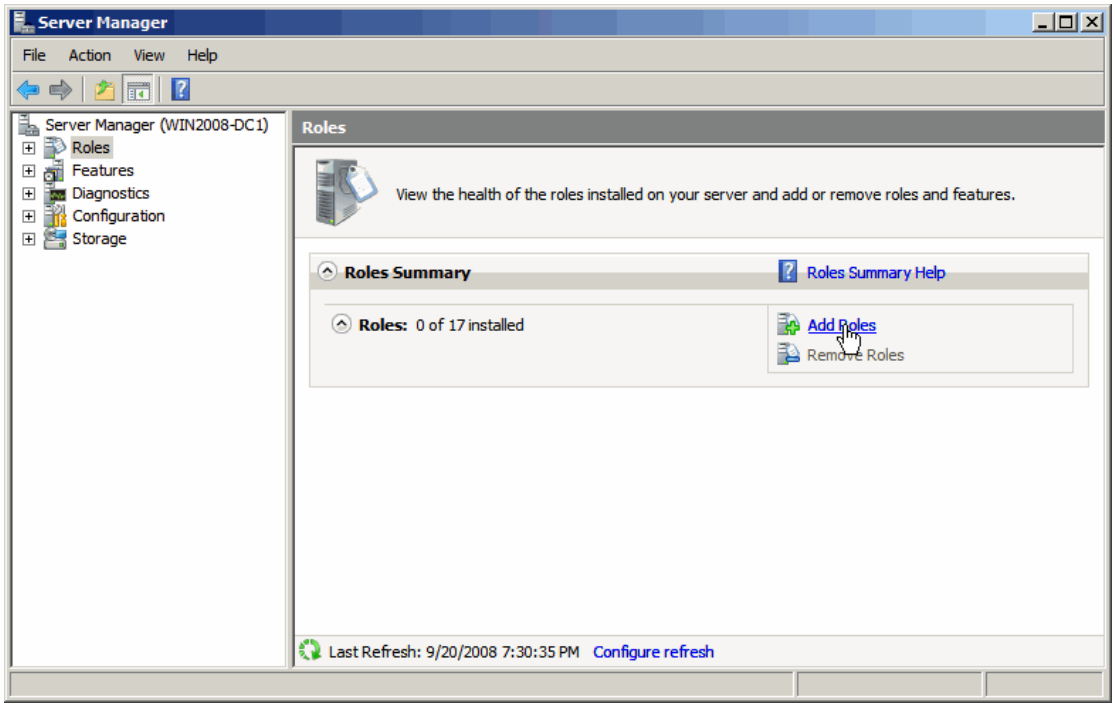


Αν και παραπάνω αναθέσαμε μία σταθερή διεύθυνση για το πρωτόκολλο IPv4, σε ένα δίκτυο που κάνει χρήση της έκδοσης 6 του πρωτοκόλλου είναι απαραίτητη η ανάθεση σταθερών διευθύνσεων και για αυτό. Αυτό σημαίνει ότι στο πλαίσιο που προβάλει τα υποστηριζόμενα πρωτόκολλα θα έπρεπε να γίνει παρόμοια διαδικασία για το Internet Protocol Version 6.

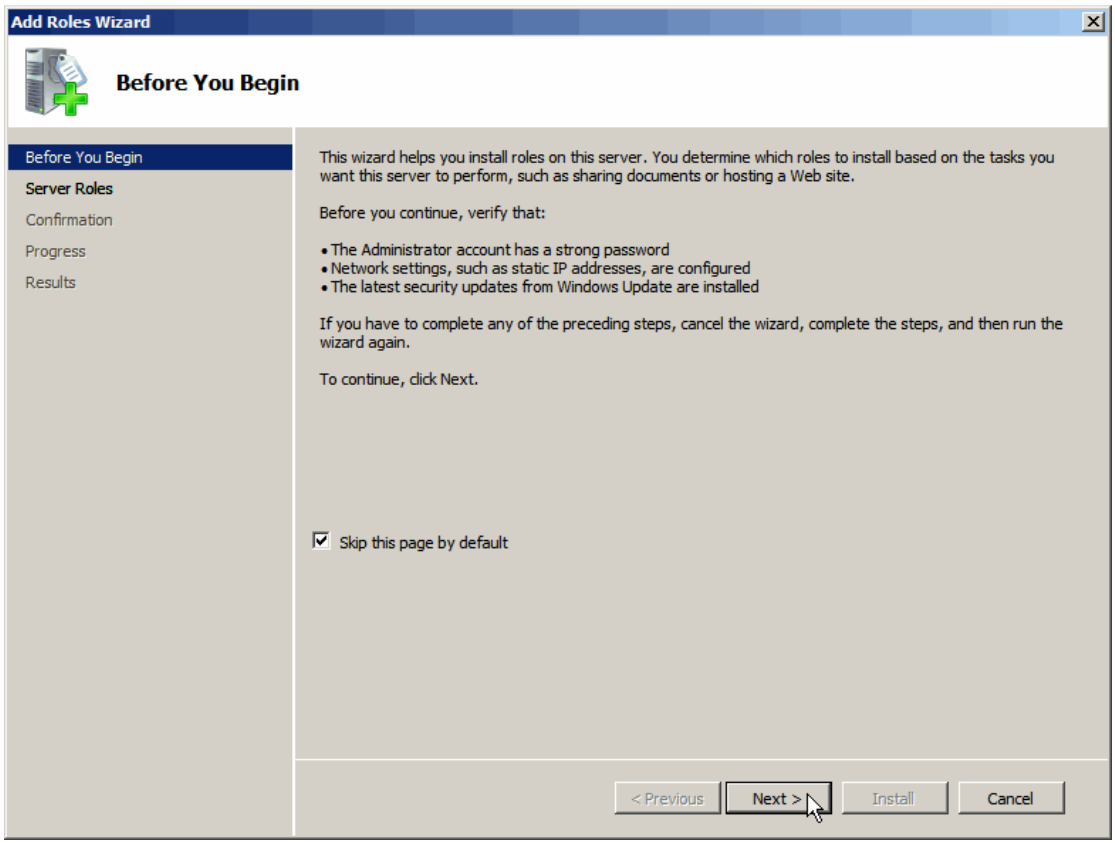
5.3 Ρύθμιση Active Directory

Το επόμενο βήμα είναι η ρύθμιση του Active Directory, ώστε να δημιουργήσουμε το περιβάλλον για την διαμόρφωση του PKI.

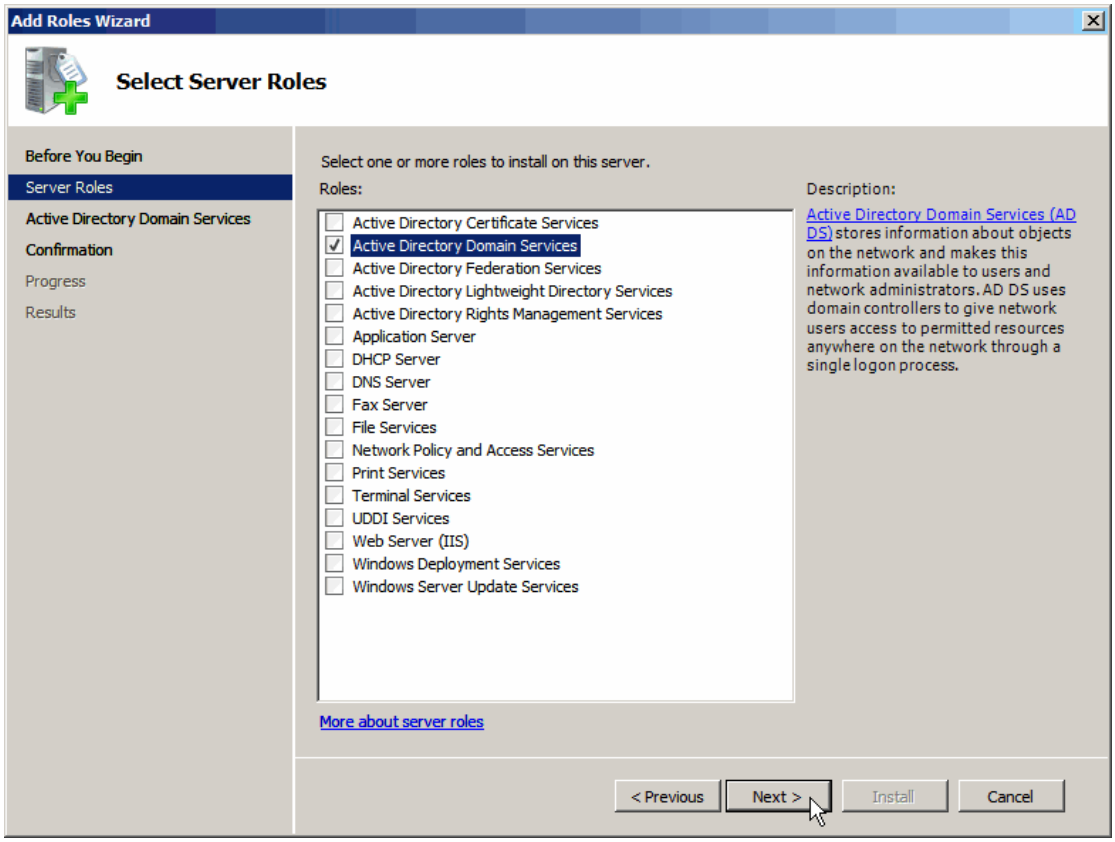
Ξεκινάμε με την εκκίνηση του Εργαλείου Server Manager από την μπάρα εργασιών. Από το δέντρο με τις επιλογές επιλέγουμε το Roleskαι έπειτα την επιλογή Add Role.



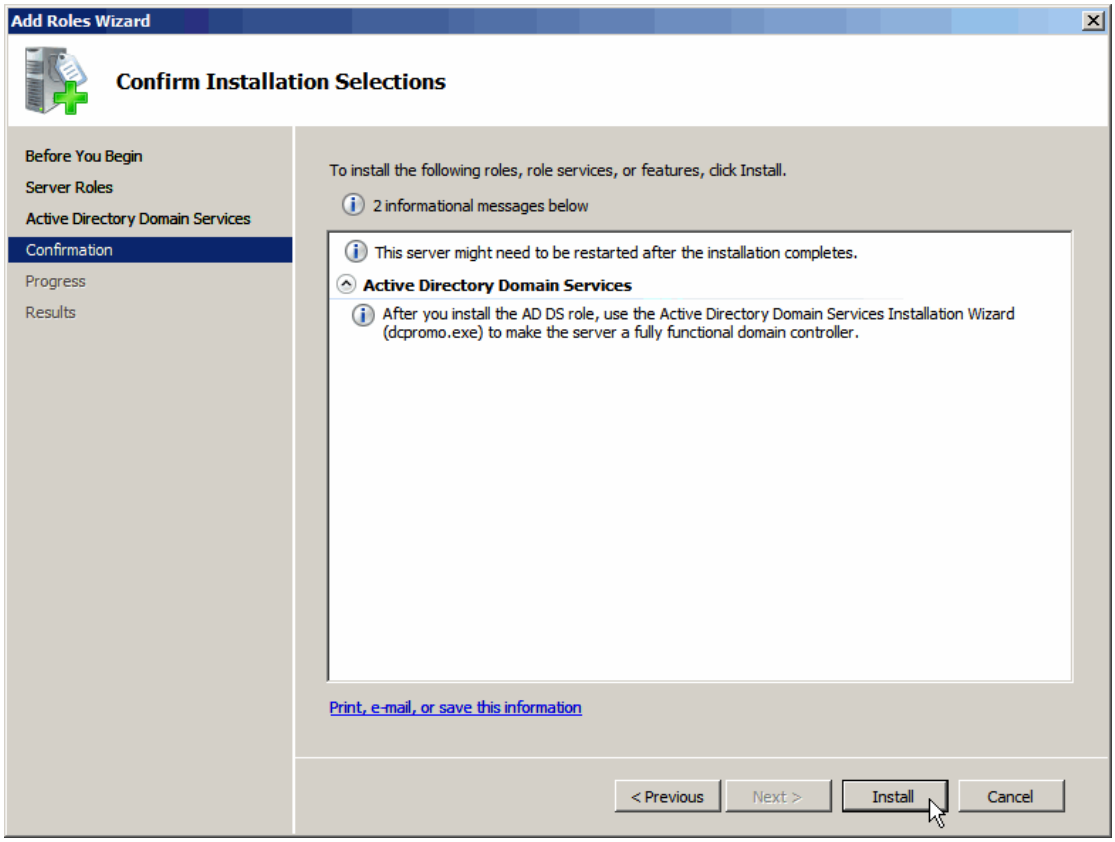
Η επόμενη οθόνη δίνει κάποιες βασικές οδηγίες σχετικά με την εγκατάσταση ρόλων.



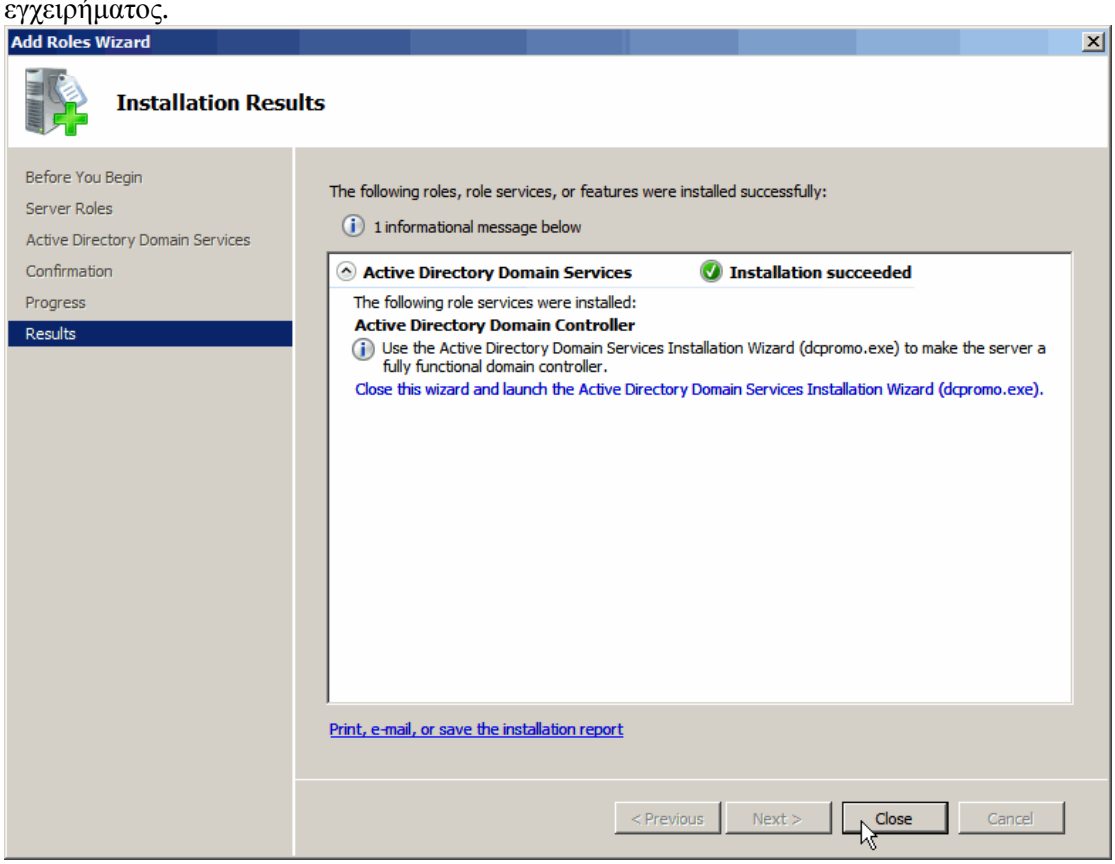
Έπειτα χρειάζεται να επιλέξουμε τις υπηρεσίες που θέλουμε να εκτελεί ο Server. Σε αυτό το στάδιο μας ενδιαφέρει απλά το Active Directory Domain Services.



Οι επόμενες οθόνες δίνουν κάποιες πληροφορίες για την εγκατάσταση.

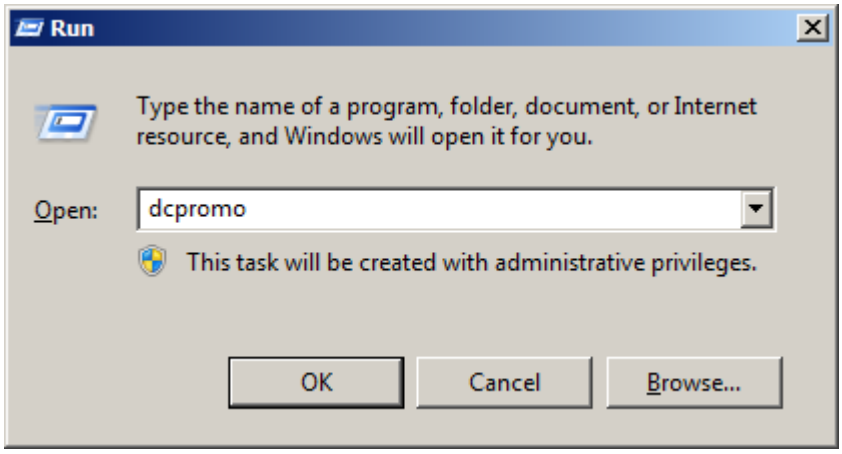


Με το πέρας της εγκατάστασης το σύστημα μας ενημερώνει για την επιτυχία του εγχειρήματος.



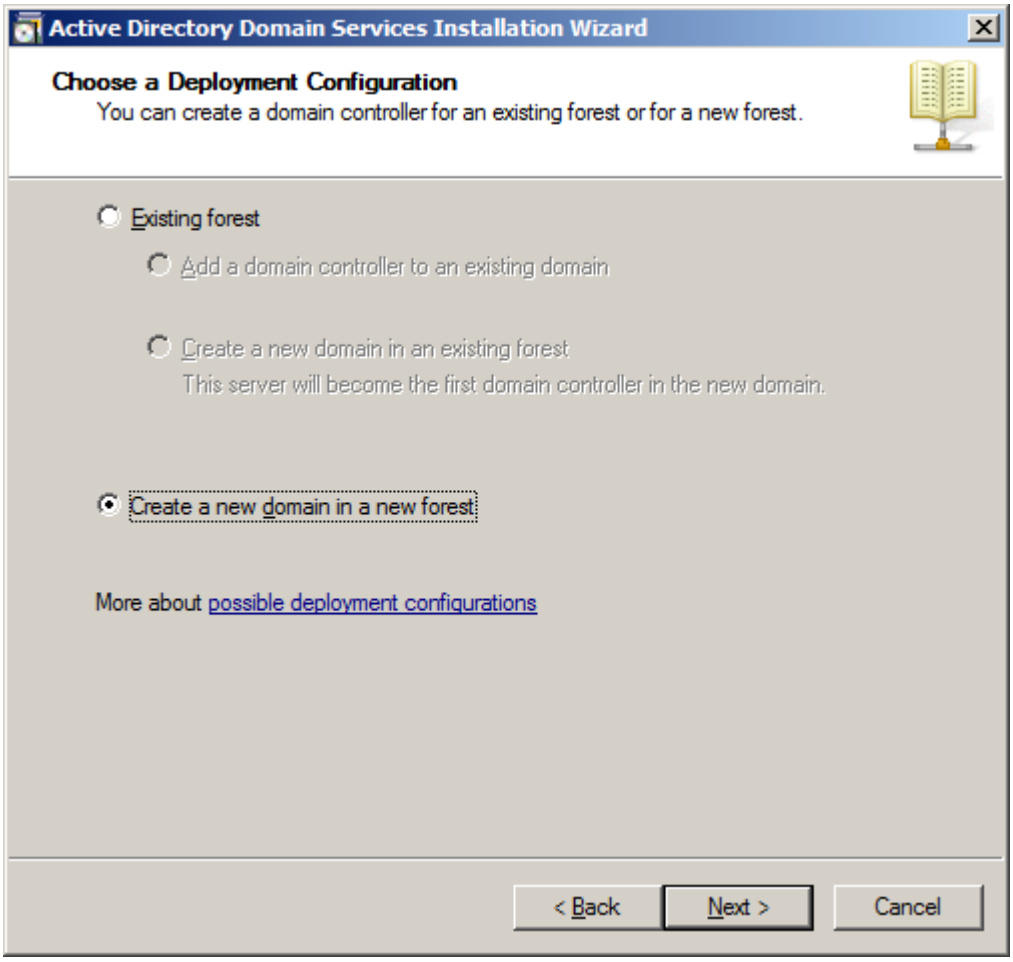
Αν και εγκαταστήσαμε τις κατάλληλες υπηρεσίες ώστε το σύστημα να λειτουργήσει σαν domain controller, είναι απαραίτητο να δημιουργήσουμε και το κατάλληλο domainπριν προχωρήσουμε.

Για την ρύθμιση του domainπρέπει από το παράθυρο Run να εκτελέσουμε το εργαλείο dcpromo.

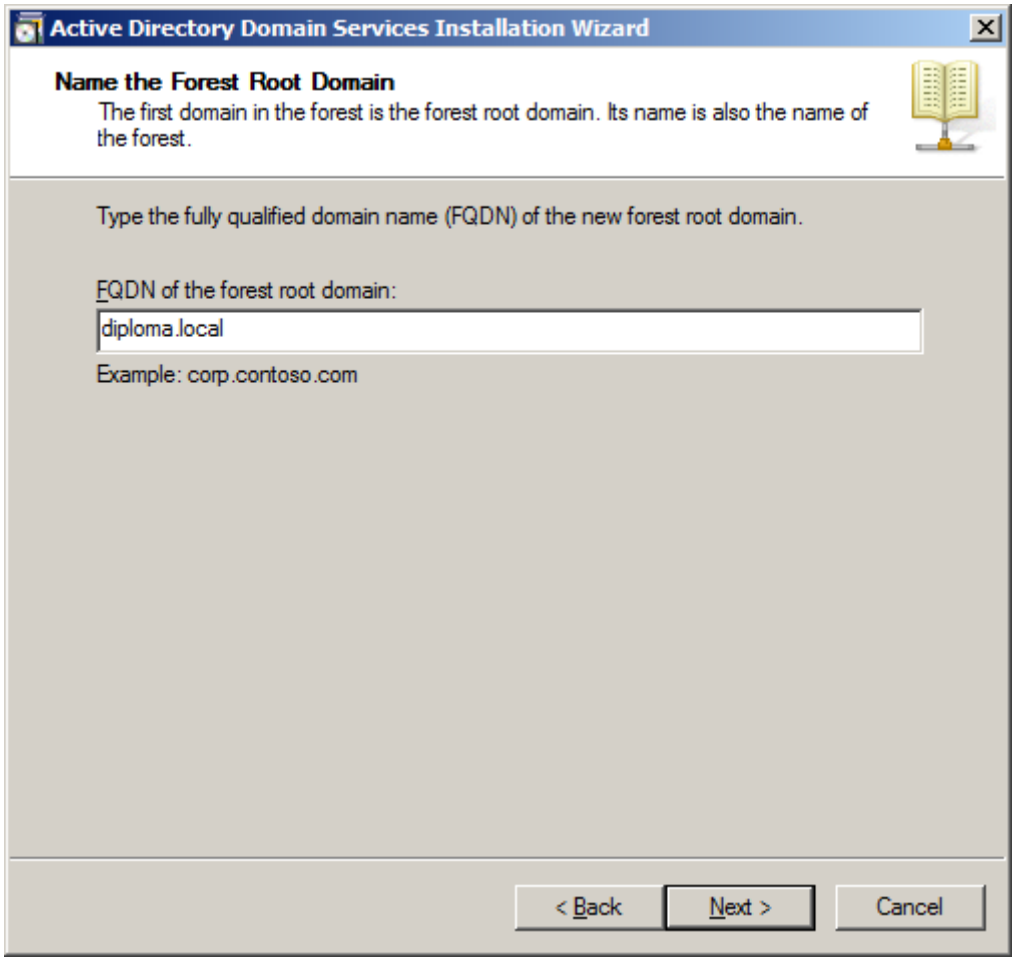


Αυτή η εντολή εκτελεί τον οδηγό ρύθμισης του Active Directory.

Οι επόμενες οθόνες περιέχουν οδηγίες για την εγκατάσταση. Η πρώτη επιλογή που μας δίνεται είναι αν θέλουμε να δημιουργήσουμε ένα νέο δέντρο ή αν θέλουμε να εισάγουμε τον domain controller σε κάποιο υπάρχον δέντρο. Καθώς δεν έχουμε κάποια υπάρχουσα υποδομή δικτύου επιλέγουμε το Create a new domain in a new forest και προχωράμε.

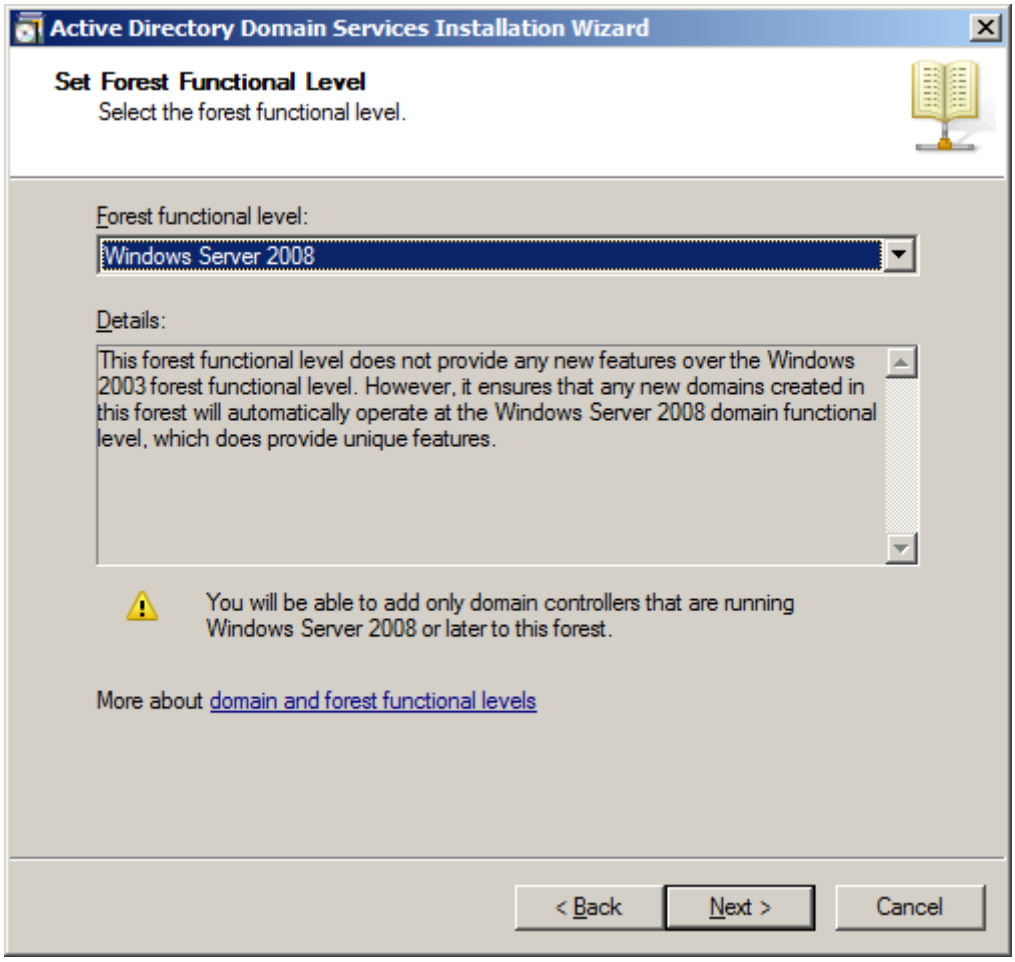


Το επόμενο παράθυρο ζητάει το όνομα του νέου domain. Αυτό είναι απαραίτητο να περιέχει τουλάχιστον δύο επίπεδα, δηλαδή δύο λέξεις χωρισμένες με τελεία. Επιλέγουμε το diploma.local.

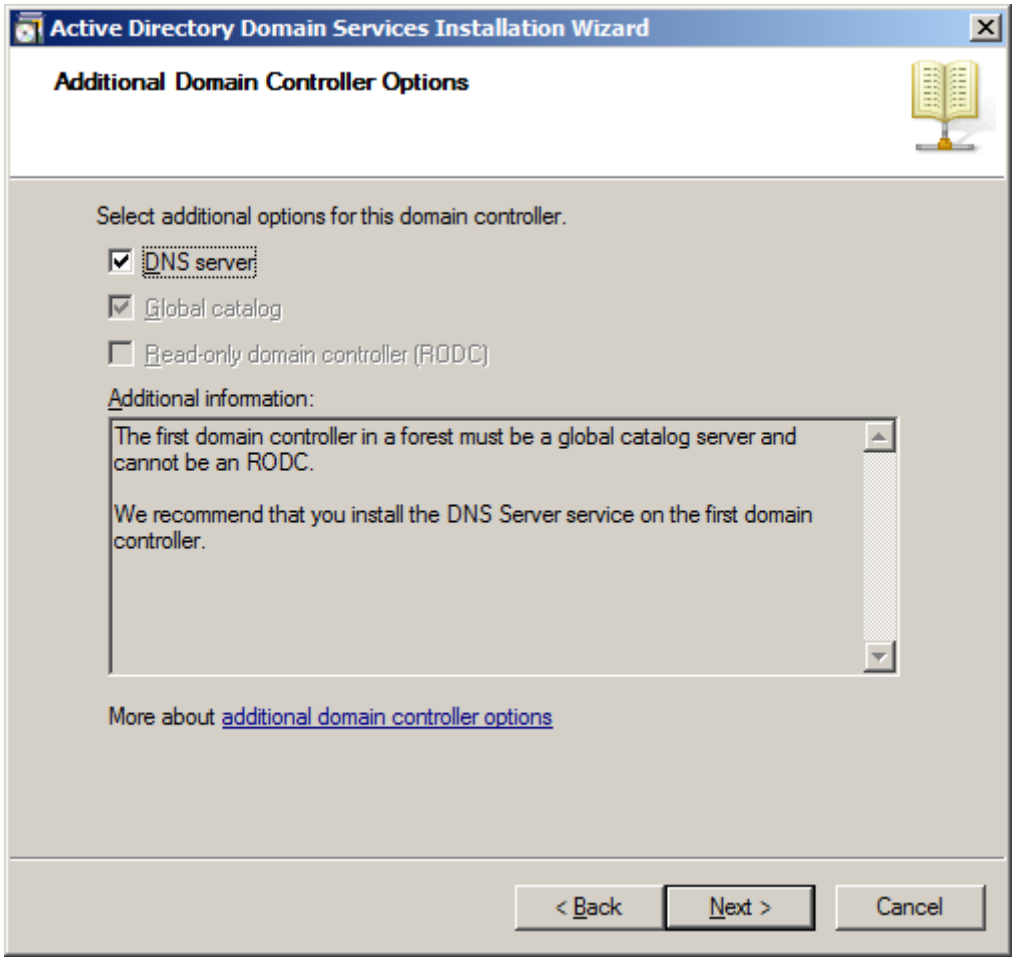


Το σύστημα ελέγχει αν το όνομα χρησιμοποιείται ήδη και μετά ρωτάει το επίπεδο συμβατότητας του δάσους. Αυτή επηρεάζει την μικρότερη έκδοση του λειτουργικού συστήματος που μπορεί να τρέχει ένας domain controller.

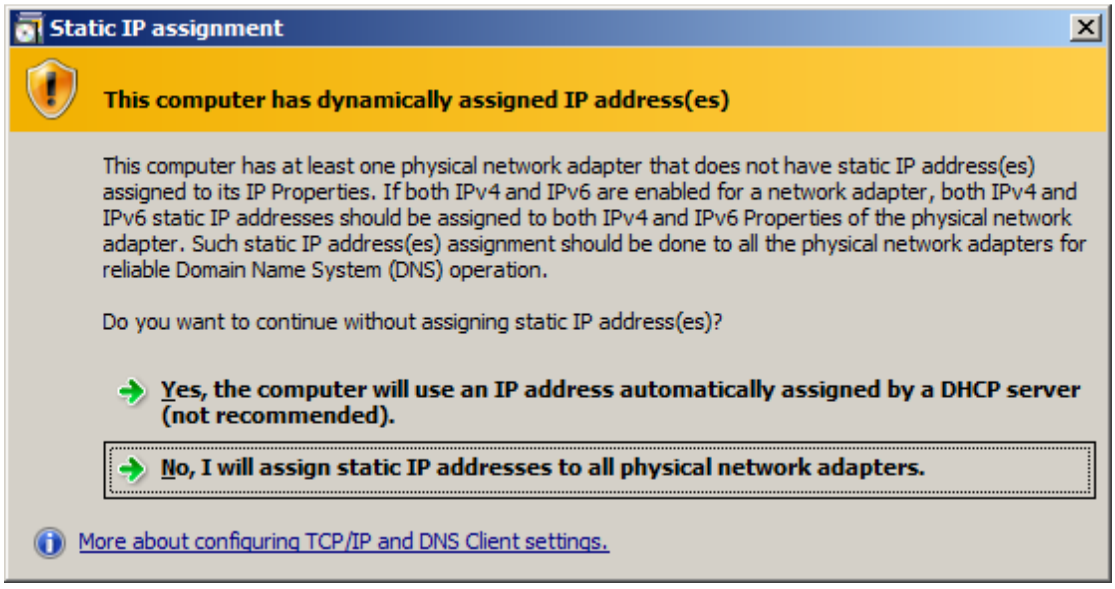
Επιλέγουμε το Windows Server 2008 αφού δεν μας ενδιαφέρει η συμβατότητα με παλιότερα συστήματα.



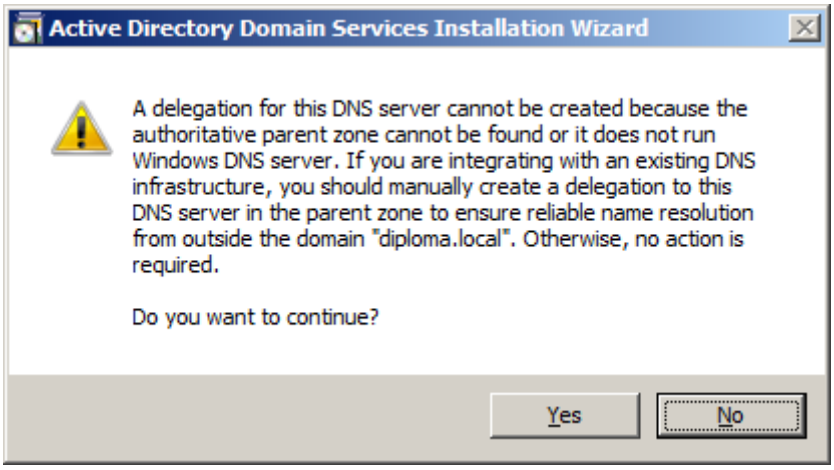
Από τη στιγμή που το μηχάνημα είναι domain server πρέπει να μπορεί να λειτουργήσει και σαν Domain Name Server. Αφού δεν υπάρχει ήδη τέτοιος server πρέπει να εγκατασταθεί.



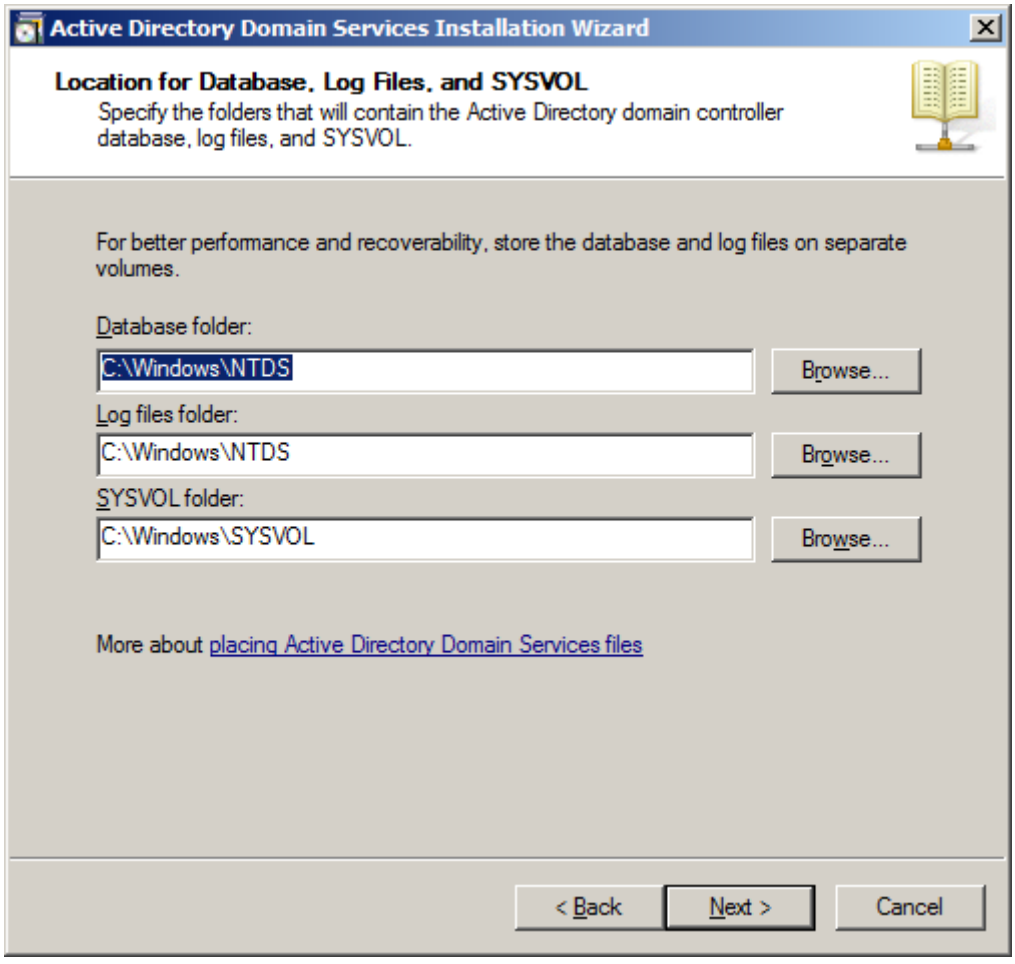
Εμφανίζεται μία προειδοποίηση για το ότι ο υπολογιστής δεν έχει μία σταθερή διεύθυνση IP. Φυσιολογικά ένα server πρέπει να έχει στατική διεύθυνση IP, η οποία πρέπει να ανατεθεί από τις ρυθμίσεις του.



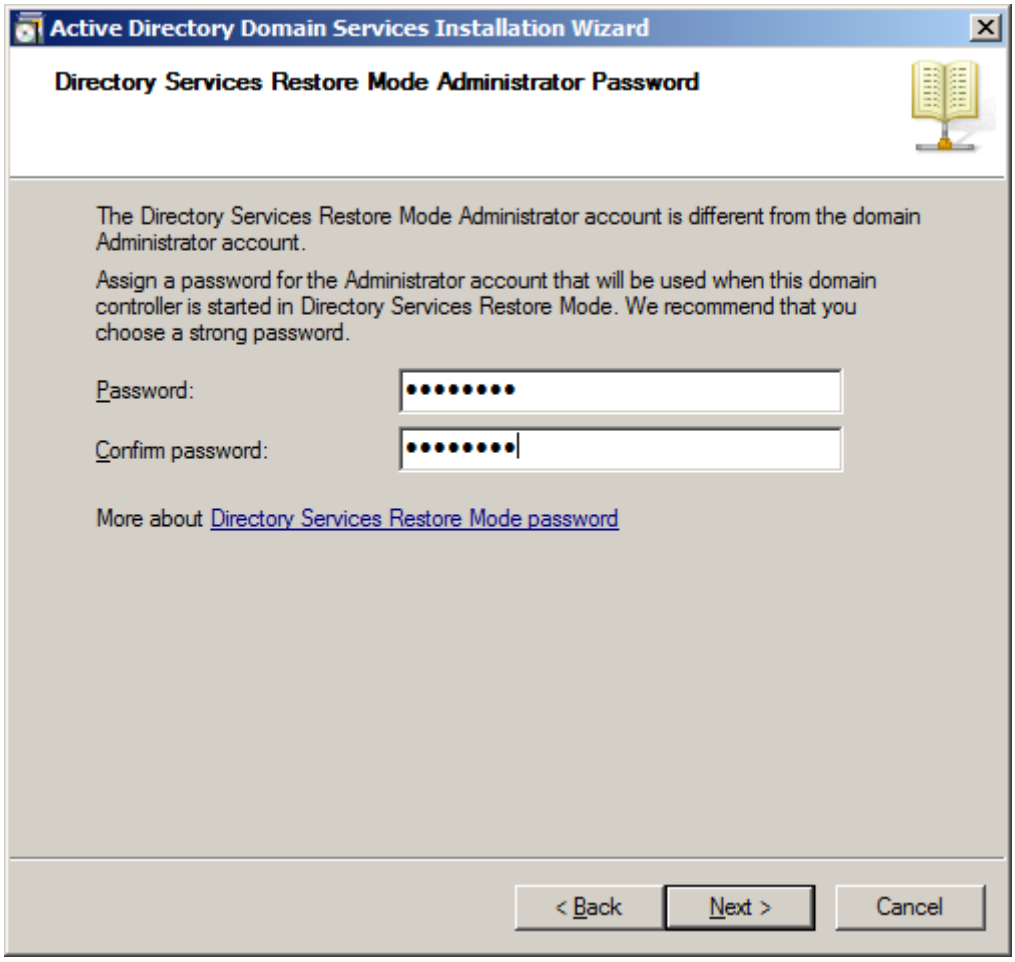
Το επόμενο μήνυμα προειδοποιεί πως δεν υπάρχει άλλος DNS Server και αφού το δίκτυο δεν περιέχει άλλο διακομιστή μπορούμε να το αγνοήσουμε.



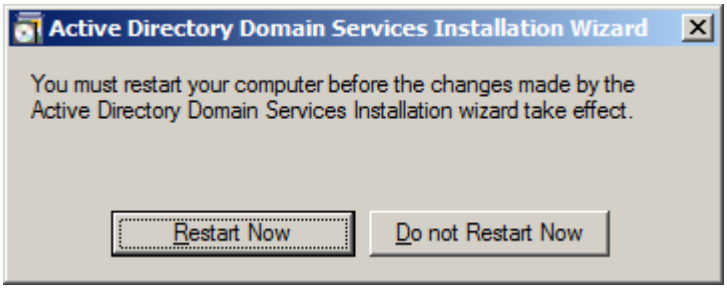
Έπειτα ζητούνται οι φάκελοι στους οποίους θα αποθηκεύονται τα αρχεία του Active Directory, τα αρχεία καταγραφής και οι πληροφορίες συστήματος. Φυσιολογικά αυτά καλό είναι να βρίσκονται σε διαφορετικούς δίσκους για λόγους αξιοπιστίας και επιδόσεων. Εδώ κρατάμε τις αρχικές ρυθμίσεις.



Μετά εισάγουμε έναν κωδικό για τον διαχειριστή ανάκτησης της υπηρεσίας καταλόγου. Πρόκειται για έναν ειδικό χρήστη του οποίου ο ρόλος είναι η ανάκτηση των δεδομένων σε περίπτωση δυσλειτουργίας του συστήματος.



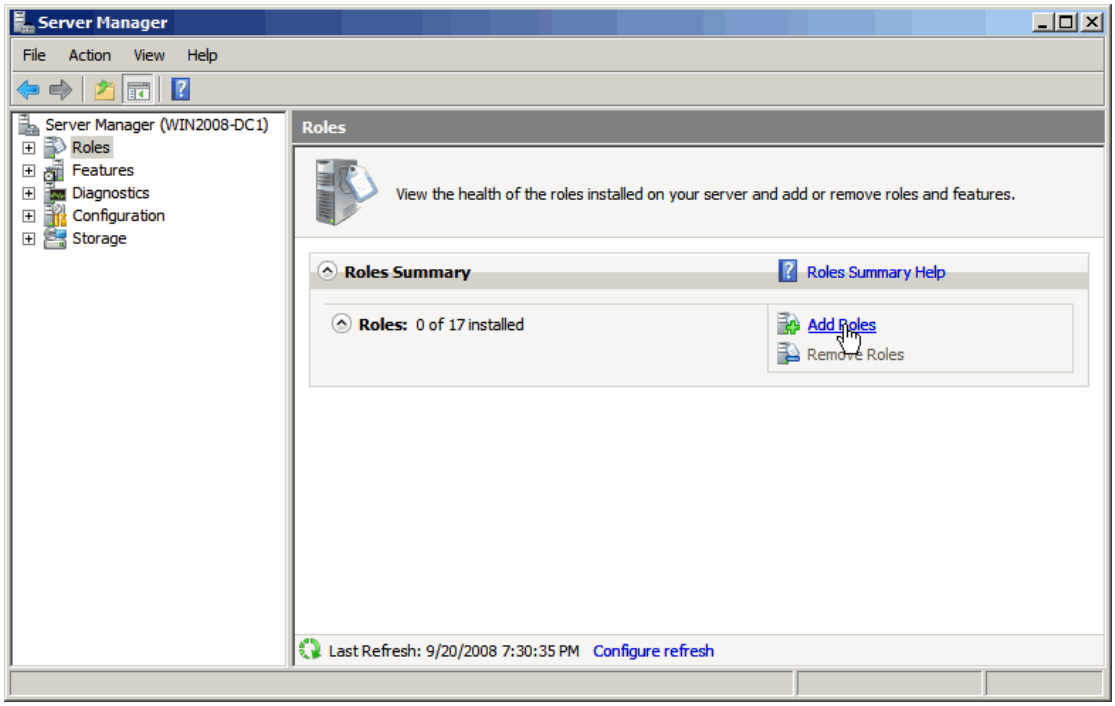
Μετά και από αυτό δημιουργείται ο νέος κατάλογος και εγκαθίστανται τα αναγκαία αρχεία. Με το πέρας της εγκατάστασης είναι απαραίτητη η επανεκκίνηση του υπολογιστή.



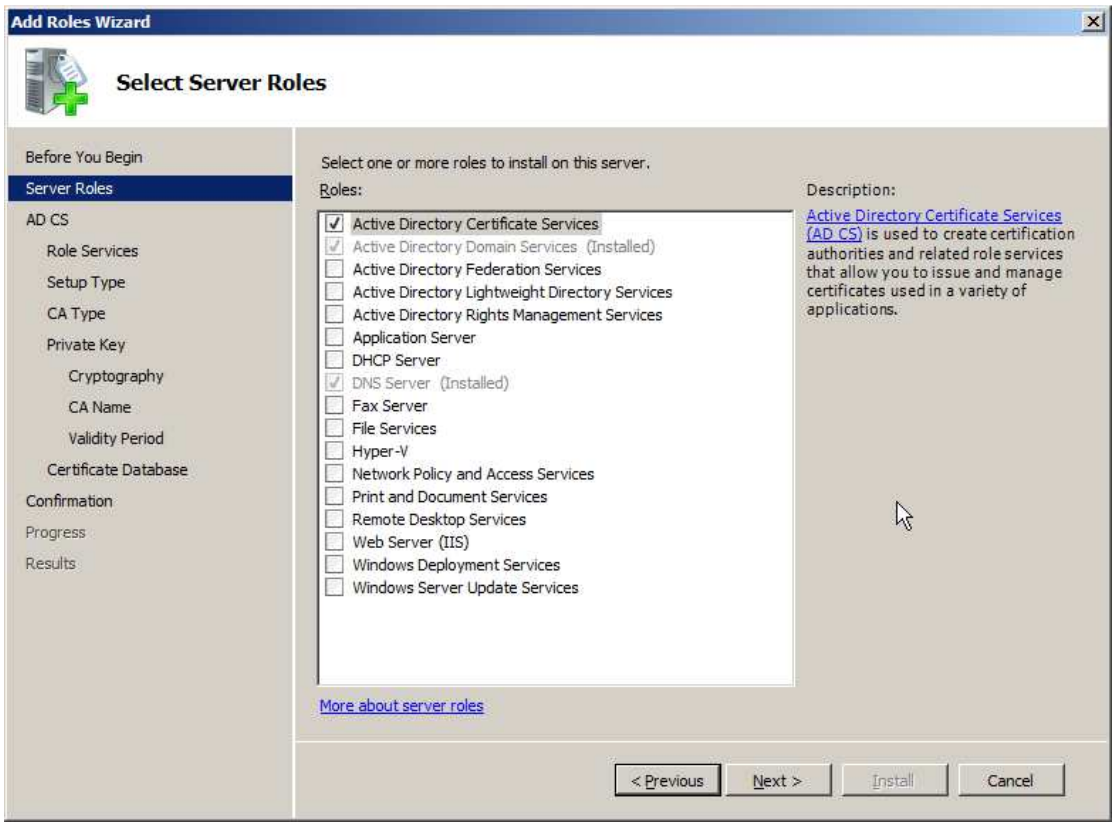
5.4 Δημιουργία αρχής πιστοποίησης

Έπειτα χρειάζεται να δημιουργήσουμε την αρχής πιστοποίησης. Από το εργαλείο Server Manager επιλέγουμε πάλι Add Role.

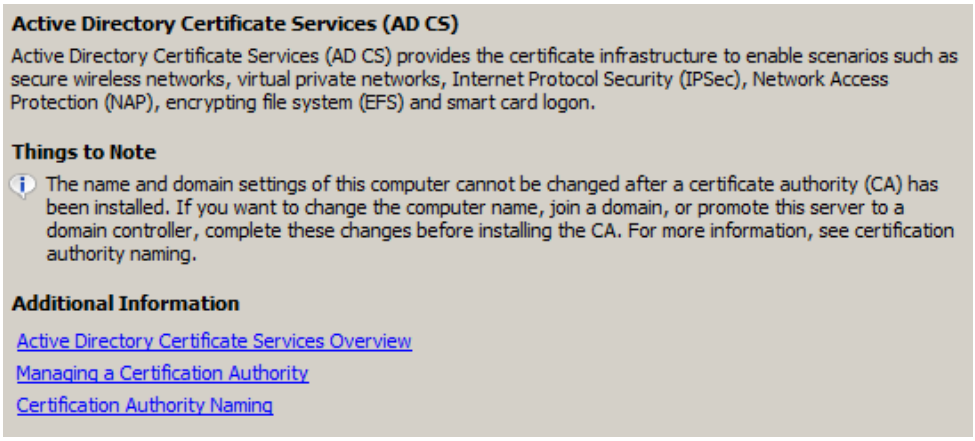
Υπό φυσιολογικές συνθήκες θα χρειαζόταν να εγκαταστήσουμε και τον ρόλο DHCP Server ώστε οι υπολογιστές που συνδέονται στο δίκτυο να παίρνουν την διεύθυνση IP τους από τον server. Όμως καθώς κάτι τέτοιο δημιουργεί προβλήματα στο δίκτυο που κάνουμε τις δοκιμές δεν θα το κάνουμε.



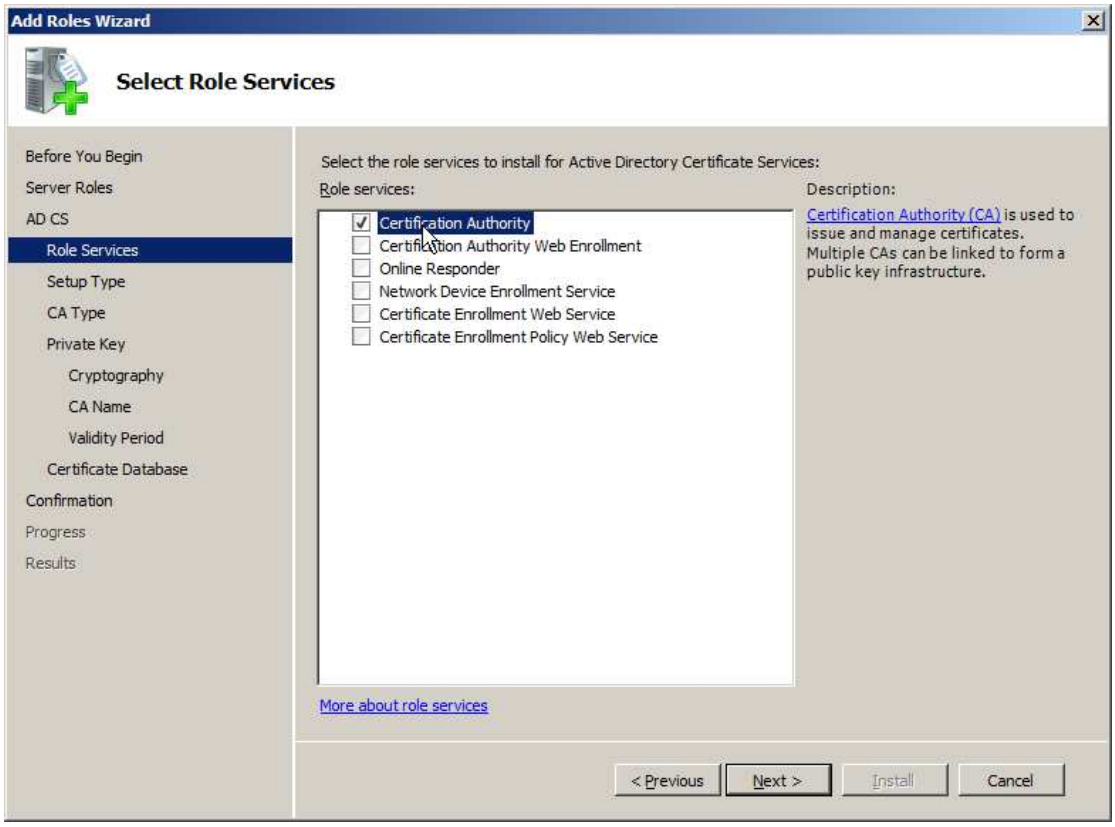
Αυτή τη φορά επιλέγουμε το Active Directory Certificate Services και πατάμε Next.



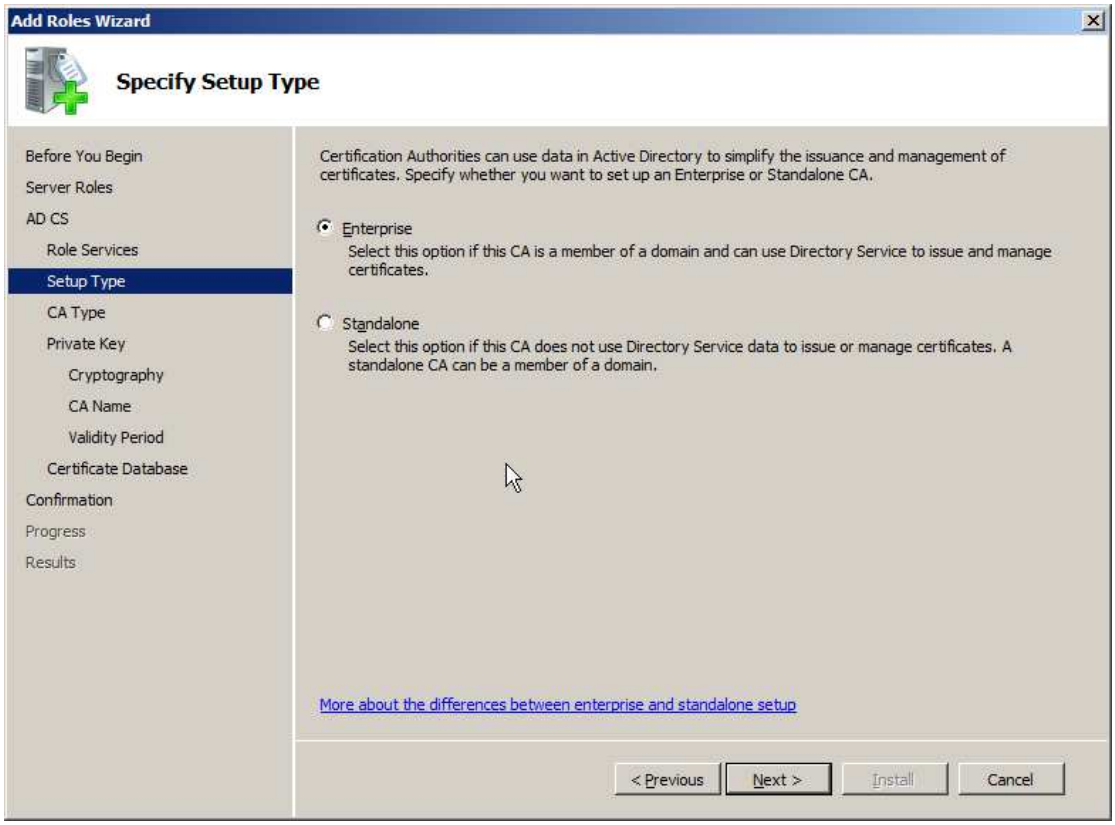
Εμφανίζεται μία προειδοποίηση πως μετά την εγκατάσταση δεν θα μπορέσουμε να τροποποιήσουμε το όνομα του υπολογιστή ή το domain στο οποίο ανήκει.



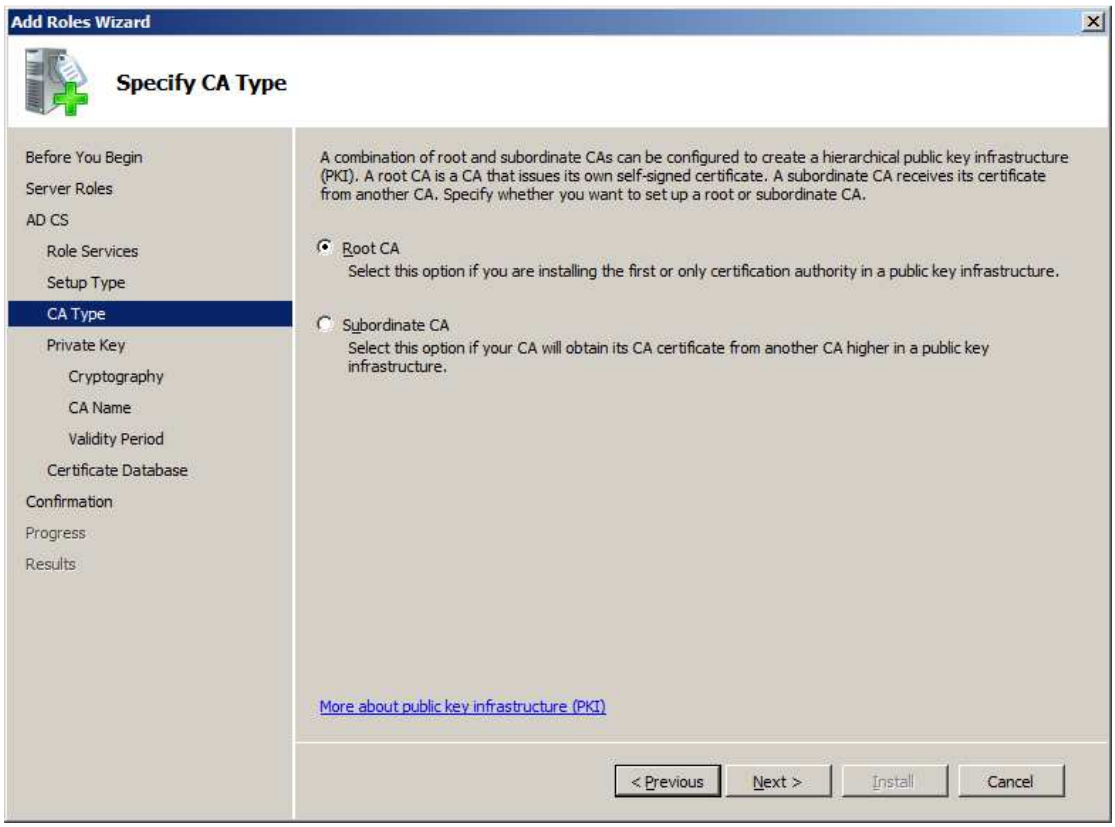
Στην επόμενη οθόνη επιλέγουμε τις υπηρεσίες που θέλουμε να προσφέρει αυτός ο υπολογιστής. Επιλέγουμε το Certificate Authority. Αν ήταν επιθυμητή η παροχή υπηρεσιών PKI σε χρήστες εκτός του τοπικού δικτύου θα χρειαζόταν και το Certificate Authority Web Enrollment.



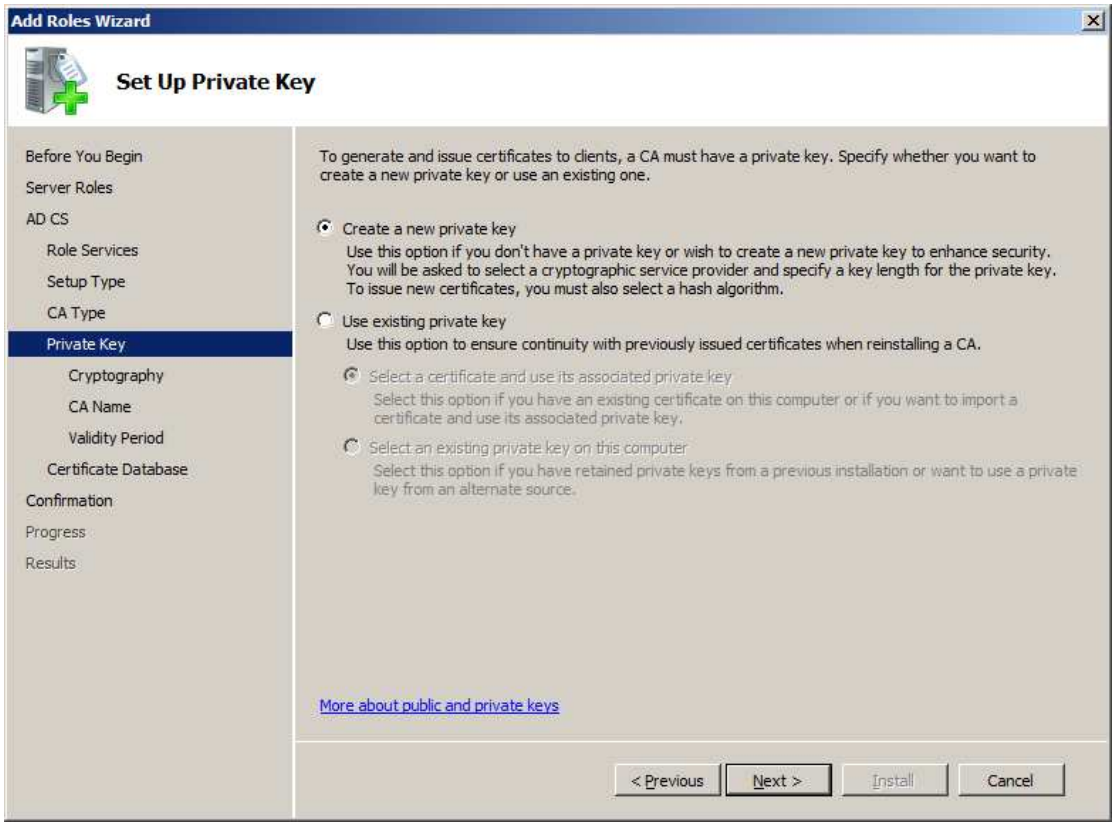
Μετά επιλέγουμε το είδος της εγκατάστασης. Οι επιλογές είναι το Enterprise όπου η αρχή πιστοποιητικών μπορεί να εκδίδει και να διαχειρίζεται πιστοποιητικά μέσω των Directory Services και το Standalone όπου δεν γίνεται κάτι τέτοιο. Η δεύτερη επιλογή θα είχε νόημα αν είχαμε μία ιεραρχία αρχών πιστοποίησης, όμως αφού δεν έχουμε κάτι τέτοιο επιλέγουμε την πρώτη.



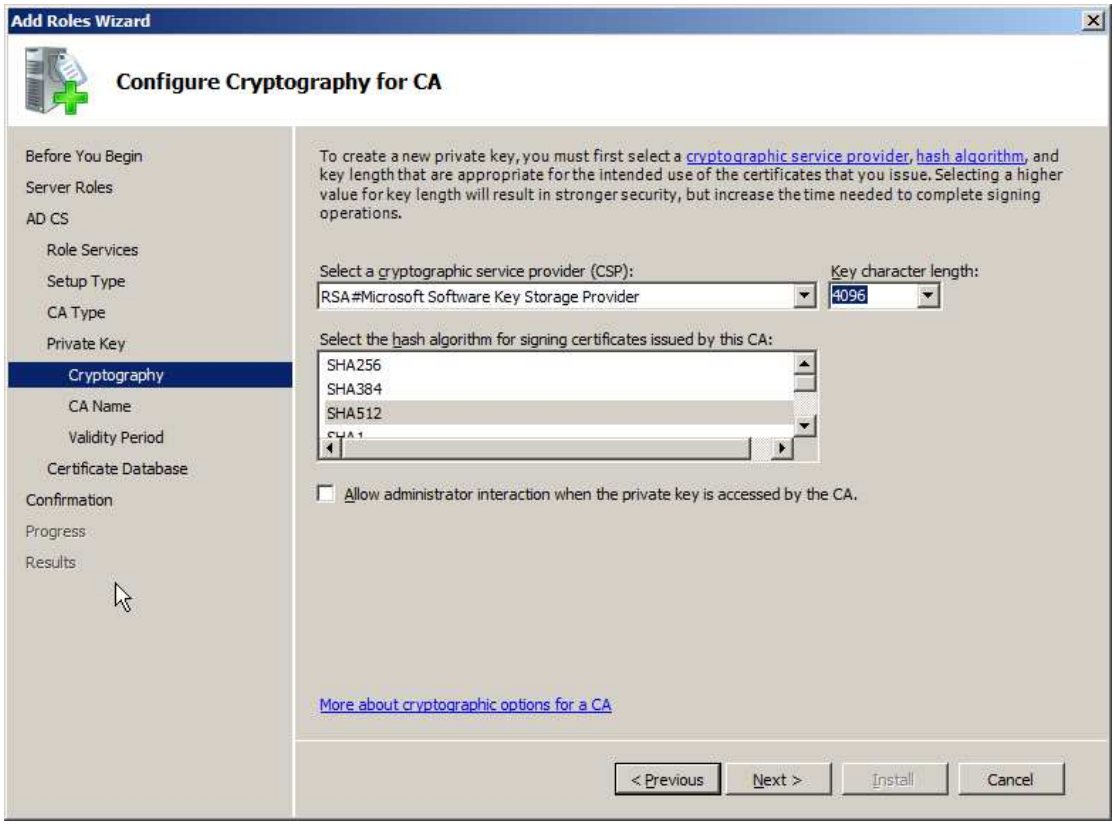
Μετά επιλέγουμε αν θέλουμε η αρχή πιστοποίησης να είναι στην ρίζα της ιεραρχίας, δηλαδή να εκδίδει τα δικά της πιστοποιητικά ή να βρίσκεται σε κάποιο χαμηλότερο τμήμα της. Αφού έχουμε μόνο έναν Server επιλέγουμε την πρώτη επιλογή.



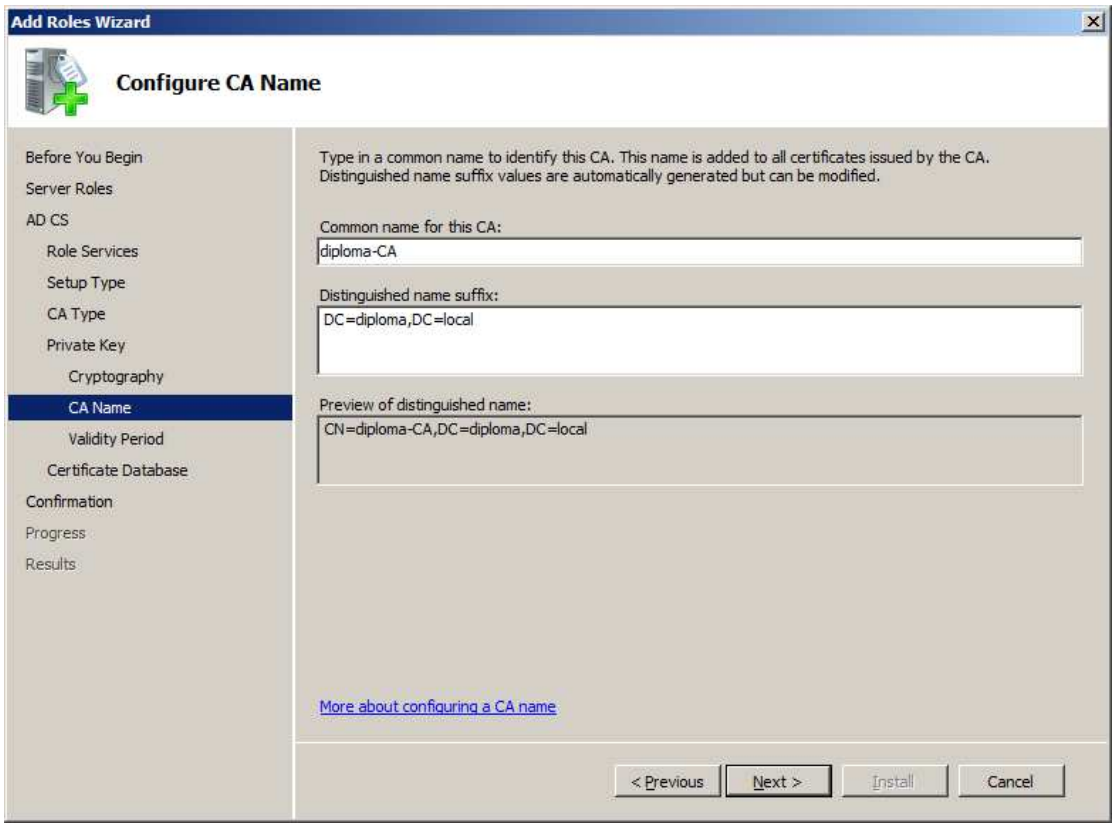
Το επόμενο βήμα είναι η δημιουργία ενός νέου ιδιωτικού κλειδιού. Αν είχαμε μία προηγούμενη εγκατάσταση θα μπορούσαμε με την δεύτερη επιλογή να εισάγουμε το παλιό κλειδί της.



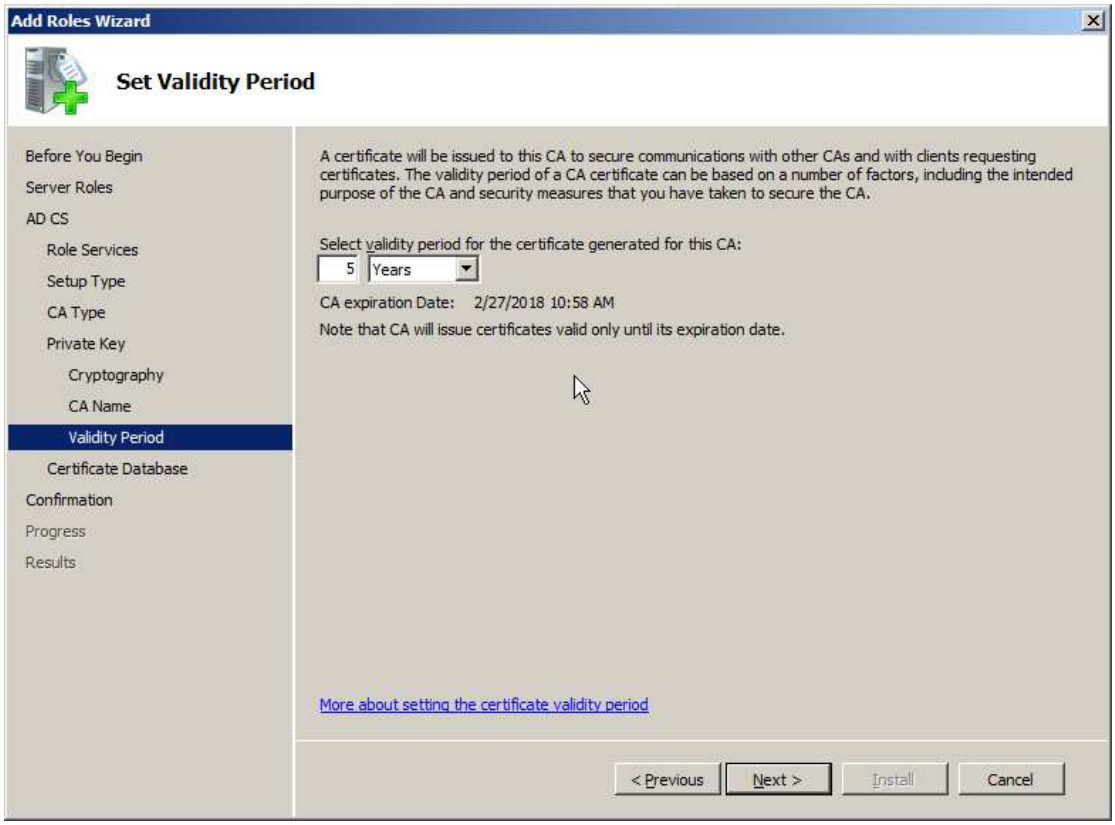
Στο επόμενο βήμα επιλέγουμε τα είδη κρυπτογραφίας που θα προστατεύουν το κλειδί και τις υπογραφές με αυτό. Επιλέγομε κλειδί μήκους 4096 bit και τον αλγόριθμο hash SHA-512. Οι επιλογές αυτές πρέπει να γίνουν με γνώμονα την συμβατότητα με τους υπολογιστές που θα συνδεθούν στο δίκτυο, καθώς δεν υποστηρίζονται όλοι οι αλγόριθμοι από όλες τις εκδόσεις των Windows.



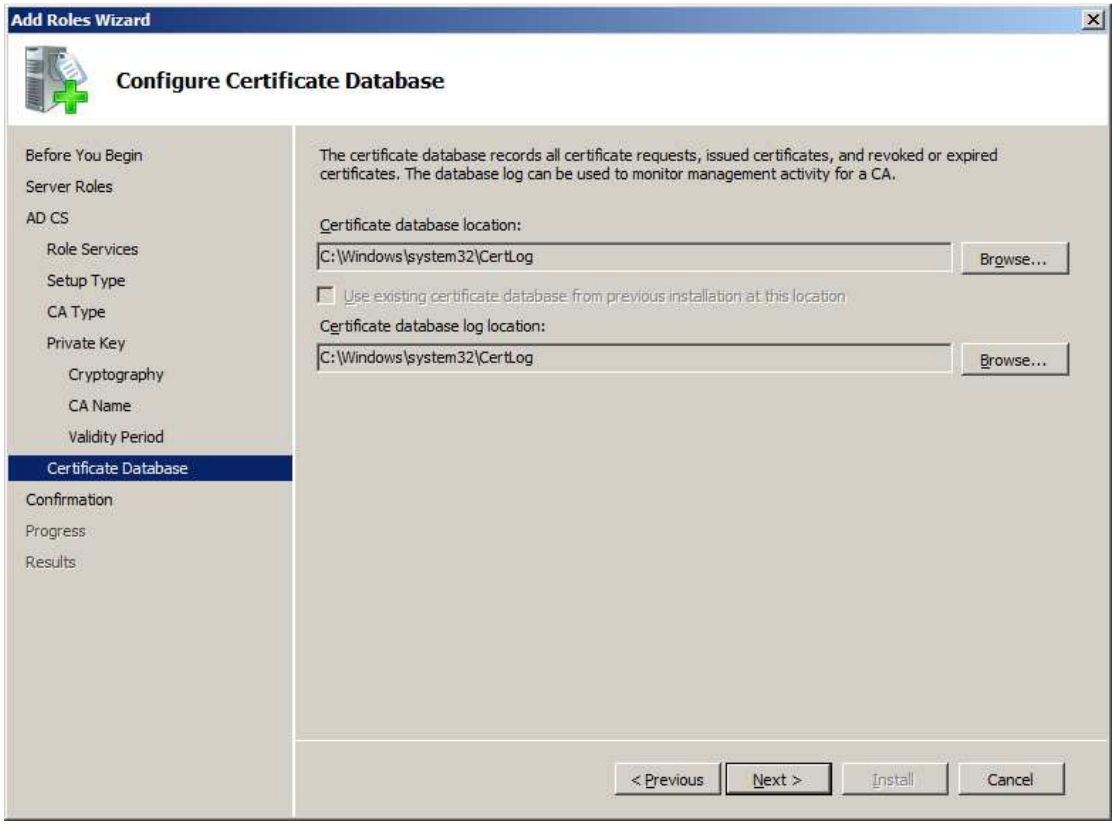
Μετά χρειάζεται να επιλέξουμε το όνομα της αρχής.



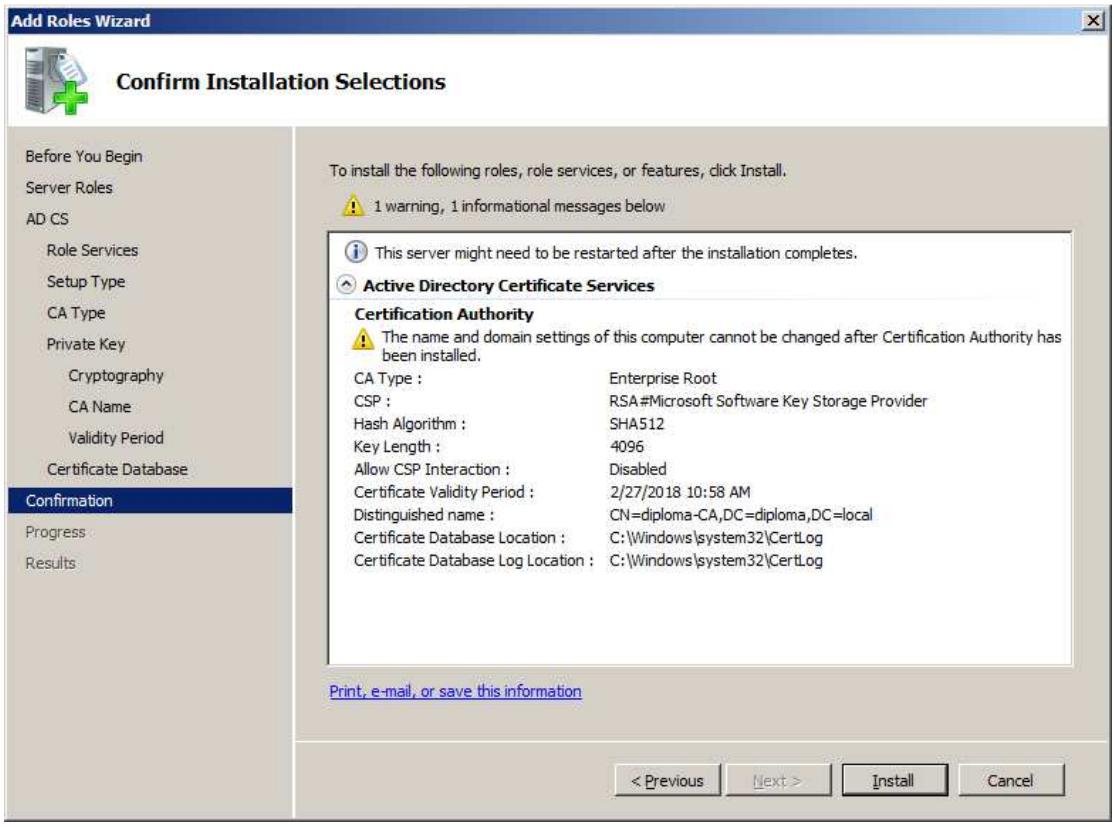
Τέλος επιλέγουμε την ημερομηνία λήξης αυτού του πιστοποιητικού.



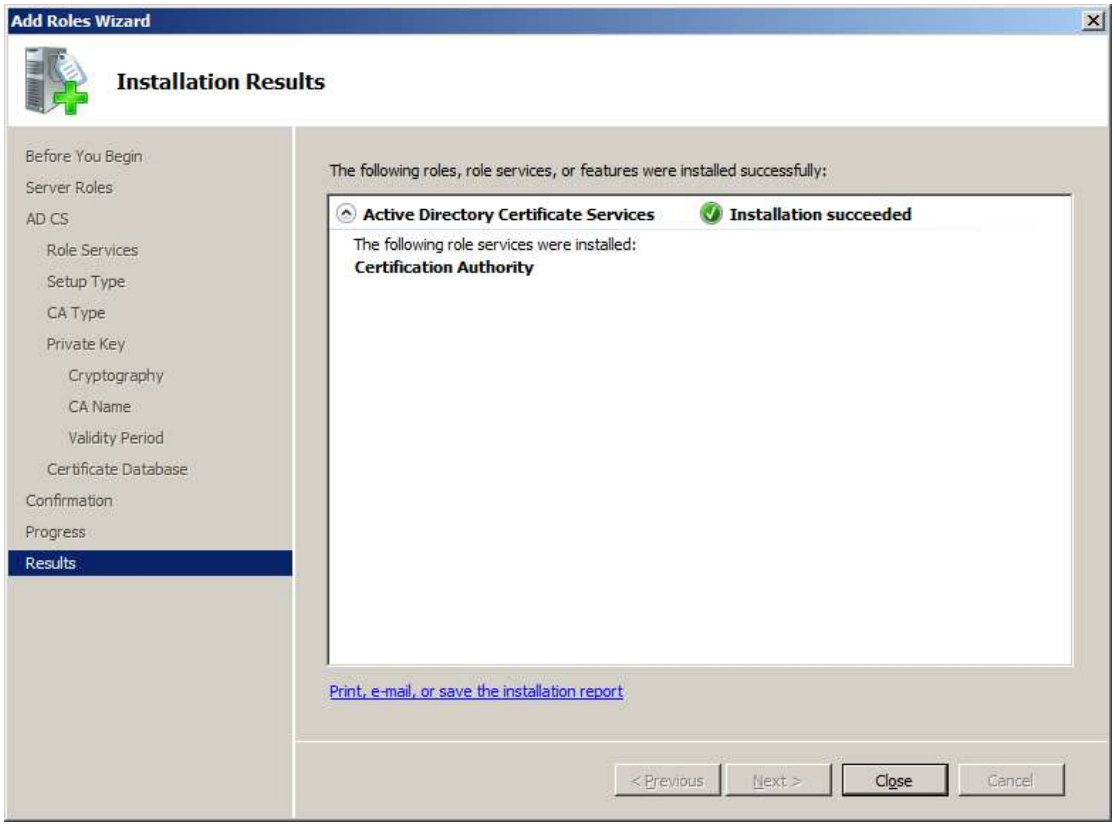
Έπειτα επιλέγουμε την τοποθεσία της βάσης δεδομένων που θα κρατάει τα κλειδιά. Είναι εφικτή η χρήση μίας παλιότερης βάσης σε περίπτωση που γίνεται μεταφορά μίας παλιότερης εγκατάστασης αρχής πιστοποίησης.



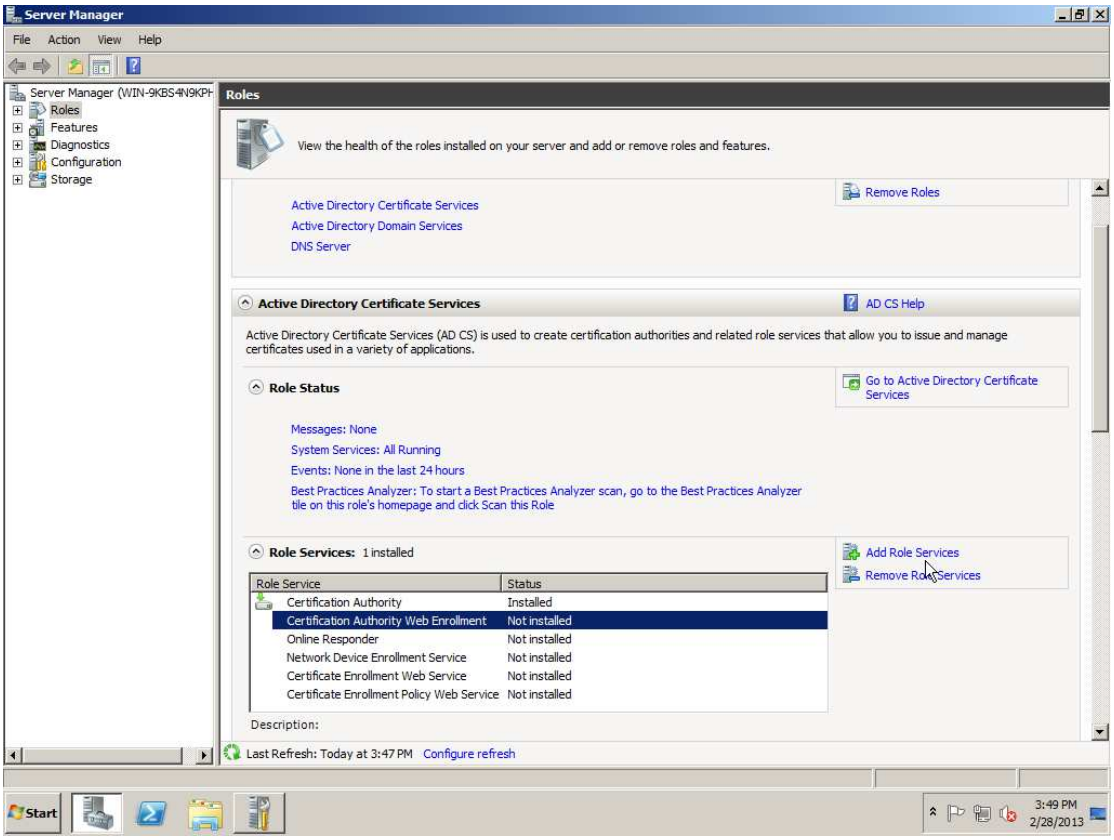
Στο τελευταίο βήμα παρουσιάζονται όλες οι επιλογές που έγιναν κατά τη διάρκεια της εγκατάστασης και ζητείται η επαλήθευσή τους.



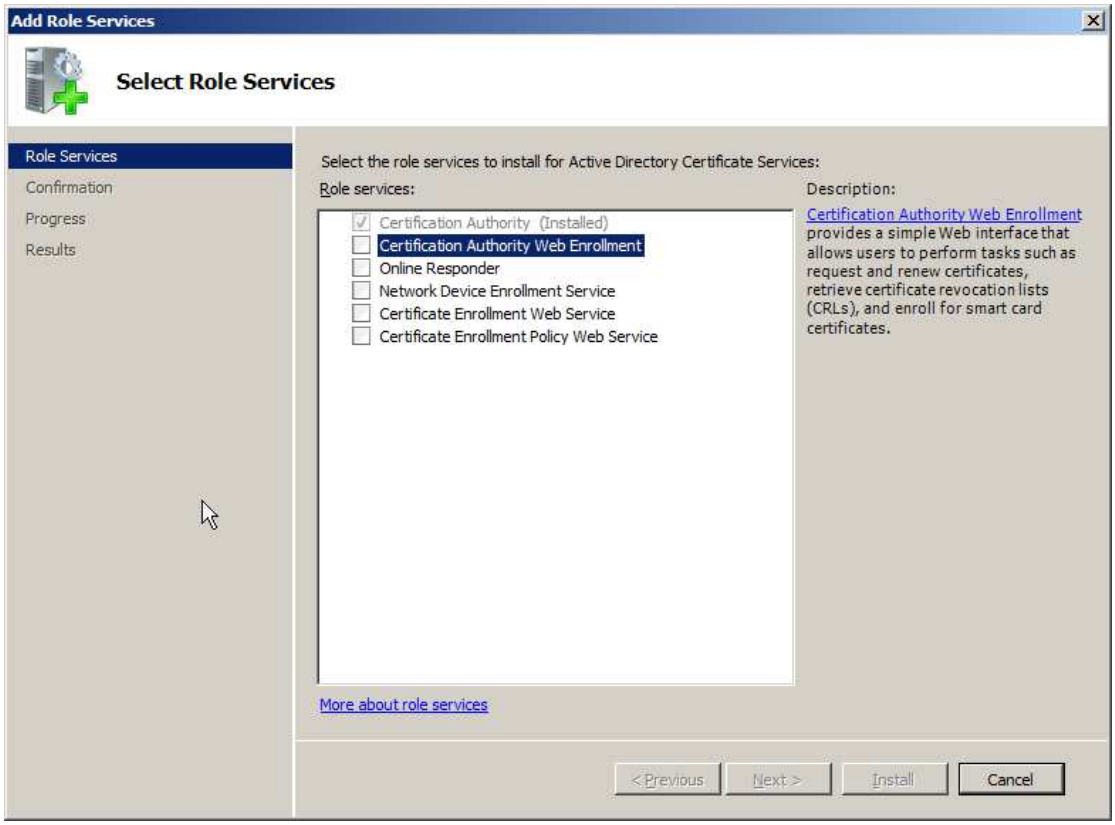
Όταν ολοκληρωθεί η διαδικασία παρουσιάζεται μία σύνοψη και τυχόν προβλήματα που παρουσιάστηκαν.



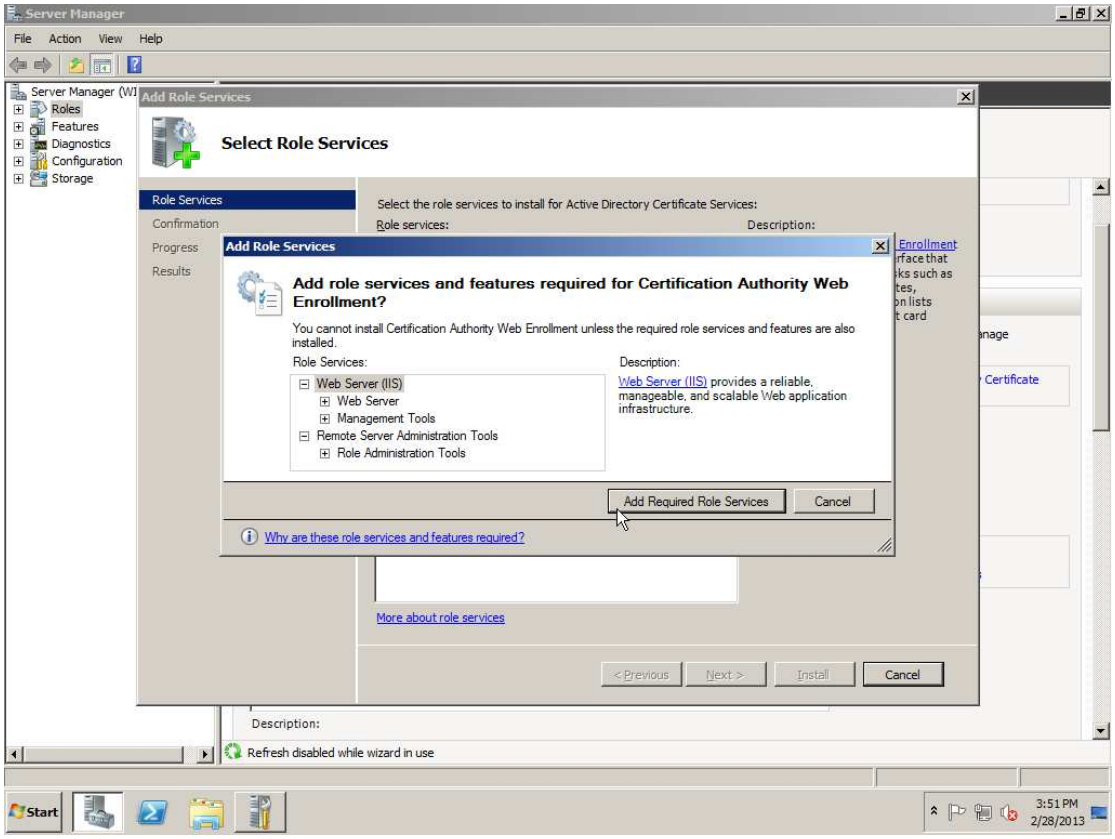
Έπειτα χρειάζεται να εγκαταστήσουμε την υπηρεσία παροχής πιστοποιητικών μέσω Web για ευκολότερη διαχείριση των πιστοποιητικών. Πατώντας το κουμπί Server Manager στην μπάρα εργασιών εμφανίζεται ένα παράθυρο με τις σημαντικότερες ενέργειες διαχείρισης του server. Από το δέντρο στα αριστερά επιλέγουμε το Roles και κάτω από το Active Directory Certificate Services επιλέγουμε το Add Role Services.



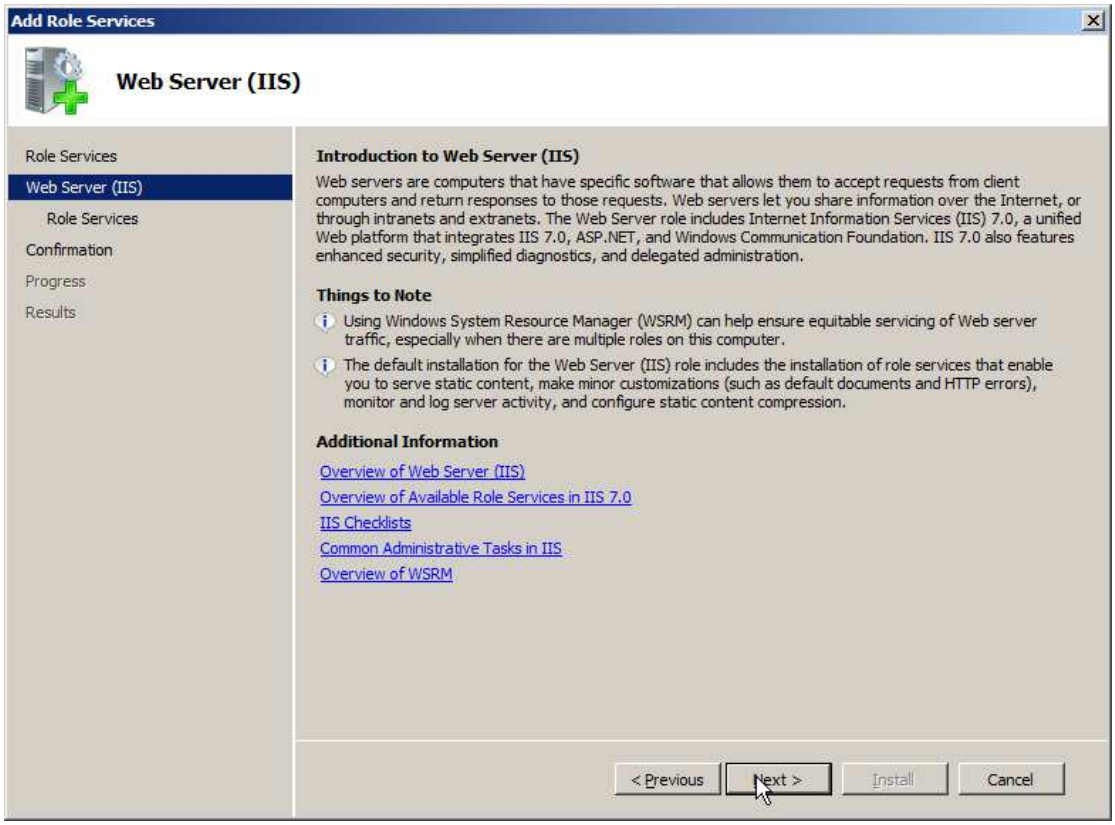
Έπειτα επιλέγουμε το Certificate Authority Web Services.



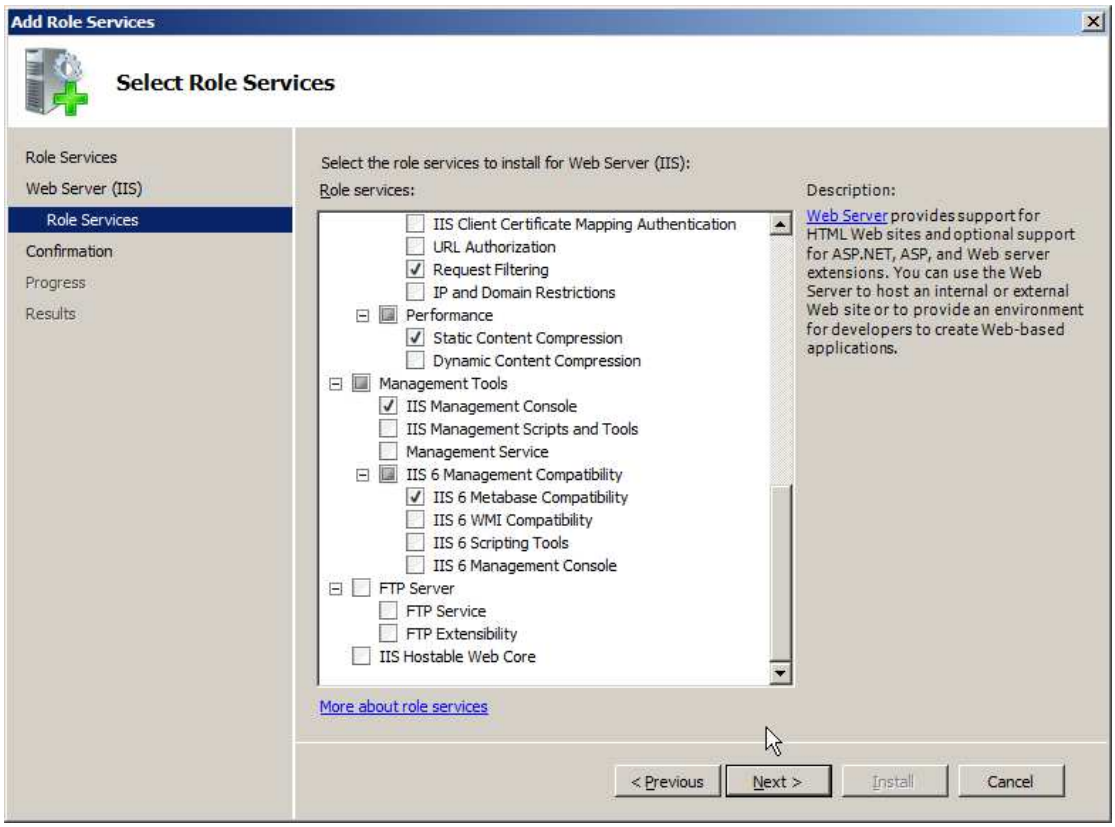
Με την επιλογή του ζητείται να εγκαταστήσουμε επιπλέον ρόλους για τον Server, συγκεκριμένα τον Internet Information Server και τις υπηρεσίες για την υποστήριξή του.



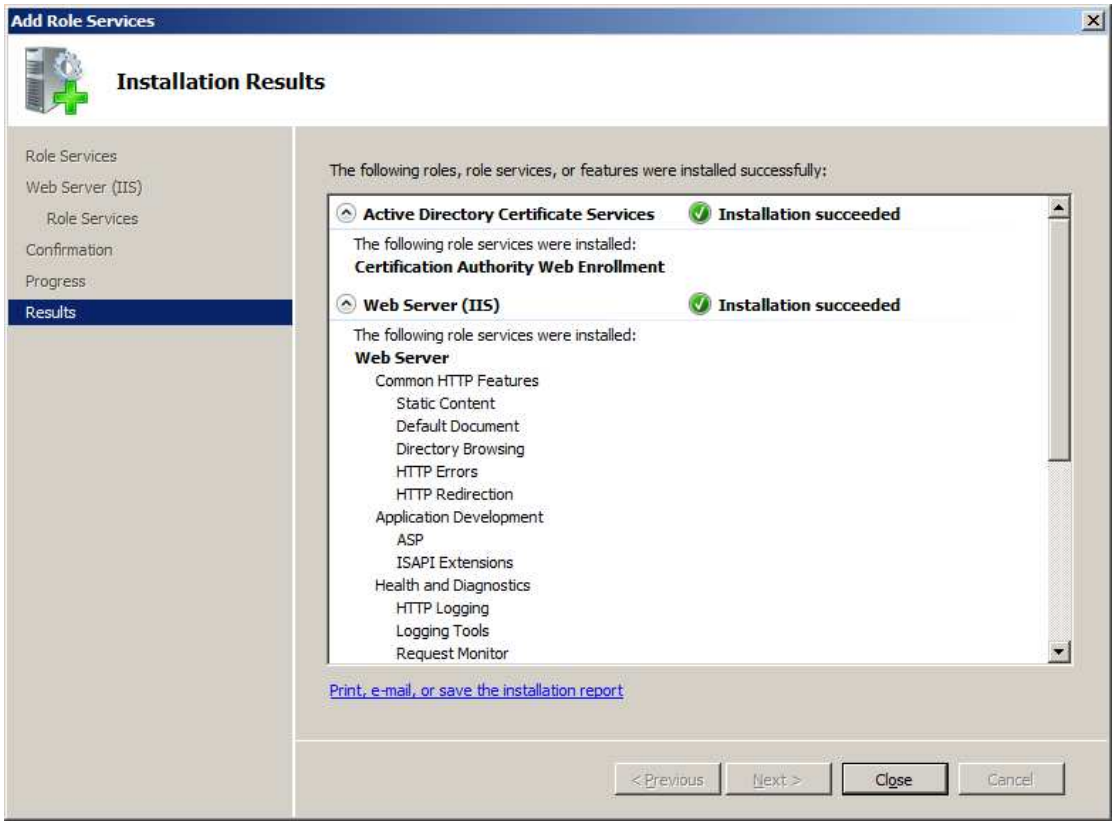
Επιλέγοντας Add Required Role Services ξεκινάει η εγκατάσταση.



Συνεχίζουμε χωρίς να πειράξουμε τις προκαθορισμένες επιλογές.

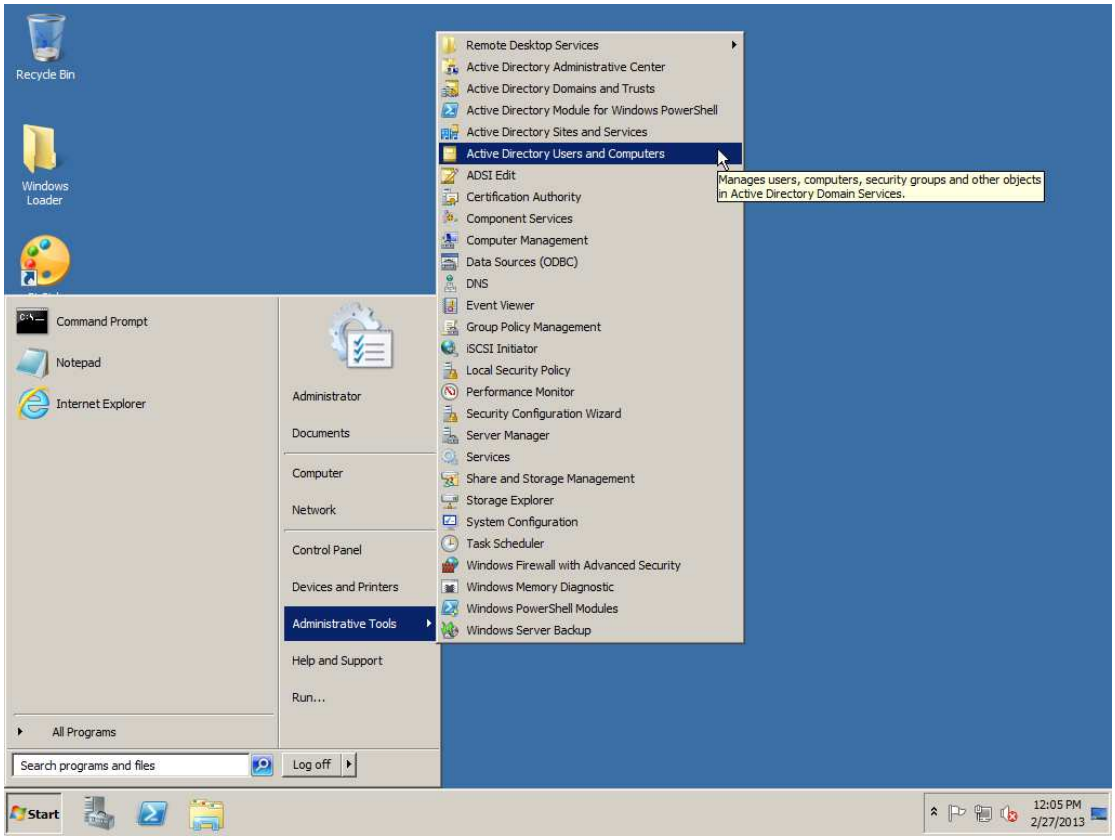


Με το πέρας της εγκατάστασης εμφανίζεται μήνυμα με τυχόν λάθη.

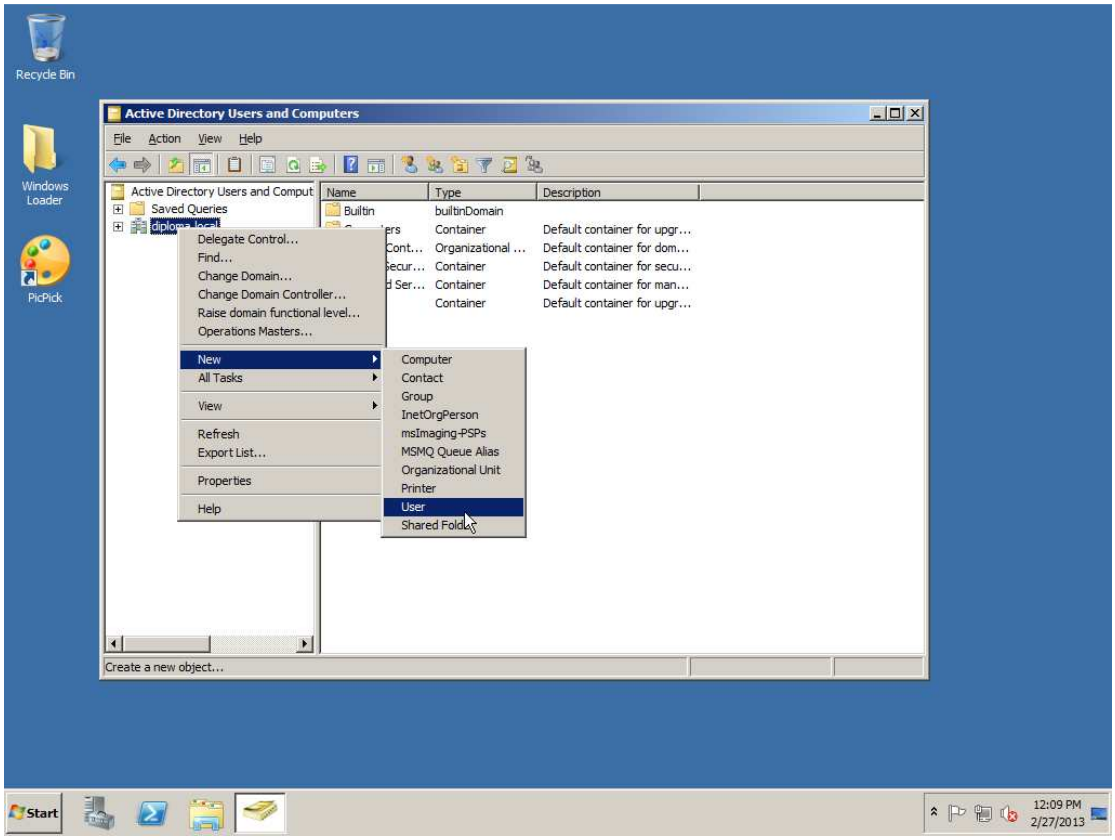


5.5 Προσθήκη χρηστών και υπολογιστών στο Active Directory

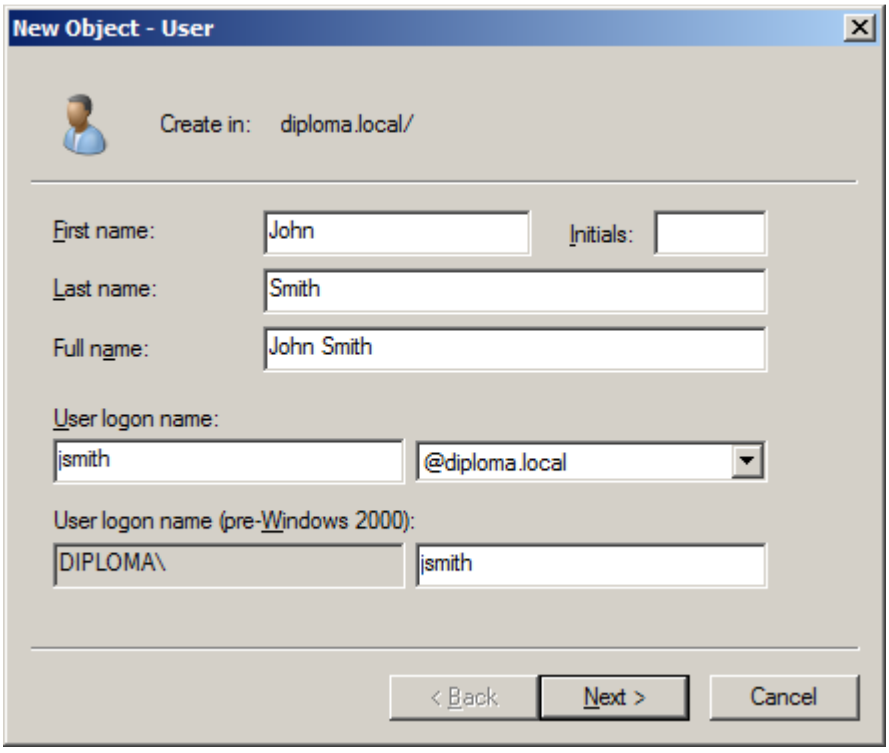
Για να μπει ένας καινούργιος χρήστης στο Active Directory επιλέγουμε το Active Directory Users and Computers από το Administrative Tools στο Start Menu.



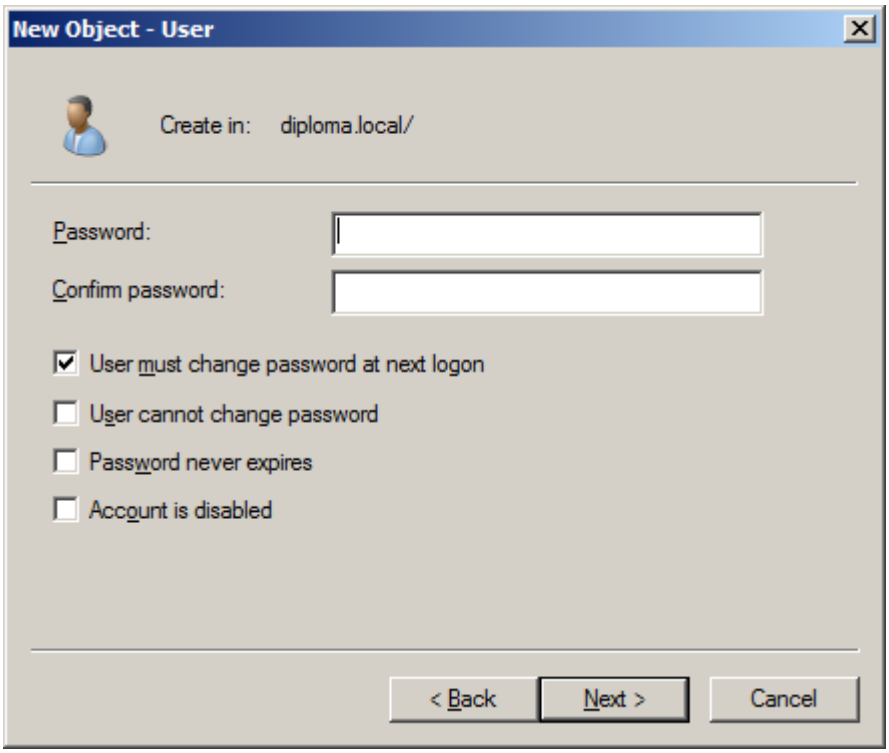
Εμφανίζεται η κονσόλα διαχείρισης των domain που υπάρχουν στο δίκτυο, δηλαδή στην περίπτωση μας του diploma.local. Με δεξί κλικ σε αυτό επιλέγουμε New User.



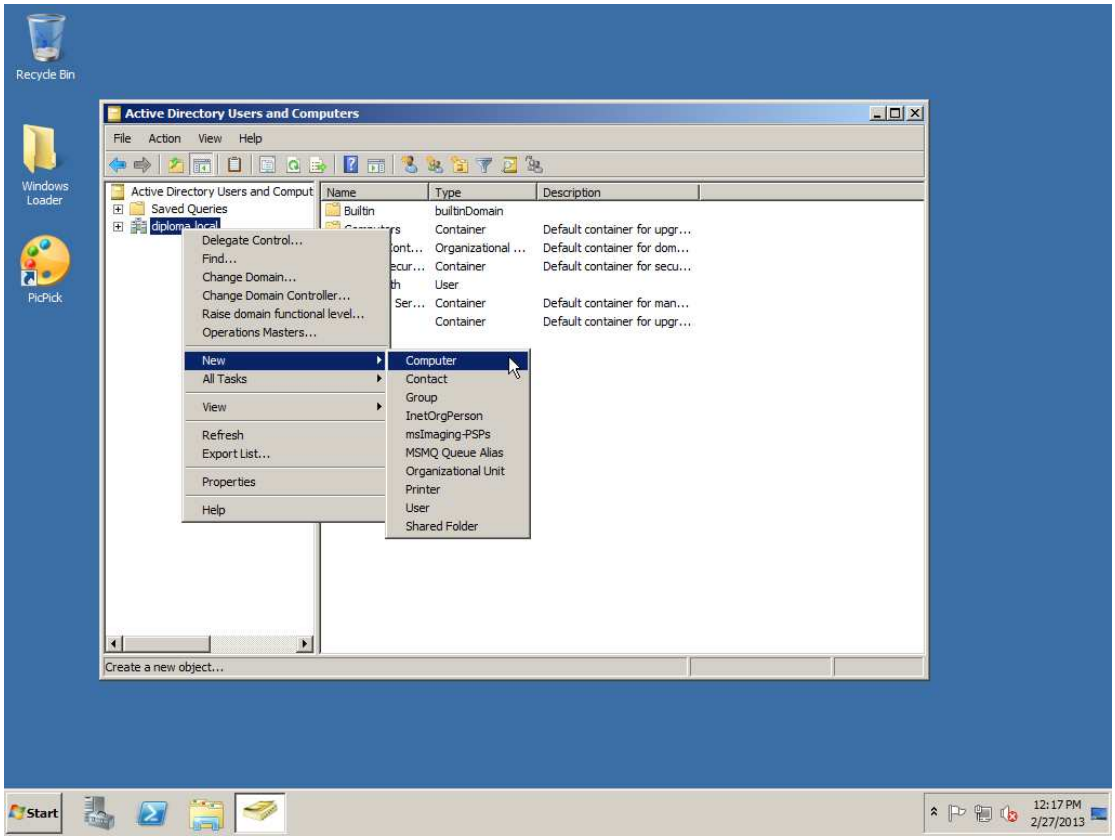
Στο νέο παράθυρο εισάγουμε τα στοιχεία του νέου χρήστη και το domain στο οποίο ανήκει.



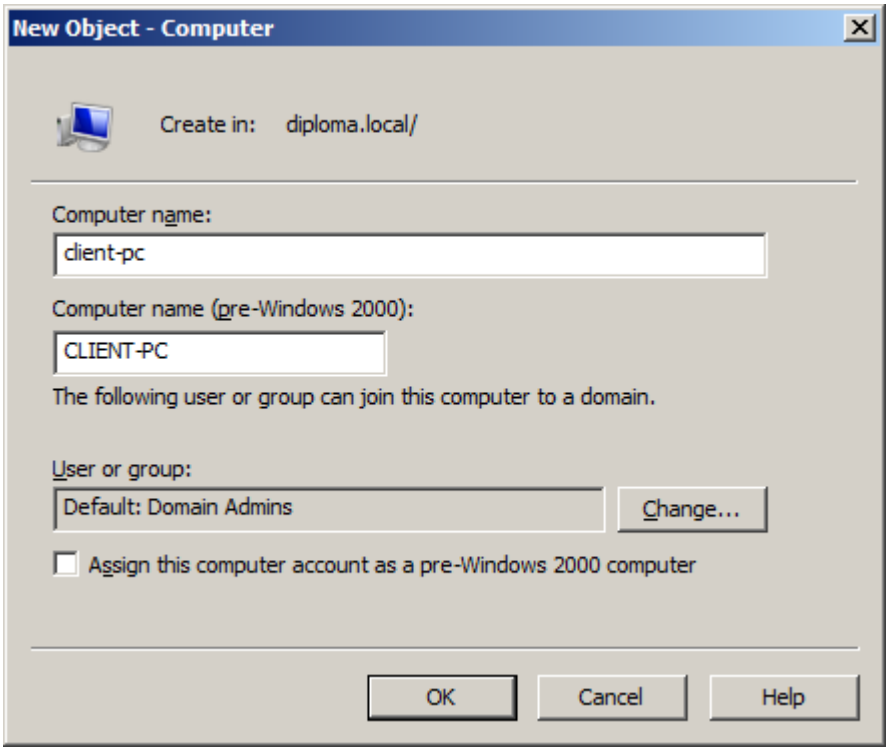
Έπειτα εισάγουμε τον κωδικό του. Αν θέλουμε μπορούμε να υποχρεώσουμε τον χρήστη να αλλάξει κωδικό όταν συνδεθεί ή να του απαγορέψουμε να αλλάξει κωδικό, ανάλογα με τους κανόνες ασφαλείας που θέλουμε να εφαρμόσουμε.



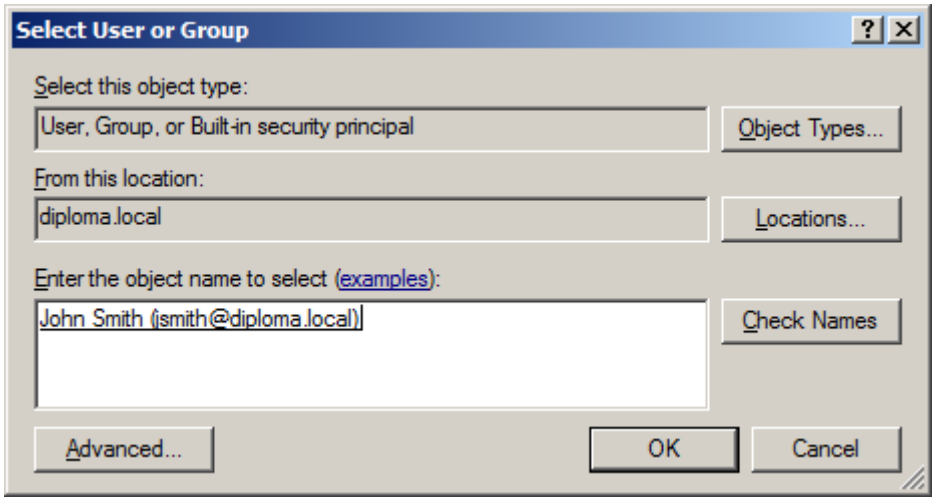
Έπειτα χρειάζεται να εισάγουμε και έναν νέο υπολογιστή στο domain. Κάνοντας πάλι δεξί κλικ πάνω στο όνομα του domain επιλέγουμε New Computer.



Εκεί εισάγουμε το όνομα του υπολογιστή.



Έπειτα χρειάζεται να δώσουμε πρόσβαση στον νέο χρήστη που δημιουργήσαμε, πατώντας το Change στο User or Group.



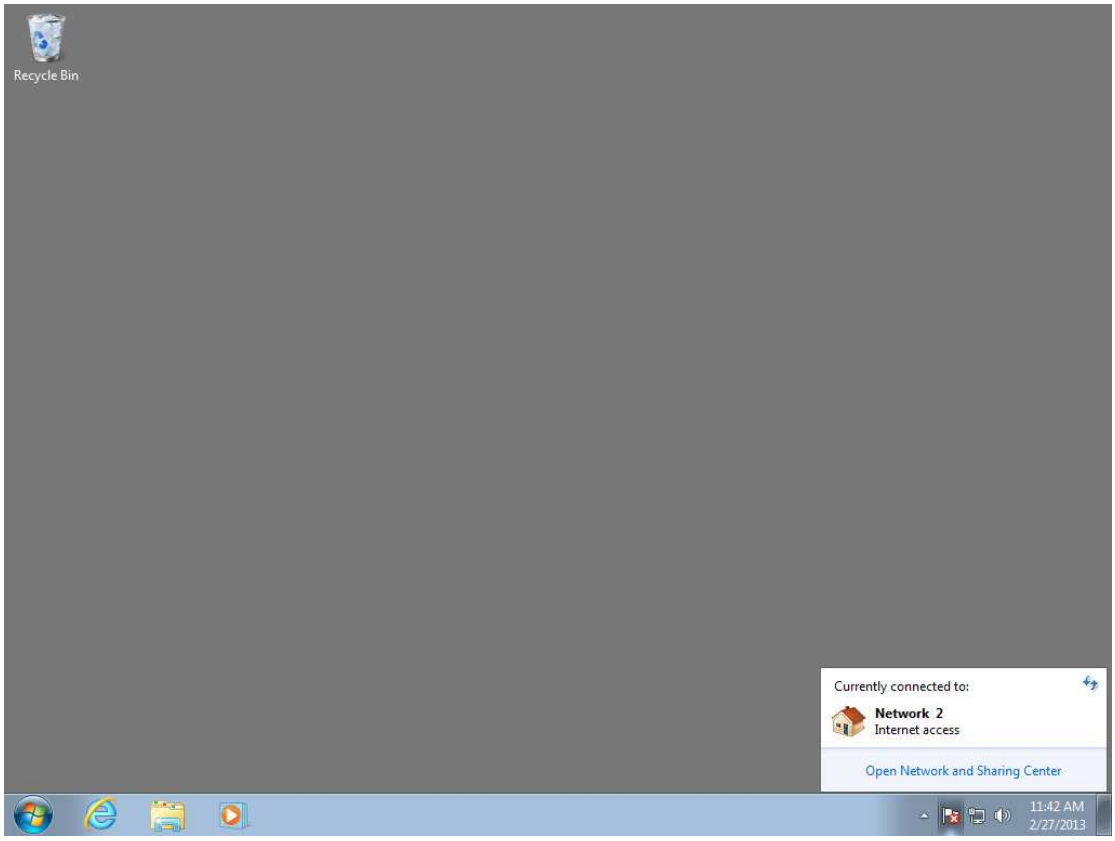
Γράφοντας το όνομα του χρήστη και πατώντας το Check Names εμφανίζεται ο χρήστης που εισάγαμε προηγουμένως.

5.6 Σύνδεση ενός υπολογιστή στο δίκτυο

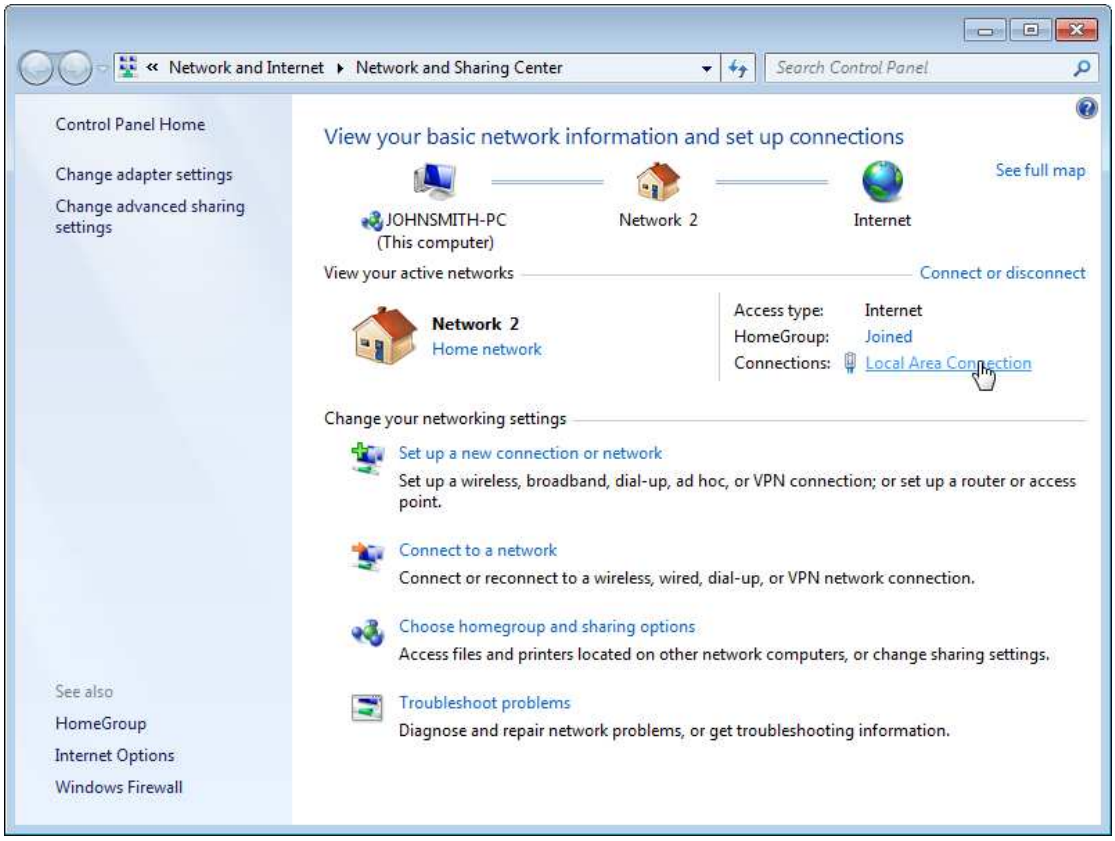
Για να επιδείξουμε τις δυνατότητες του PKI είναι απαραίτητο να υπάρχει και ένας υπολογιστής client ο οποίος θα συνδέεται στον server. Σαν client χρησιμοποιήθηκε ένα μηχάνημα Windows 7 με μία νέα εγκατάσταση.

Το πρώτο βήμα της εγκατάστασης ήταν να οριστεί μία σταθερή διεύθυνση IP για αυτόν τον υπολογιστή. Όπως αναφέραμε παραπάνω κατά την δημιουργία ενός δικτύου ενδείκνυται να εγκατασταθεί η υπηρεσία DHCP Server στον server ώστε να διαχειρίζεται τις διευθύνσεις των υπολογιστών που συνδέονται στο δίκτυο. Η διαδικασία είναι παρόμοια με αυτή του server.

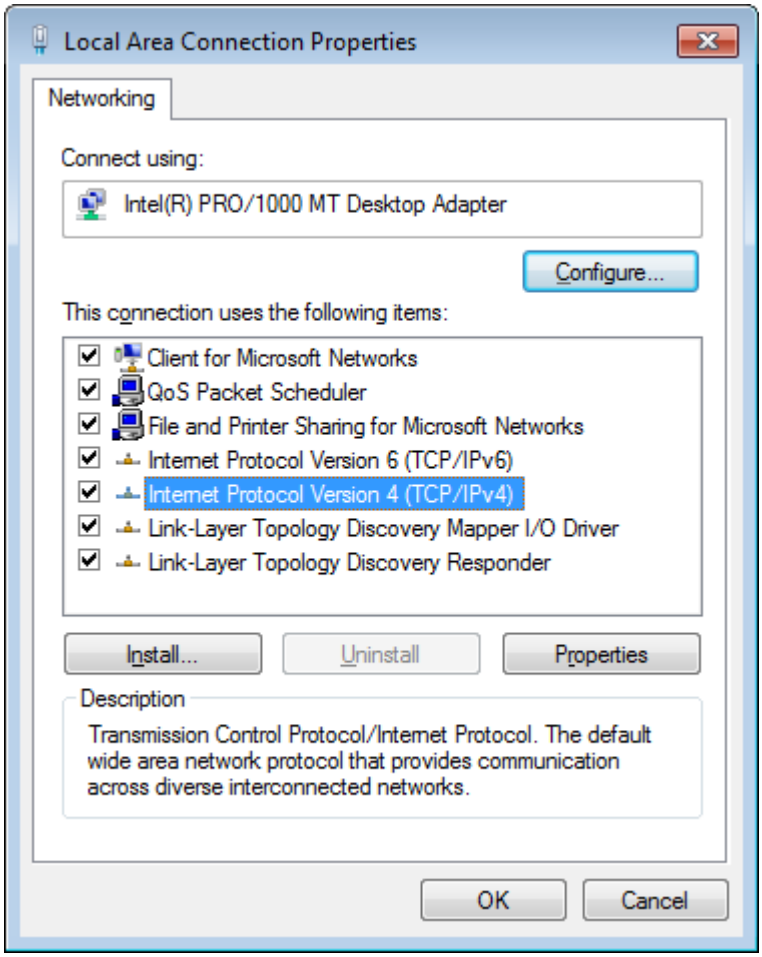
Για την απόδοση σταθερής IP χρειάζεται να ανοίξουμε το Network and Sharing Center κάνοντας κλικ στο εικονίδιο του δικτύου.



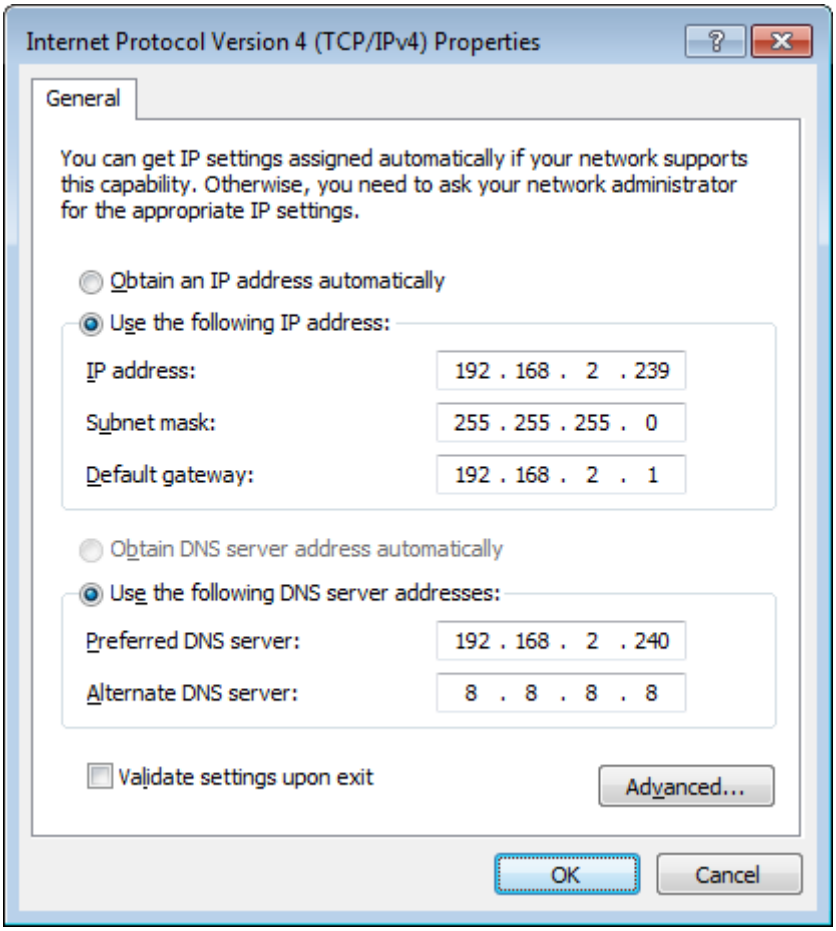
Έπειτα επιλέγουμε το Local Area Connection.



Εκεί επιλέγουμε Properties και μετά Internet Protocol Version 4 και πάλι Properties.

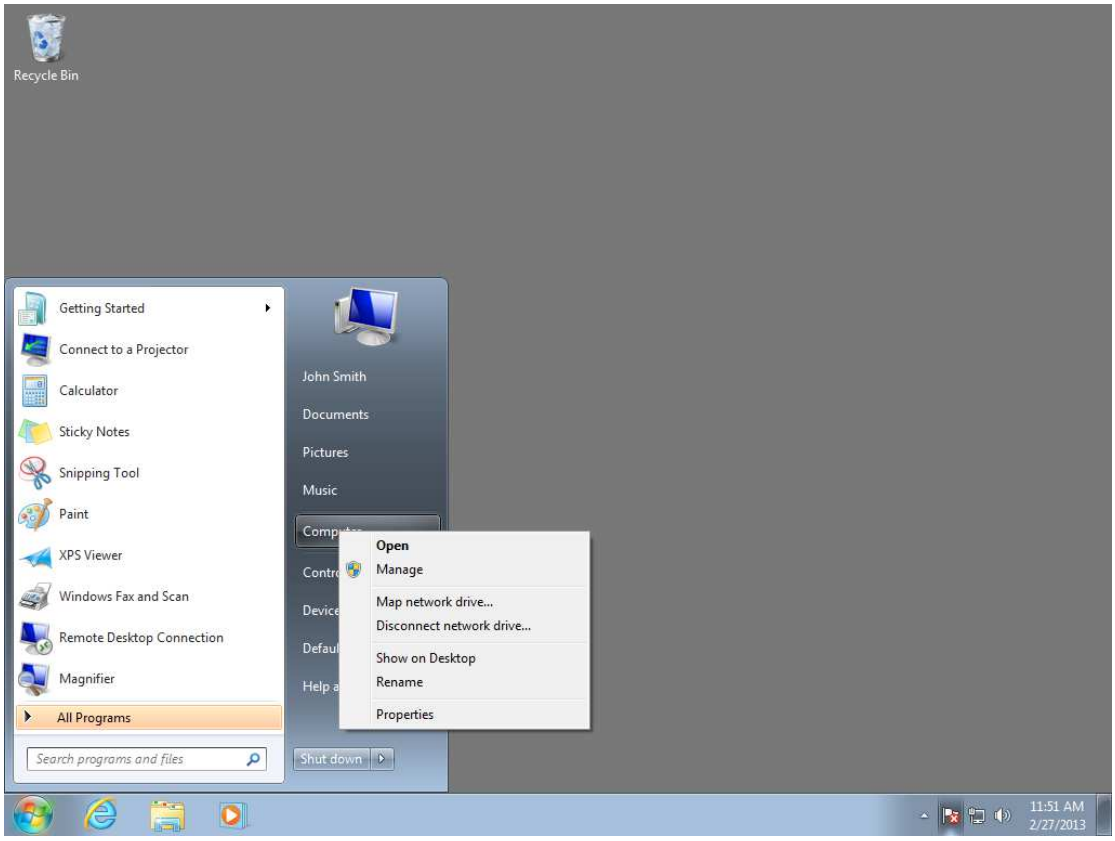


Εισάγουμε τις απαραίτητες ρυθμίσεις και πατάμε OK. Αφού δεν έχουμε ρυθμίσει τον DHCP Server πρέπει να εισάγουμε χειροκίνητα σαν DNS την διεύθυνση που έχουμε δώσει στον Server.

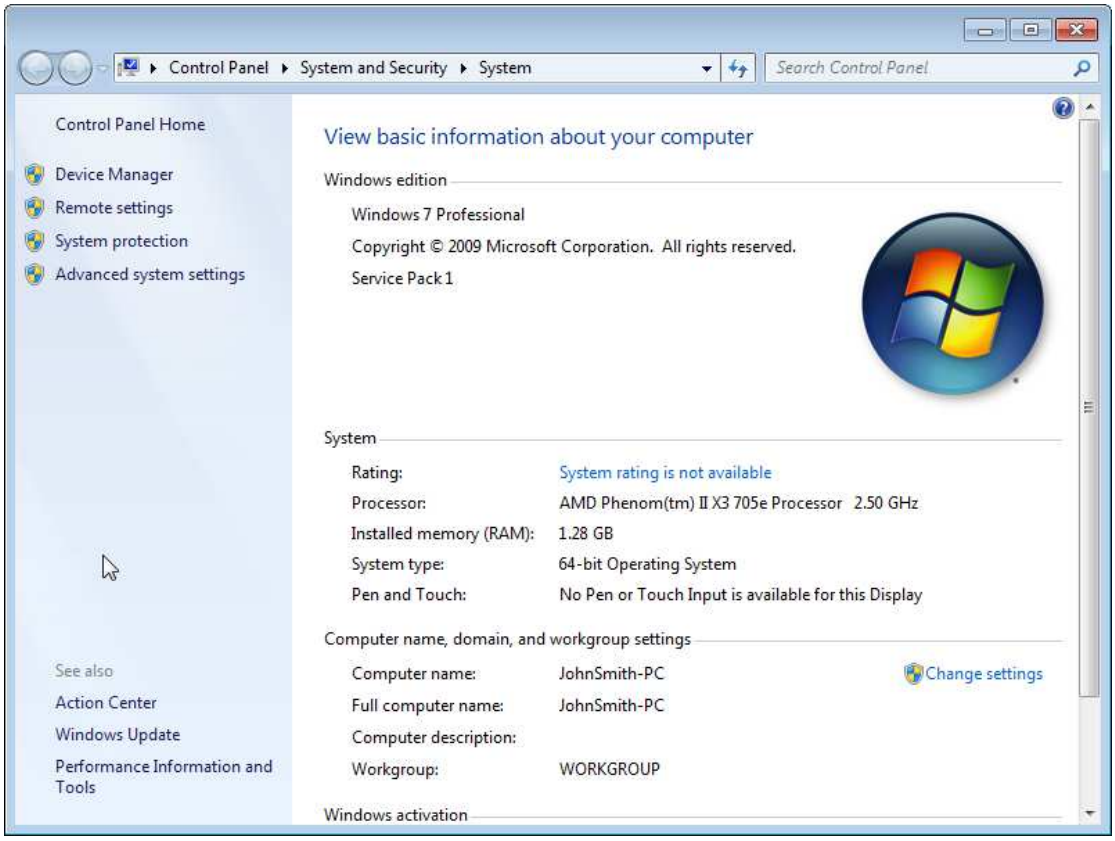


Όπως αναφέραμε προηγουμένως κατά την εγκατάσταση του Server αν είναι επιθυμητή η χρήση διευθύνσεων IPv6 χρειάζεται να γίνει παρόμοια διαδικασία και για το Internet Protocol Version 6.

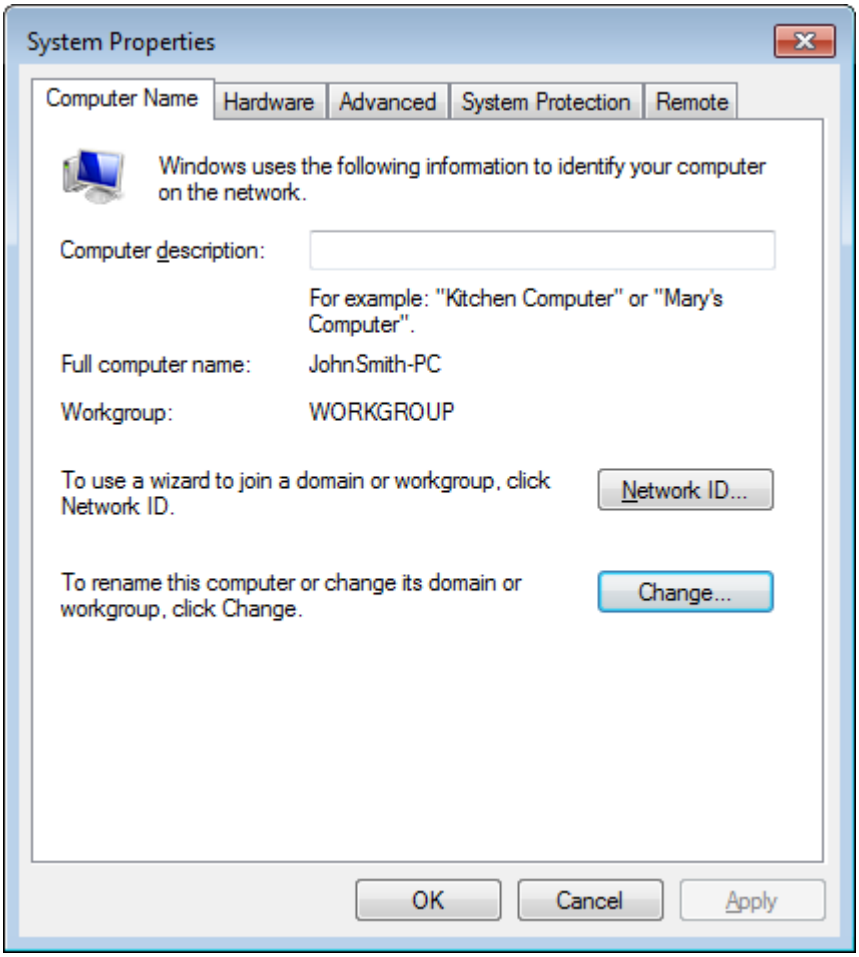
Έπειτα πρέπει να ρυθμίσουμε τον υπολογιστή ώστε να αποτελεί μέρος του domain που κατασκευάσαμε στην αρχή. Χρειάζεται να κάνουμε δεξί κλικ στην επιλογή Computer του Start Menu και να διαλέξουμε Properties.



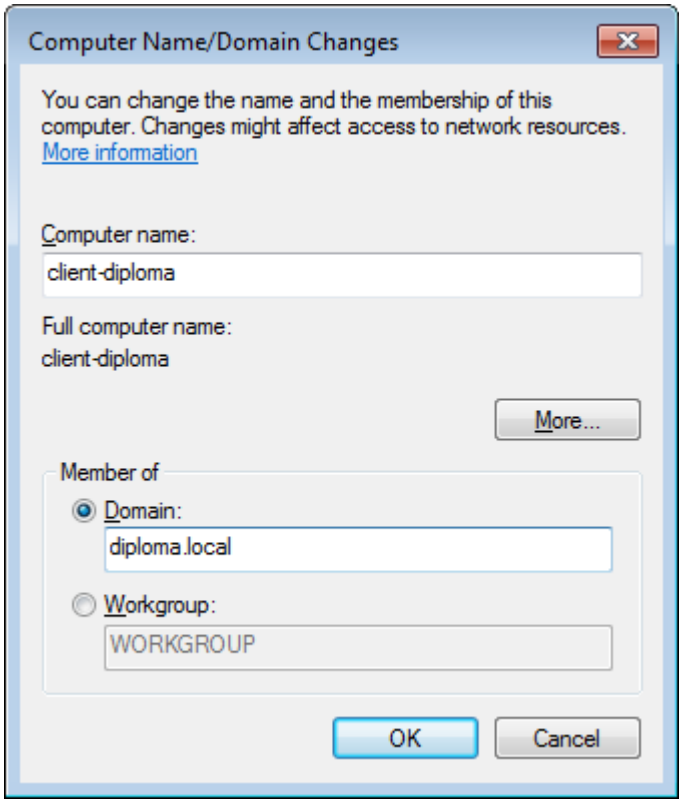
Από εκεί επιλέγουμε το Advanced System Settings από την αριστερή στήλη.



Από την καρτέλα Computer Name επιλέγουμε το Change.

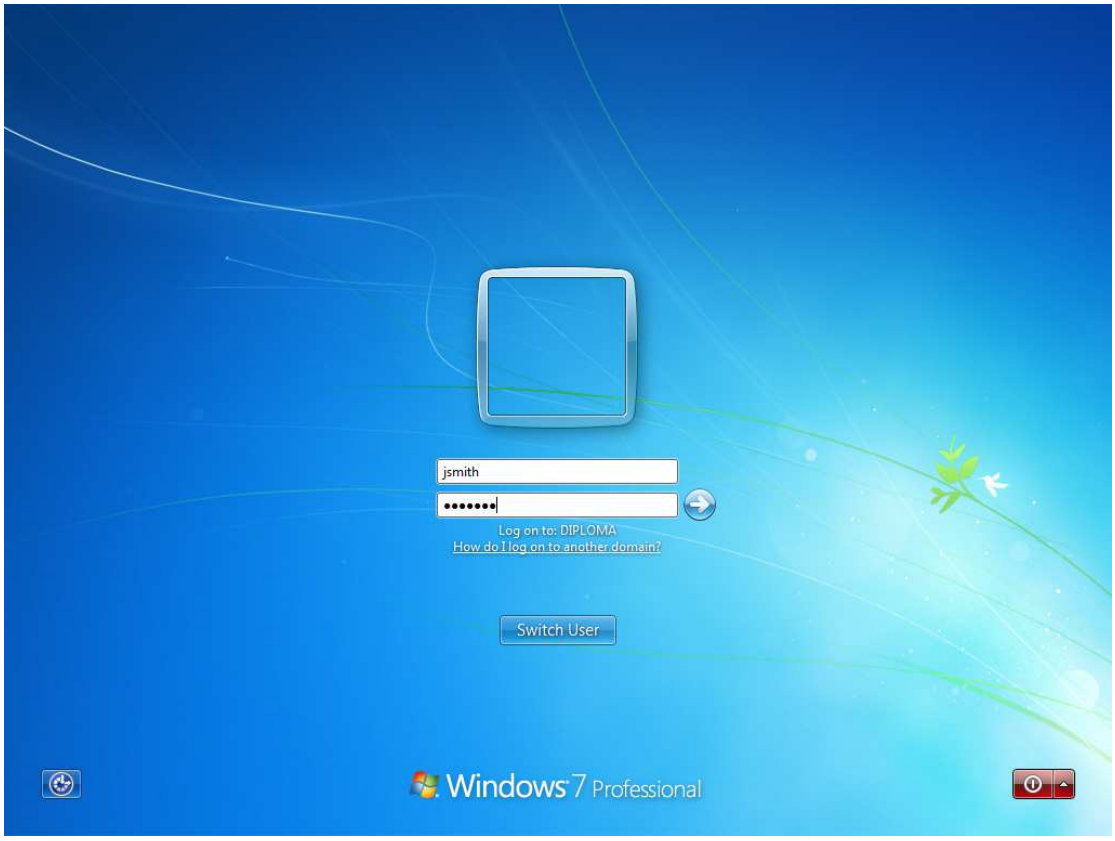


Τέλος συμπληρώνουμε το όνομα του υπολογιστή και το όνομα του domain. Σαν domain βάζουμε το diploma.local που δημιουργήσαμε προηγουμένως. Εμφανίζεται ένα παράθυρο το οποίο ζητάει τα απαραίτητα στοιχεία για την σύνδεση με το domain.



Εμφανίζεται μία οθόνη που ζητάει τα στοιχεία ενός χρήστη με δικαίωμα πρόσβασης στο domain. Εισάγουμε τα στοιχεία του χρήστη jsmith που δημιουργήσαμε προηγουμένως στον server. Αν όλα πήγαν καλά θα παρουσιαστεί ένα παράθυρο επιβεβαίωσης.

Για να ολοκληρωθούν οι αλλαγές χρειάζεται να γίνει επανεκκίνηση του υπολογιστή. Μετά την επανεκκίνηση η οθόνη εισόδου ζητάει τα στοιχεία για έναν χρήστη στο domain diploma.

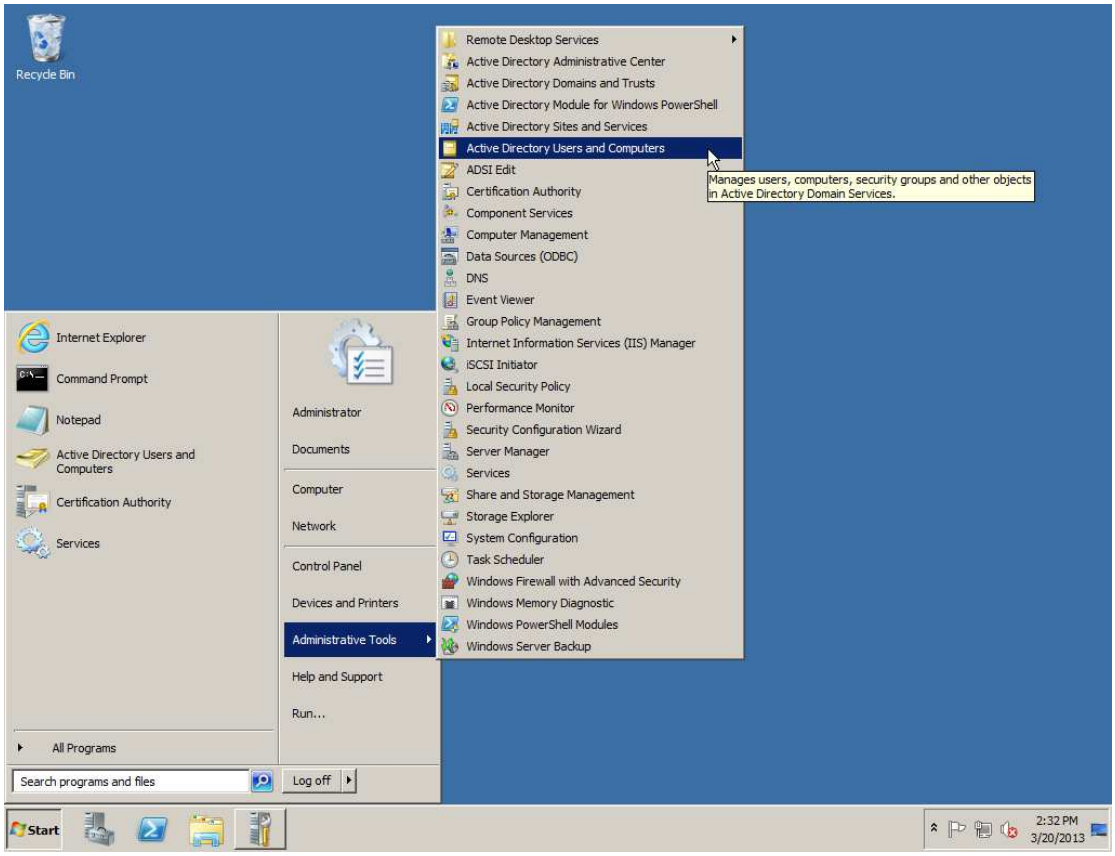


Αξίζει να σημειωθεί ότι είναι ακόμη δυνατόν να συνδεθεί ένας χρήστης σαν τοπικός χρήστης σε αυτόν τον υπολογιστή. Αν κάτι τέτοιο δεν είναι επιθυμητό μπορούν να τροποποιηθούν τα Local Group Policies του μηχανήματος ώστε να δέχεται χρήστες μόνο από το domain diploma.

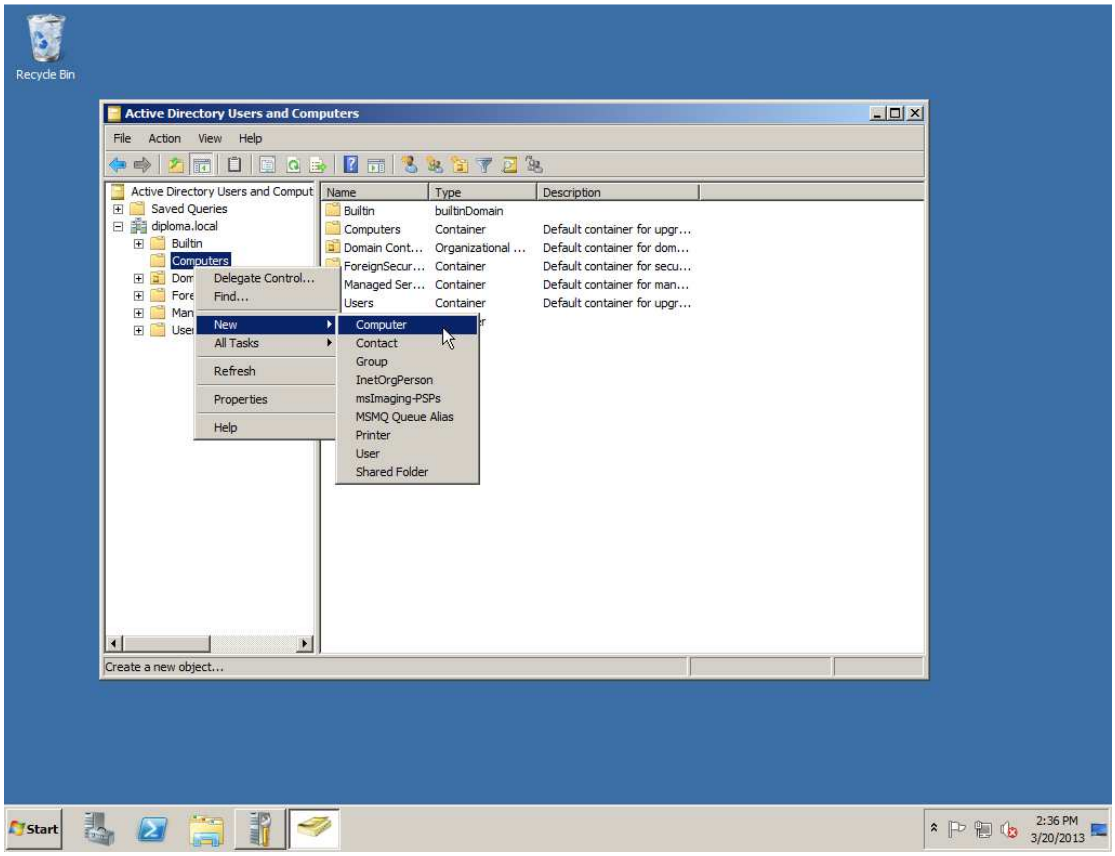
5.7 Προσθήκη υπολογιστών και χρηστών στο Active Directory

Πριν κάνουμε κάποια αλλαγή χρειάζεται να προσθέσουμε τους νέους υπολογιστές και χρήστες στον κατάλογο του Active Directory.

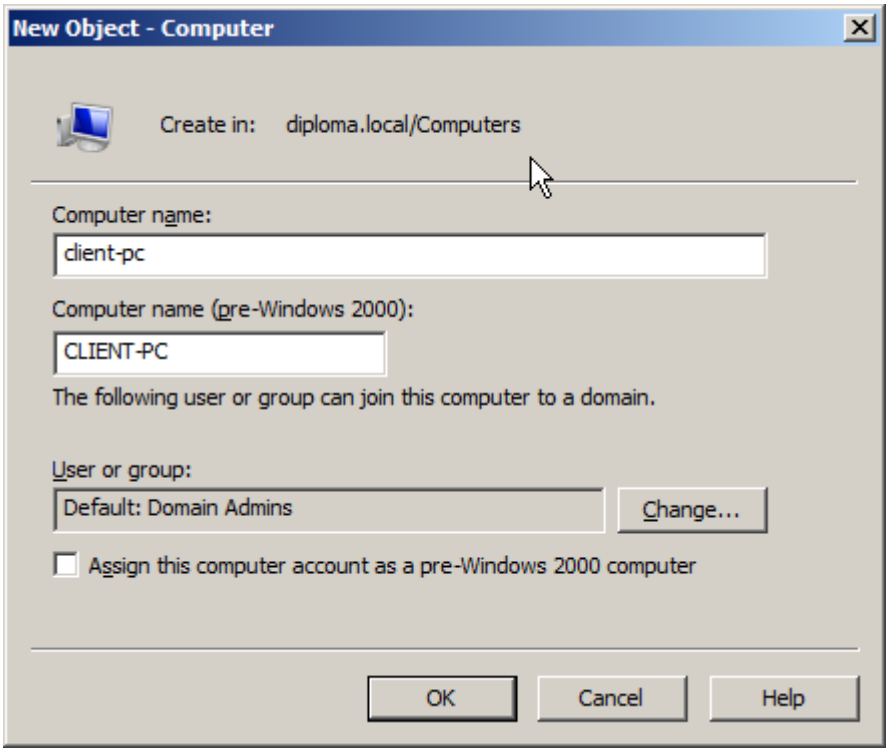
Από το Start menu επιλέγουμε Active Directory Users and Computers



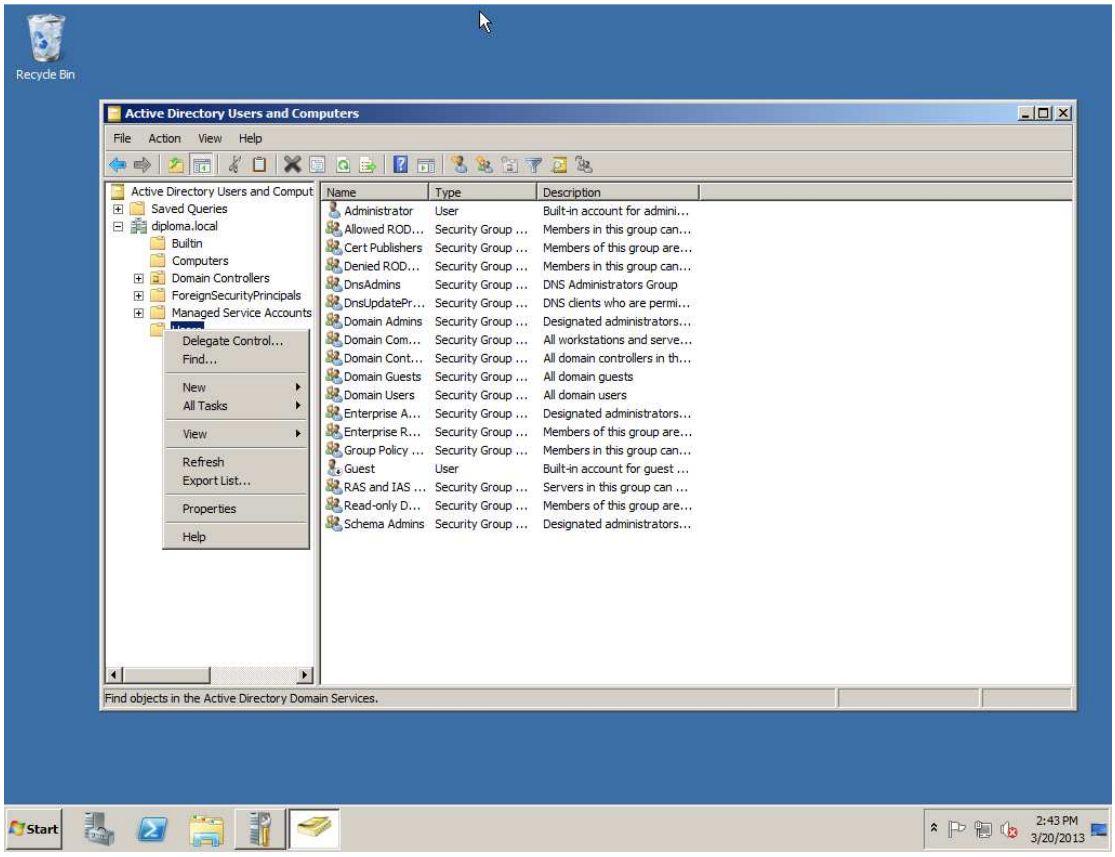
Έπειτα επιλέγουμε το όνομα του domain, diploma.local και κάνουμε δεξί κλικ στο Computers, επιλέγοντας New, Computer.



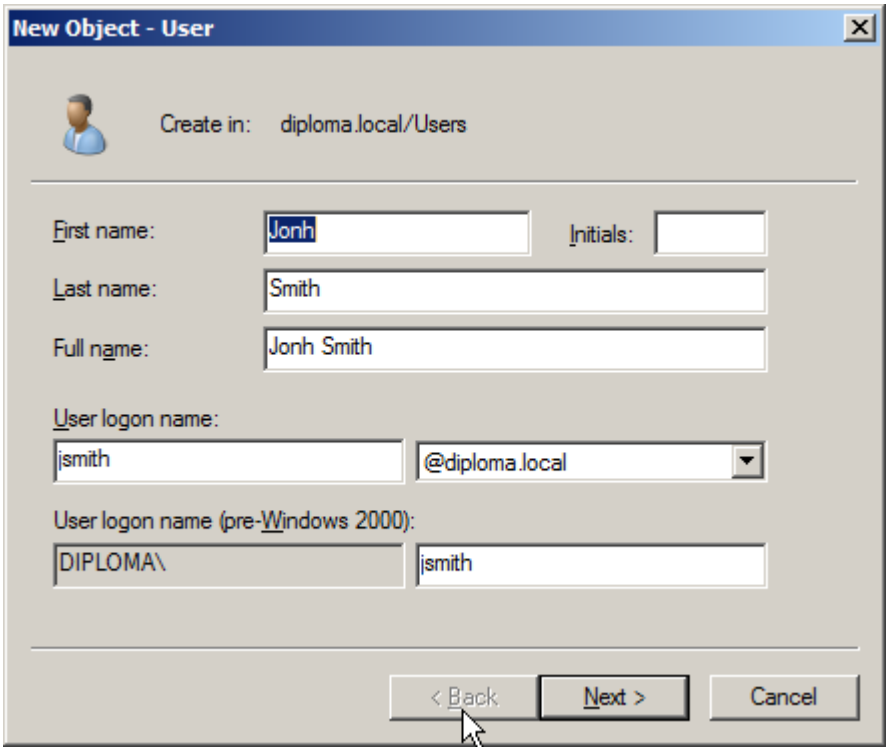
Στο νέο παράθυρο συμπληρώνουμε τα στοιχεία του υπολογιστή.



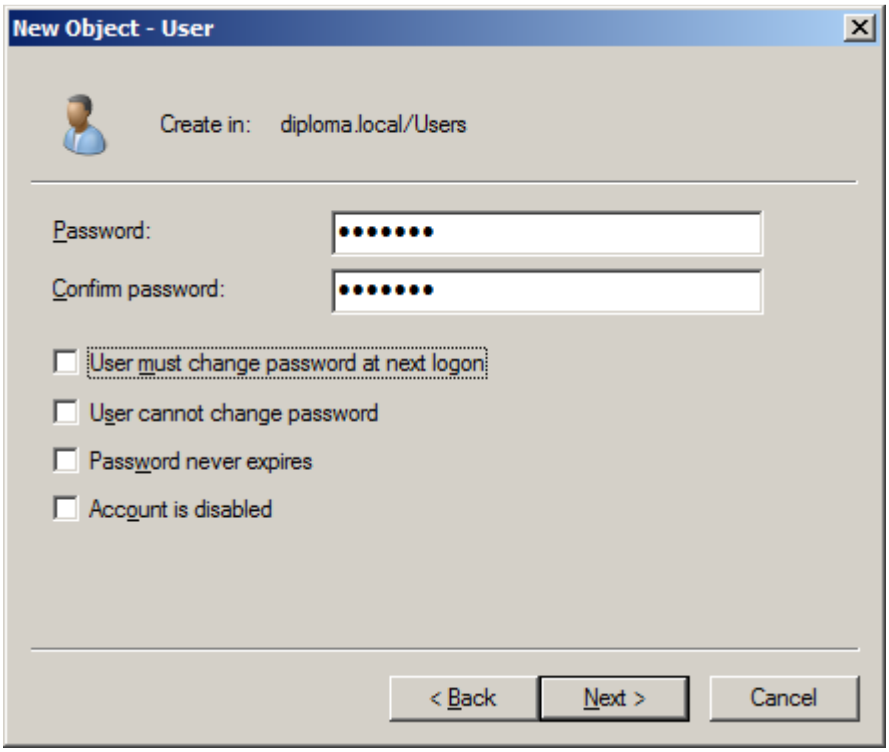
Με τον ίδιο τρόπο δημιουργούμε έναν νέο χρήστη κάνοντας στο Users δεξί κλικ και μετά New, User.



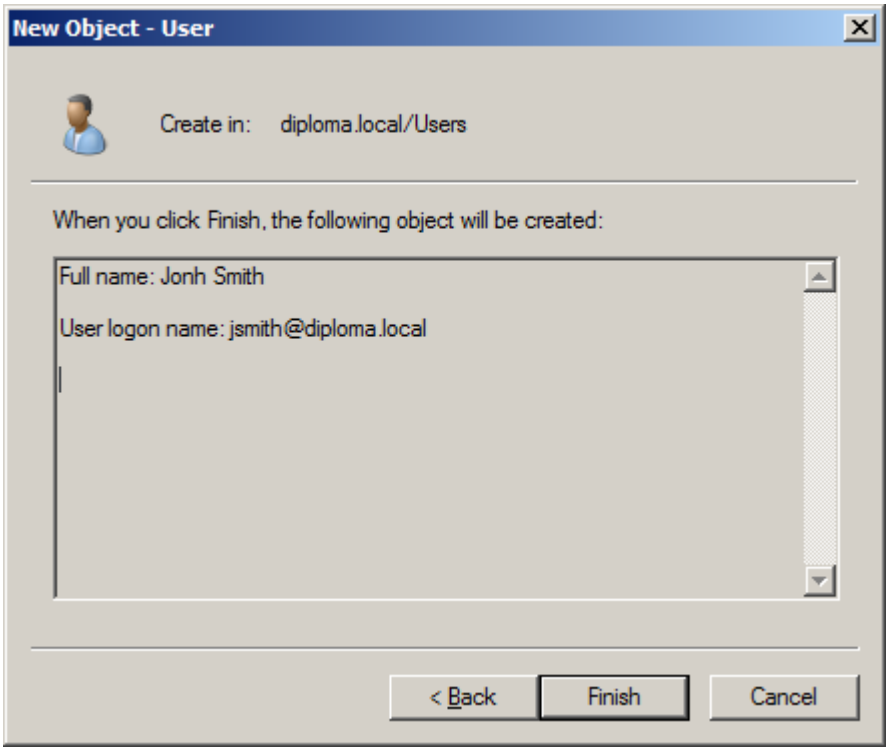
Εκεί συμπληρώνουμε τα στοιχεία του χρήστη.



Έπειτα συμπληρώνουμε τον κωδικό.



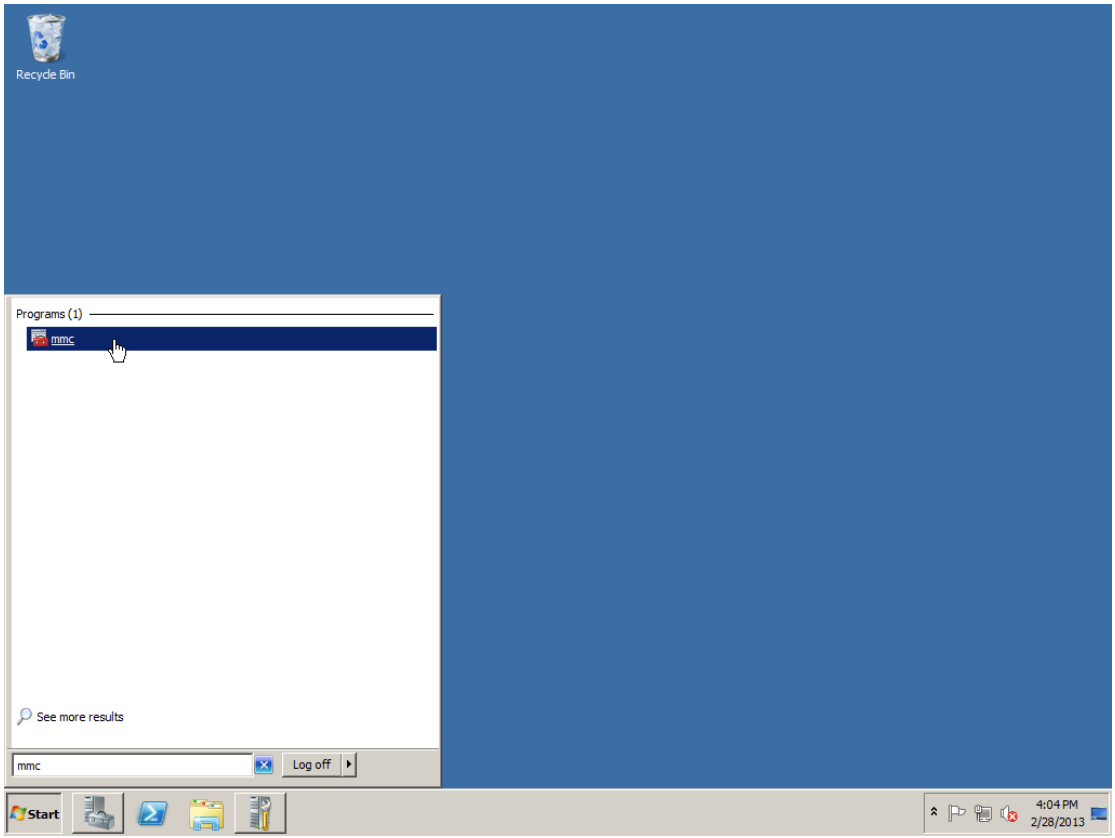
Τέλος επιβεβαιώνουμε τα στοιχεία.



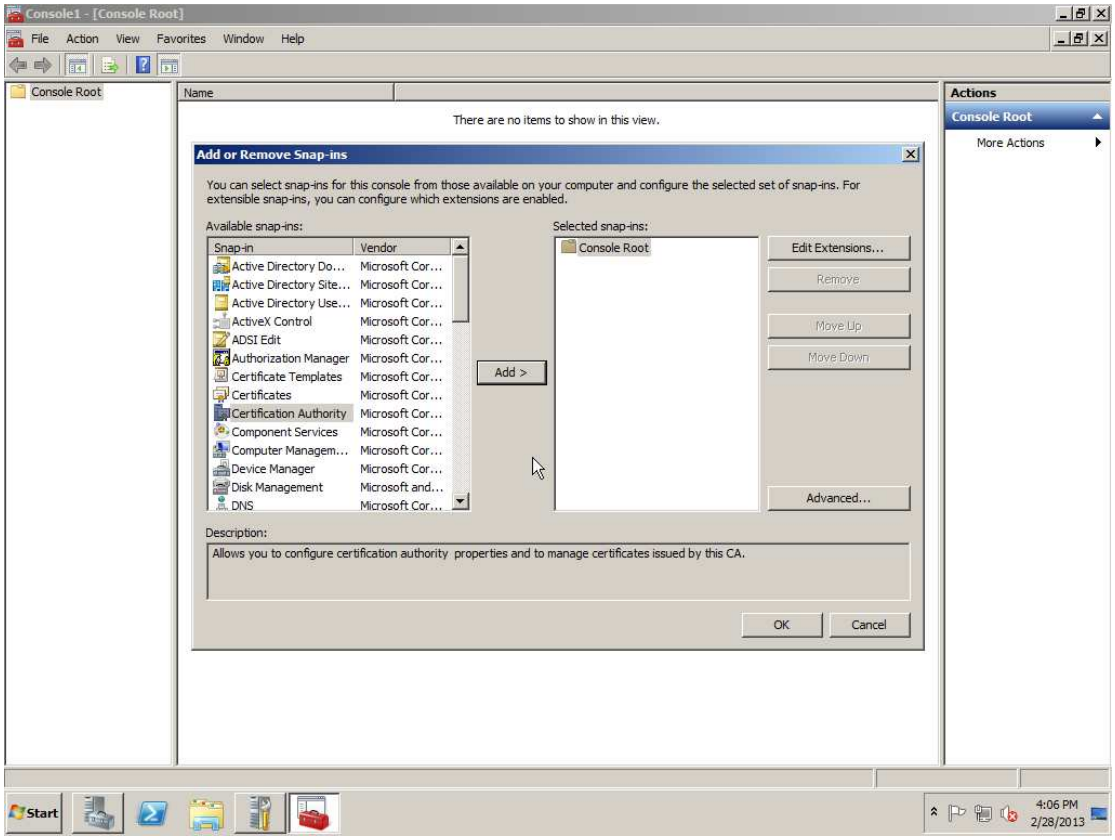
5.8 Δημιουργία πιστοποιητικού για έναν υπολογιστή

Το επόμενο βήμα είναι η δημιουργία ενός πιστοποιητικού για έναν υπολογιστή του δικτύου. Καθώς η χειροκίνητη δημιουργία πιστοποιητικών δεν είναι πρακτική θα ρυθμίσουμε την αρχή πιστοποιητικών ώστε να εκδίδει αυτόματα πιστοποιητικά για κάθε υπολογιστή του domain.

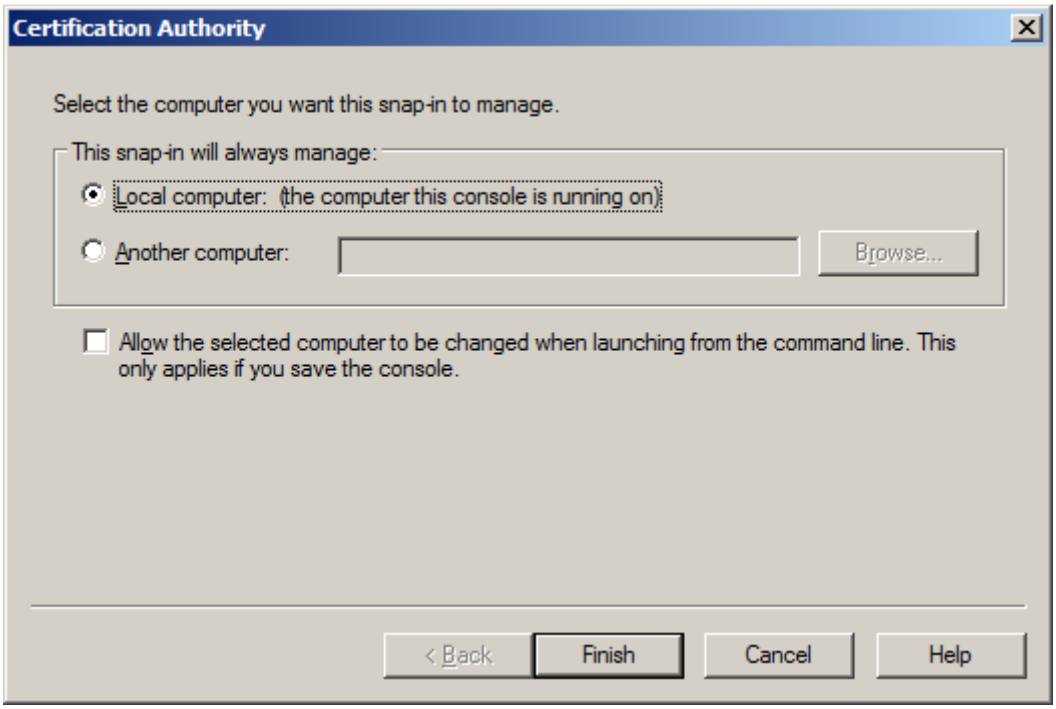
Στον server χρειάζεται να εκτελέσουμε το πρόγραμμα mmc.



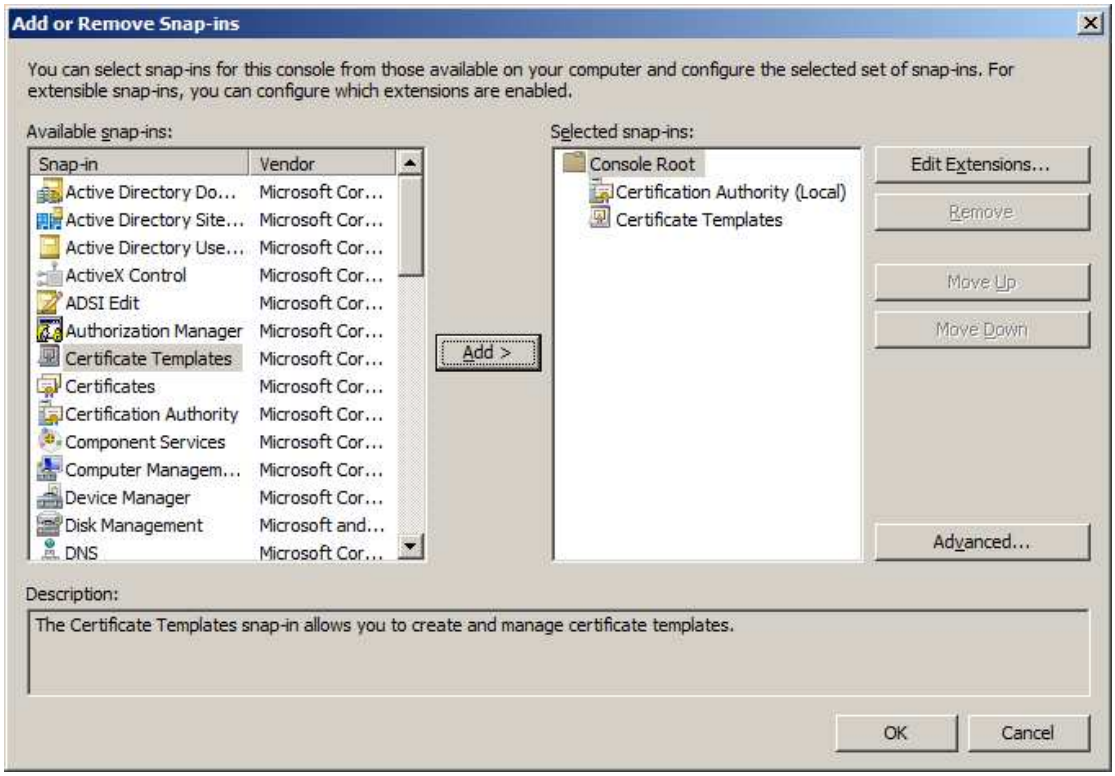
Από εκεί στο μενού File επιλέγουμε το Add/Remove Snap-in. Επιλέγουμε το Certificate Authority και πατάμε Add.



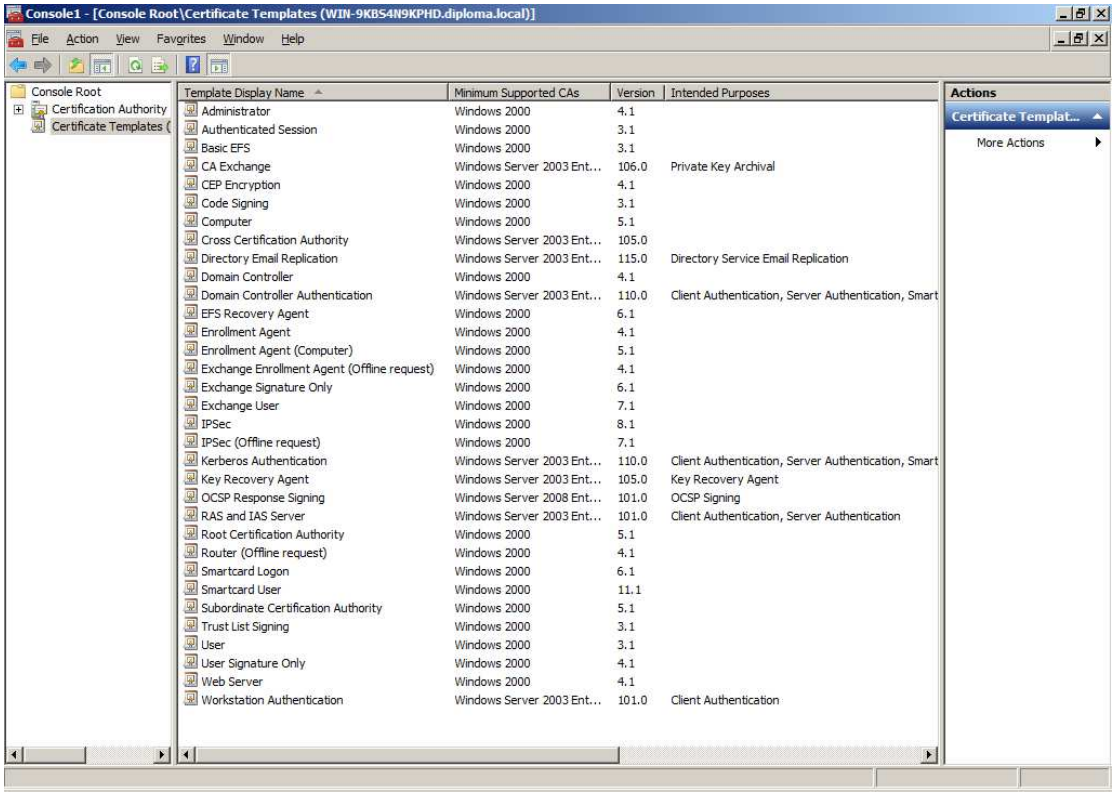
Στο παράθυρο που εμφανίζεται επιλέγουμε το Certificate Authority που θέλουμε να διαχειριστούμε, στην περίπτωσή μας το Local Computer.



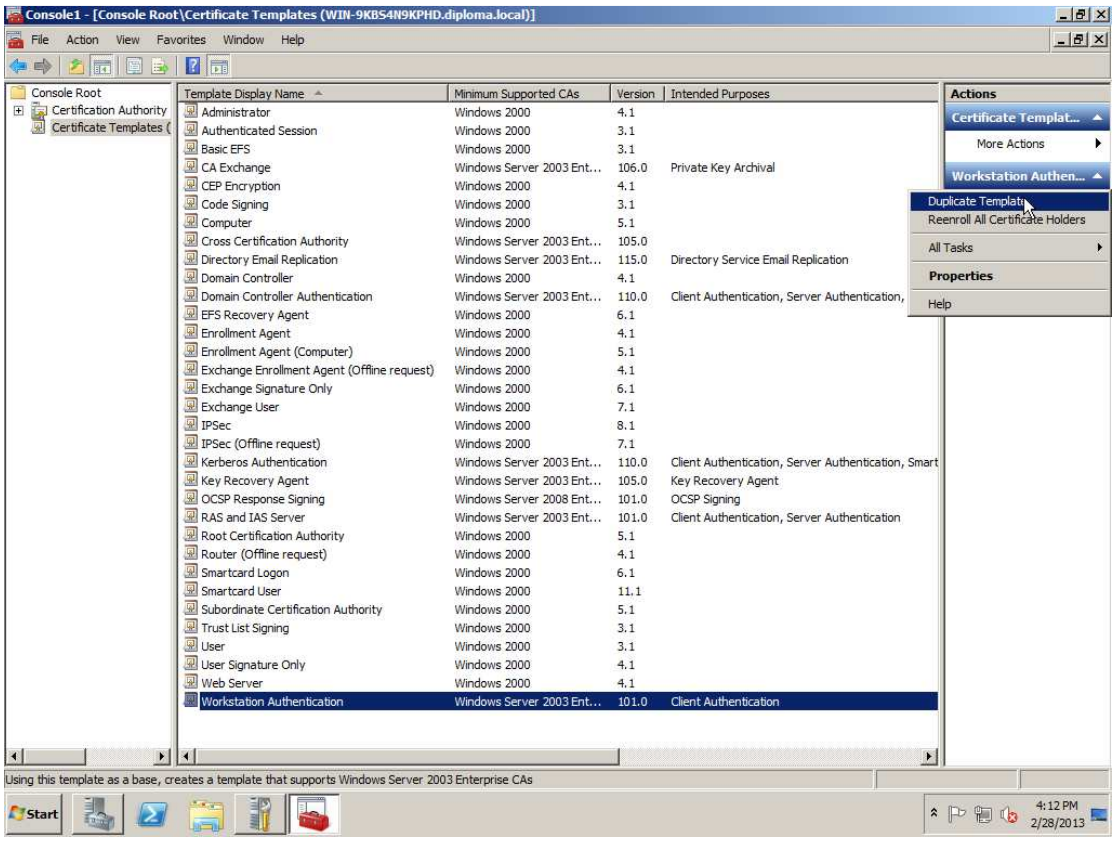
Πατάμε OK και επαναλαμβάνουμε την διαδικασία για να προσθέσουμε το Certificate Templates.



Πατώντας στο δέντρο στα αριστερά το Certificate Templates εμφανίζεται μία λίστα με όλα τα πρότυπα πιστοποιητικών που υπάρχουν στον υπολογιστή.

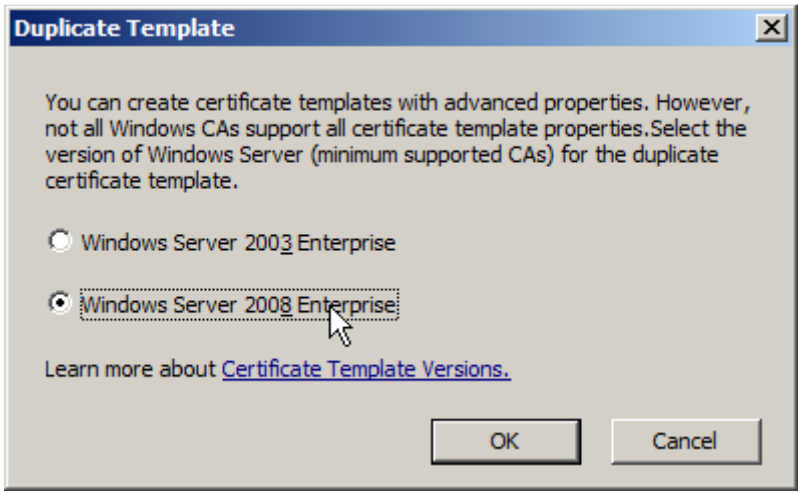


Κάνουμε κλικ στο Workstation Authentication και από την δεξιά στήλη επιλέγουμε το Duplicate Certificate κάτω από το Workstation Template και More Actions.

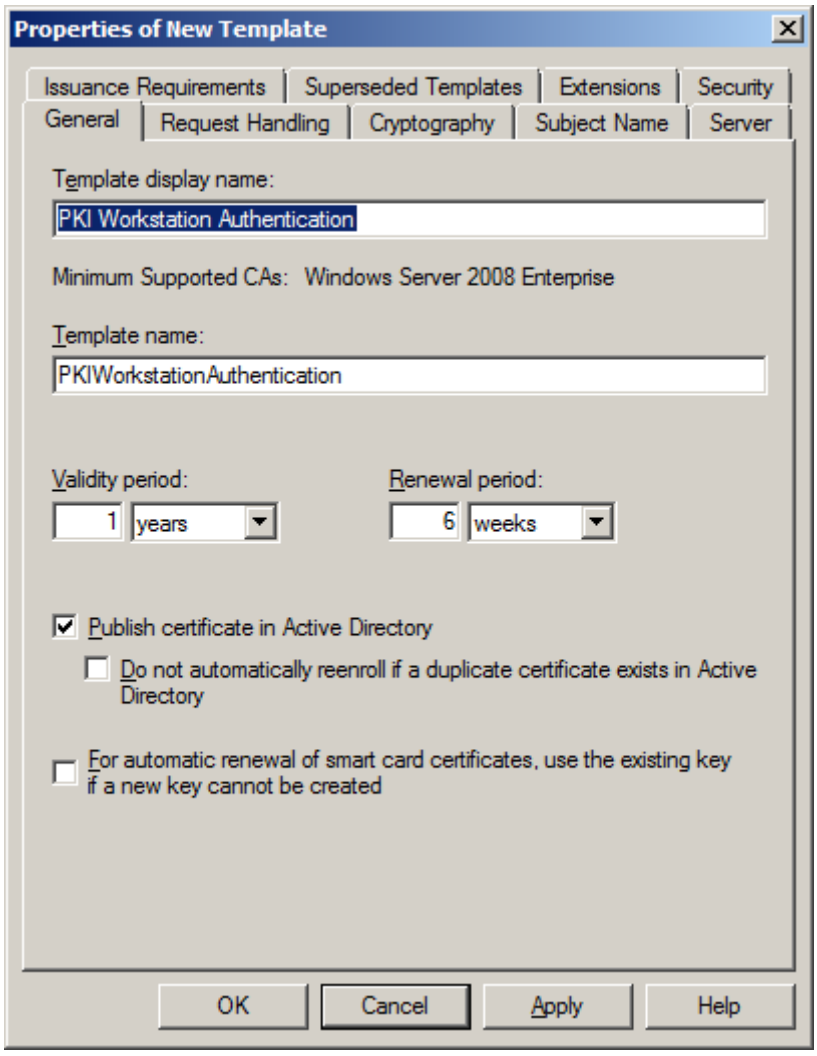


Το σύστημα ρωτάει την έκδοση του προτύπου που θέλουμε να δημιουργήσουμε. Επιλέγουμε το Windows Server 2008. Αν στο δίκτυο υπήρχαν υπολογιστές με παλιότερες

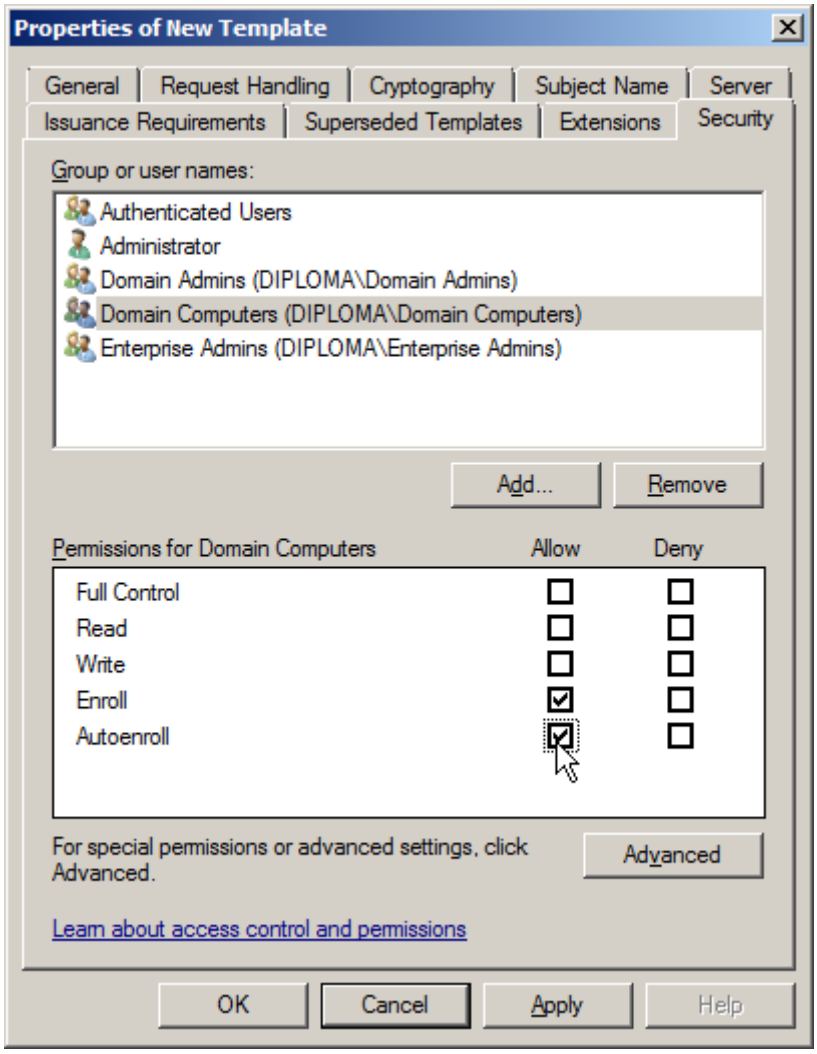
εκδόσεις των Windows μπορεί να ήταν επιθυμητή η χρήση του Windows Server 2003 για λόγους συμβατότητας.



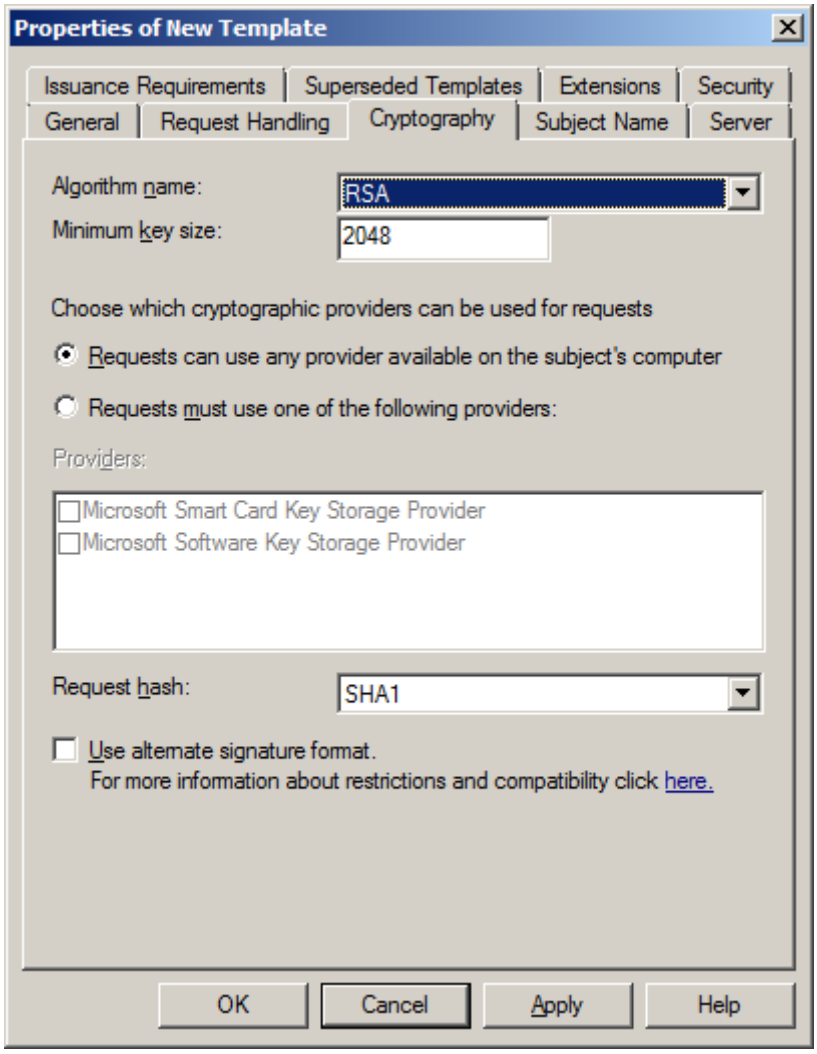
Εμφανίζεται ένα παράθυρο με τις ιδιότητες των νέων πιστοποιητικών. Από την καρτέλα General αλλάζουμε το όνομα του και αν ήταν επιθυμητό τις περιόδους ισχύς και ανανέωσης.



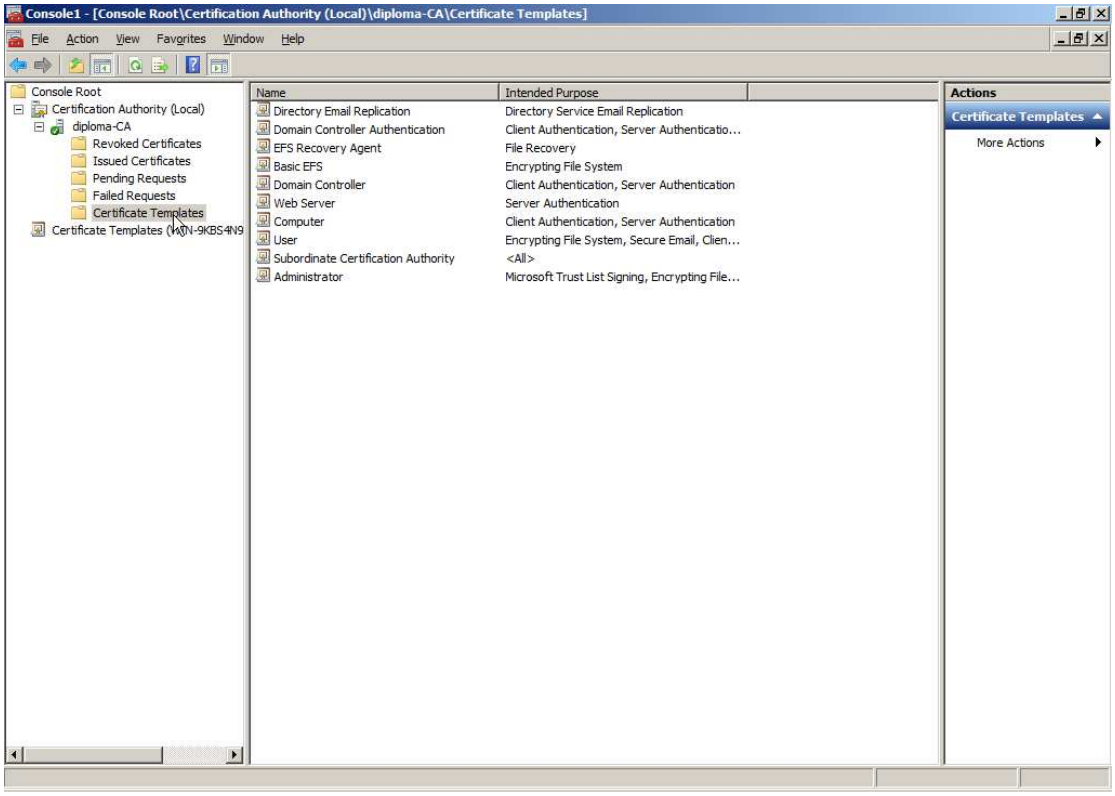
Στην καρτέλα Security επιλέγουμε το Domain Computers από την λίστα στην κορυφή. Με αυτό επιλεγμένο στην από κάτω λίστα επιλέγουμε την στήλη Allow για τις επιλογές Enroll και Autoenroll.



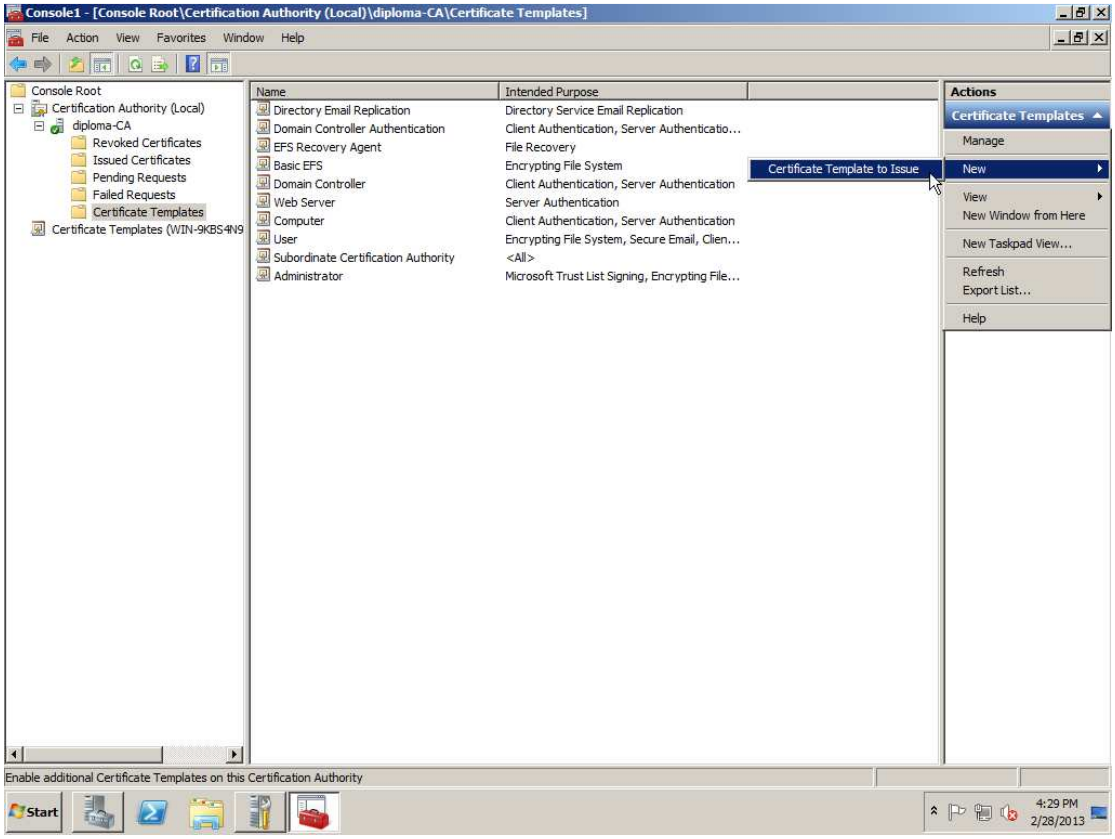
Αν θέλουμε μπορούμε να τροποποιήσουμε τις παραμέτρους κρυπτογραφίας του πιστοποιητικού από την καρτέλα Cryptography.



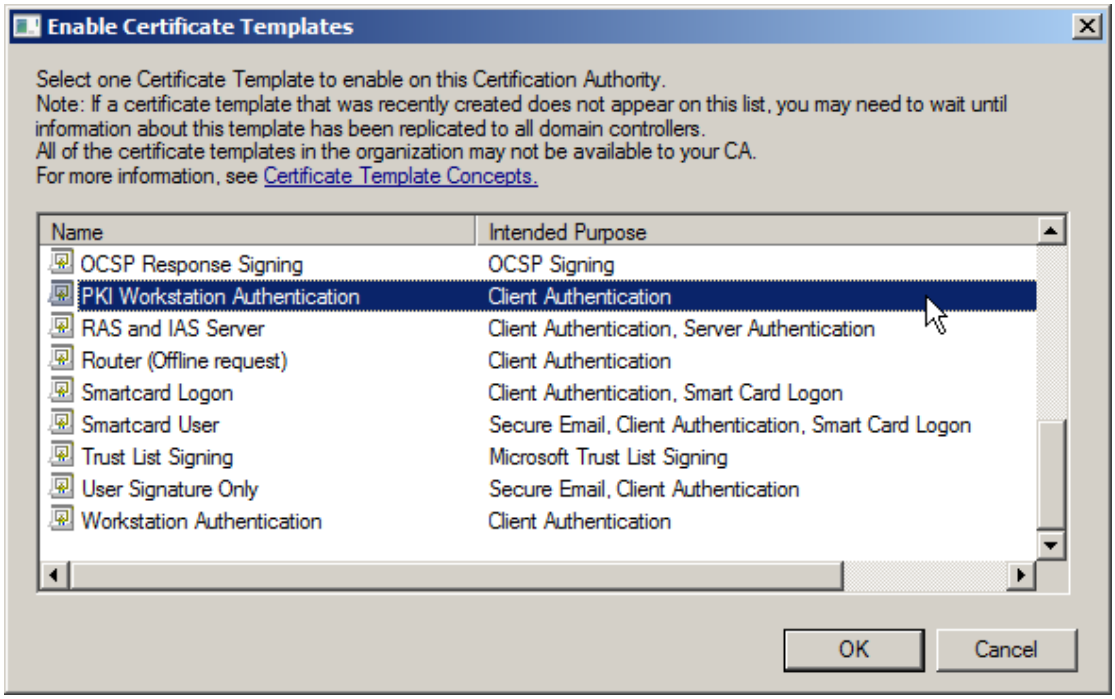
Έπειτα πατάμε OK για να κλείσει αυτό το παράθυρο. Μετά, στο δέντρο στα αριστερά ανοίγουμε το Certificate Authority, το diploma.local και κάνουμε κλικ στο Certificate Templates.



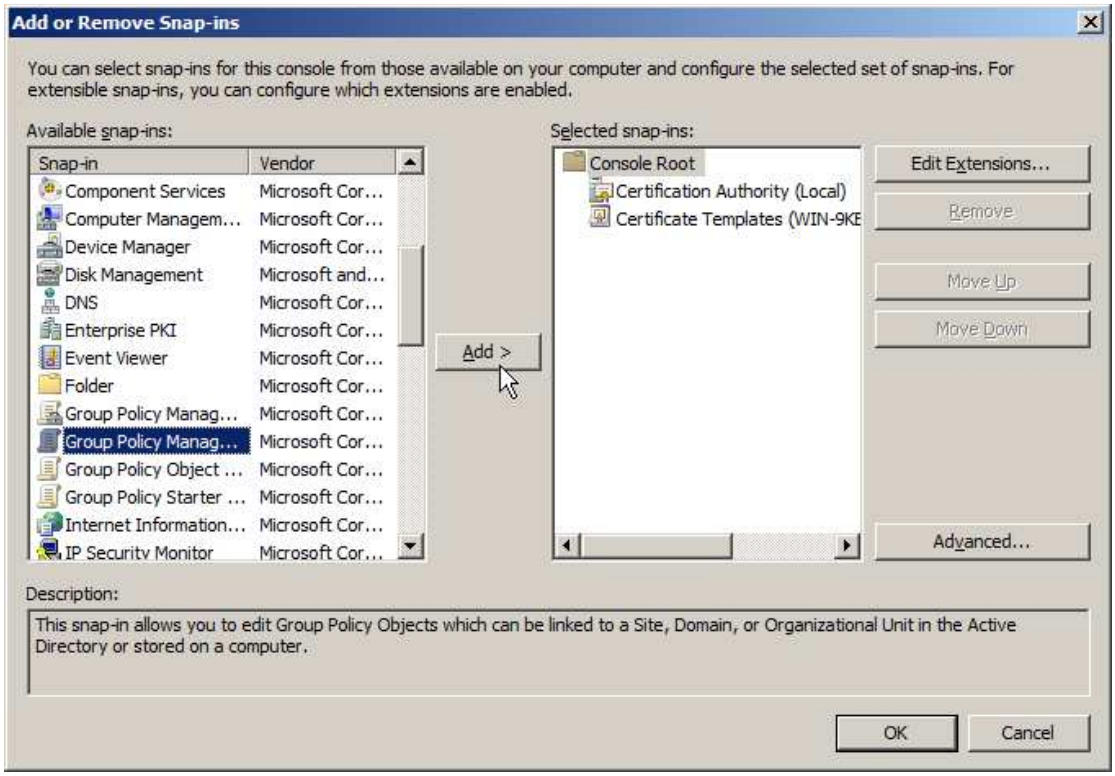
Με αυτό επιλεγμένο, από την δεξιά στήλη επιλέγουμε το More Actions, New, Certificate Template to Issue.



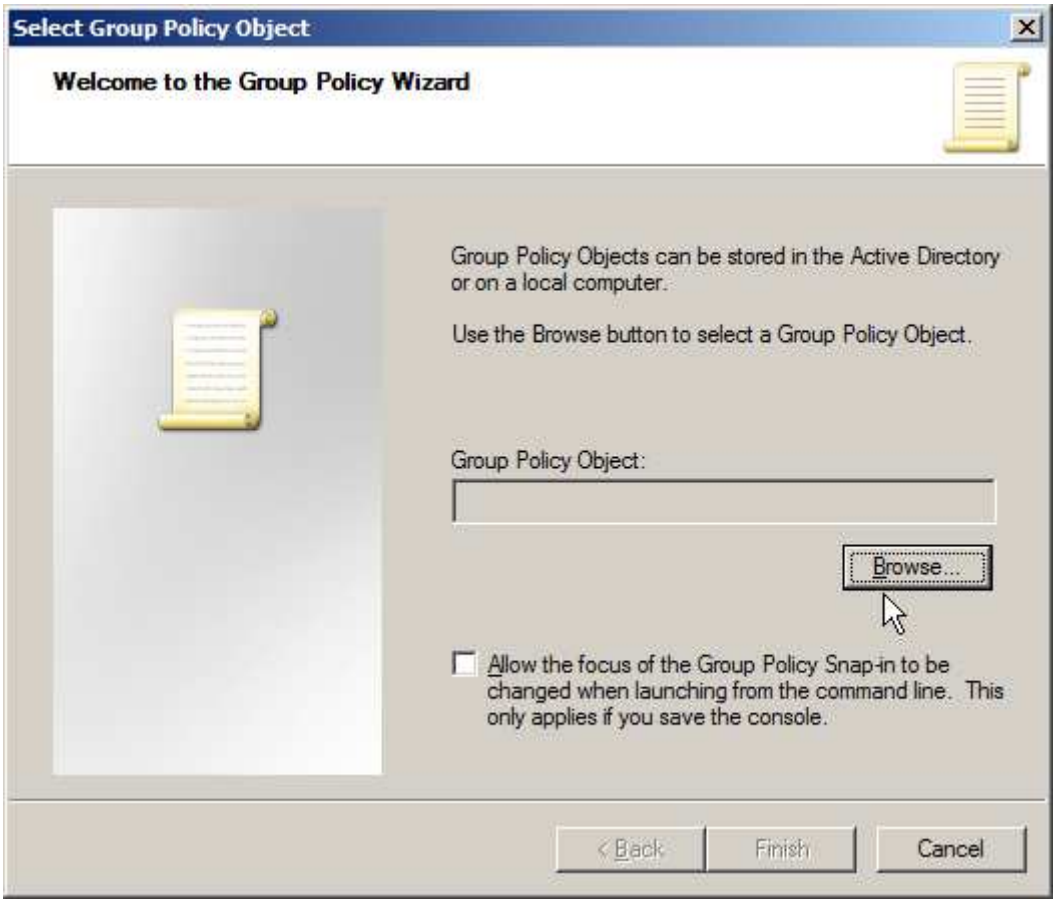
Από τη λίστα που εμφανίζεται διαλέγουμε το Πιστοποιητικό που δημιουργήσαμε προηγουμένως και πατάμε OK.



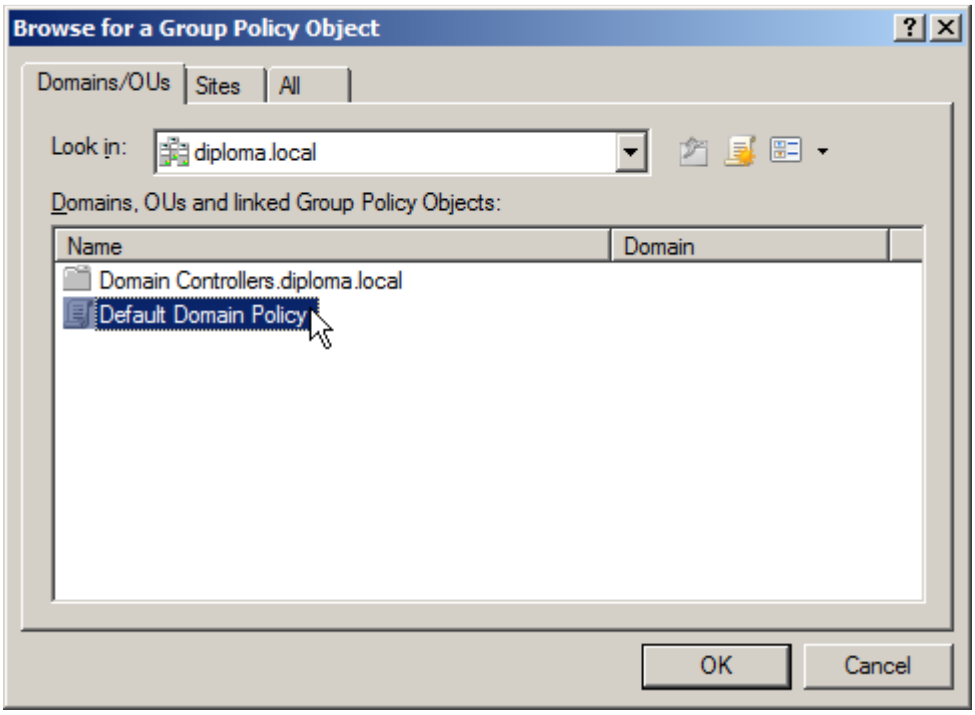
Έπειτα από το μενού File επιλέγουμε πάλι το Add/Remove Snap-in και διαλέγουμε το Group Policy Management Editor.



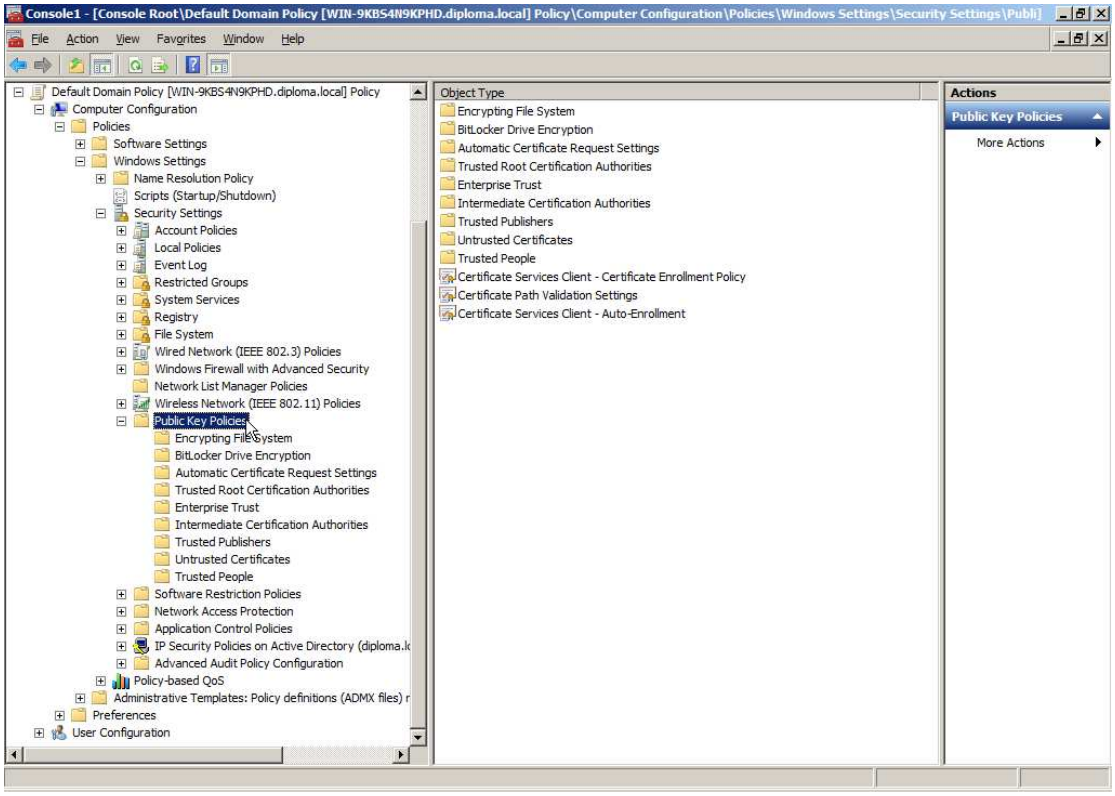
Στο παράθυρο που εμφανίζεται ζητείται να προσδιορίσουμε το αντικείμενο που θέλουμε να τροποποιήσουμε. Πατάμε Browse.



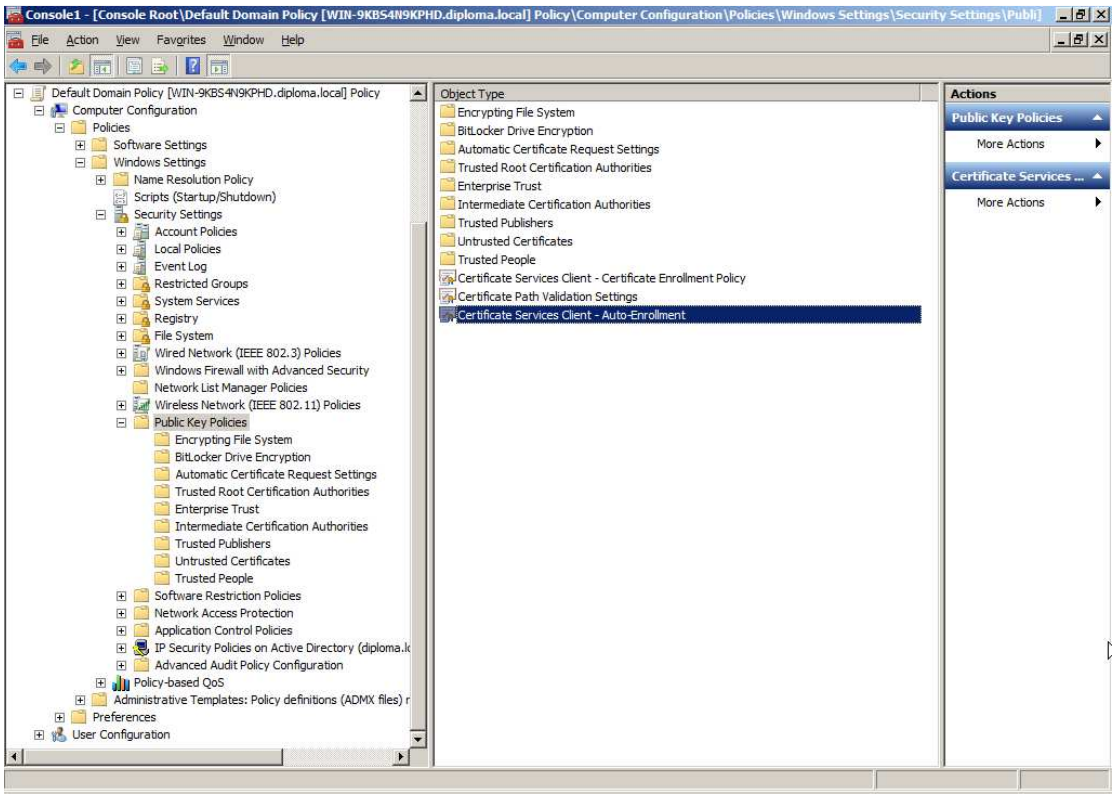
Επιλέγουμε το Default domain policy, OK, Finish και πάλι OK.



Από το δέντρο στα αριστερά ανοίγουμε τα Default domain policy, Computer configuration, Policies, Windows Settings, Security Settings, Public Key Policies και επιλέγουμε το τελευταίο.

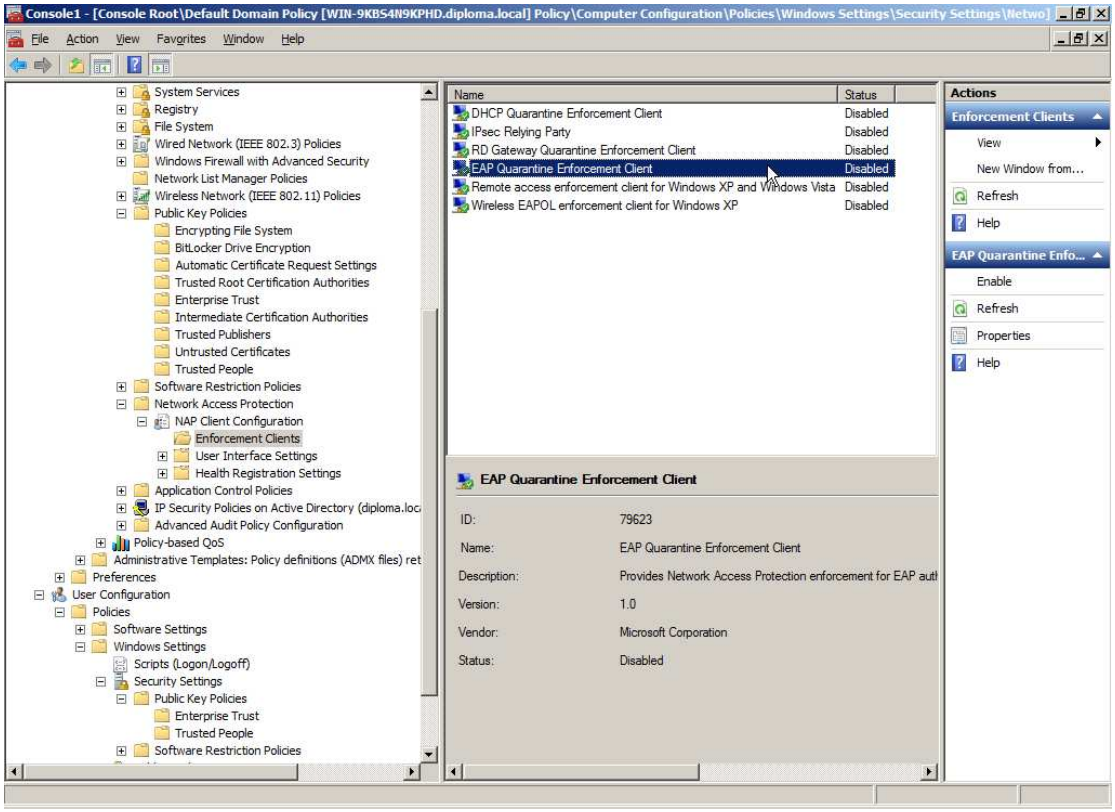


Από την μεσαία στήλη επιλέγουμε το Certificate Services Client - Auto-Enrollment και κάνουμε διπλό κλικ σε αυτό.

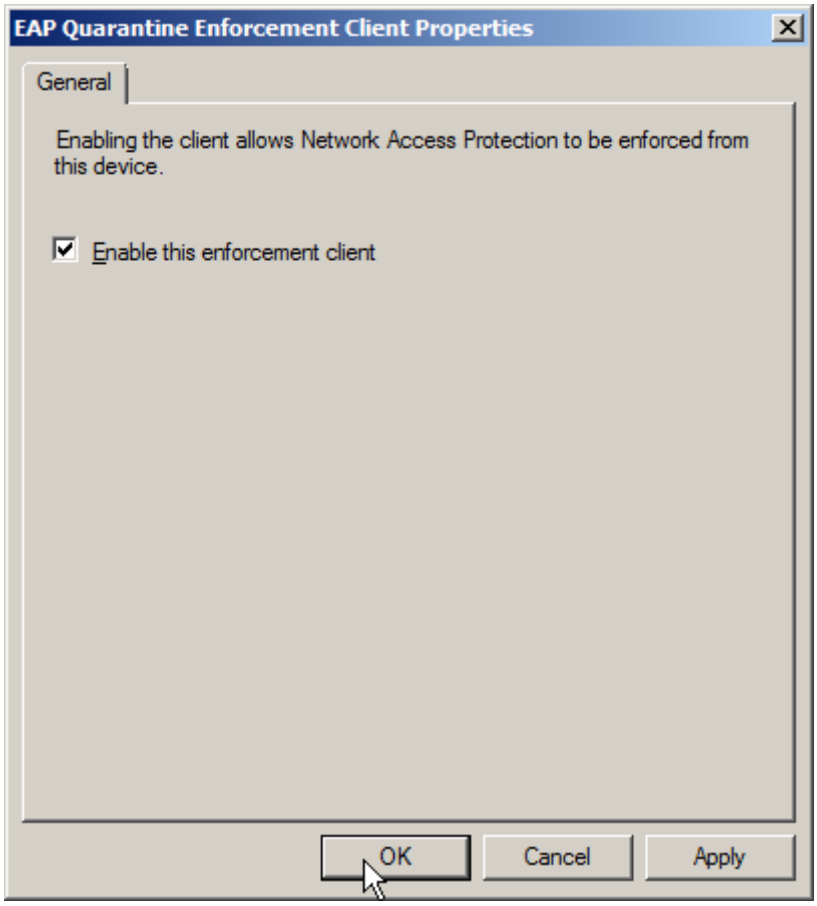


Στο παράθυρο που εμφανίζεται επιλέγουμε σαν Configuration model το Enabled. Έπειτα επιλέγουμε τα δύο πρώτα checkbox ώστε να εκδίδονται και να ανανεώνονται αυτόματα τα πιστοποιητικά και πατάμε OK.

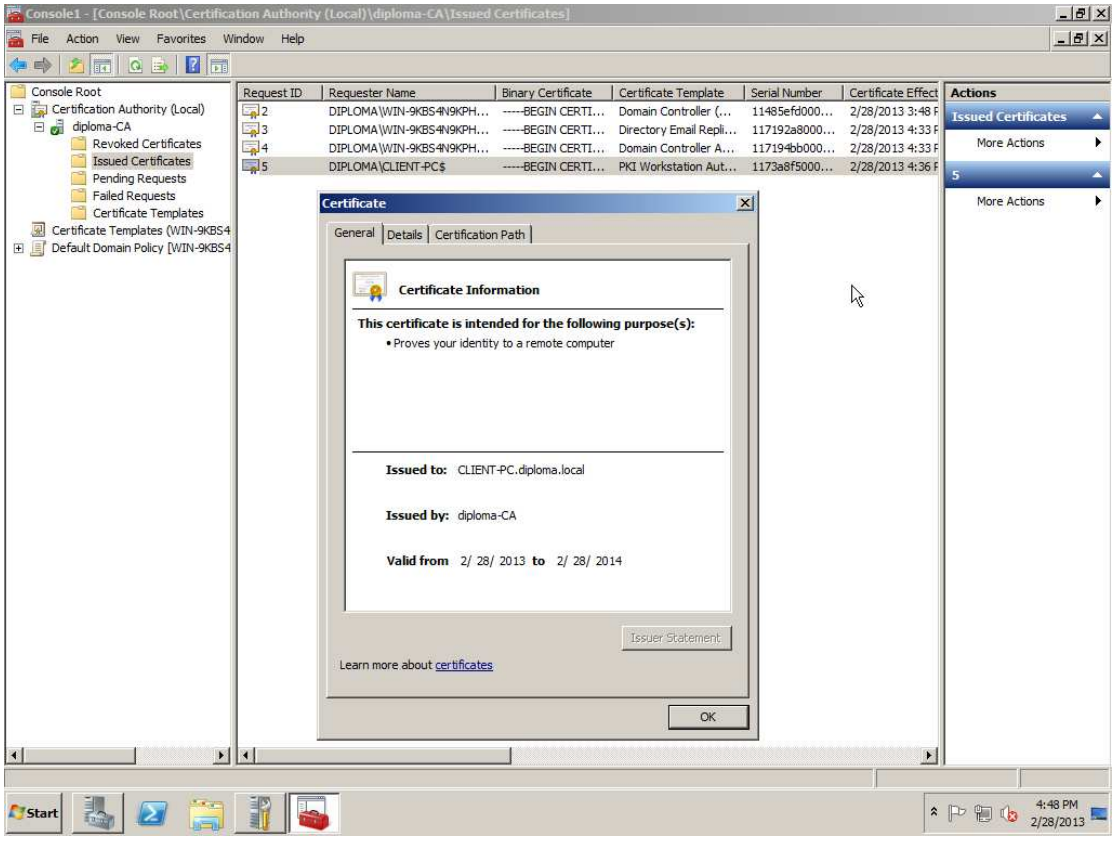
Επιπλέον από το δέντρο στα αριστερά ανοίγουμε τα Default domain policy, Computer configuration, Policies, Windows Settings, Security Settings, Network Access Protection και μετά κάνουμε διπλό κλικ στο EAP Quarantine Enforcement Client.



Στο νέο παράθυρο το ενεργοποιούμε.



Μετά από αυτή τη διαδικασία κάθε φορά που συνδέεται ένας υπολογιστής στο δίκτυο θα εκδίδεται για αυτόν ένα νέο πιστοποιητικό ή θα ανανεώνεται το υπάρχον. Για να λάβουν χώρα οι αλλαγές στον client πρέπει να γίνει επανεκκίνησή του. Μετά από αυτό μπορούμε να δούμε το πιστοποιητικό που δημιουργείται αυτόματα για αυτόν επιλέγοντας το Certificate Authority, diploma-CA, Issued Certificates.

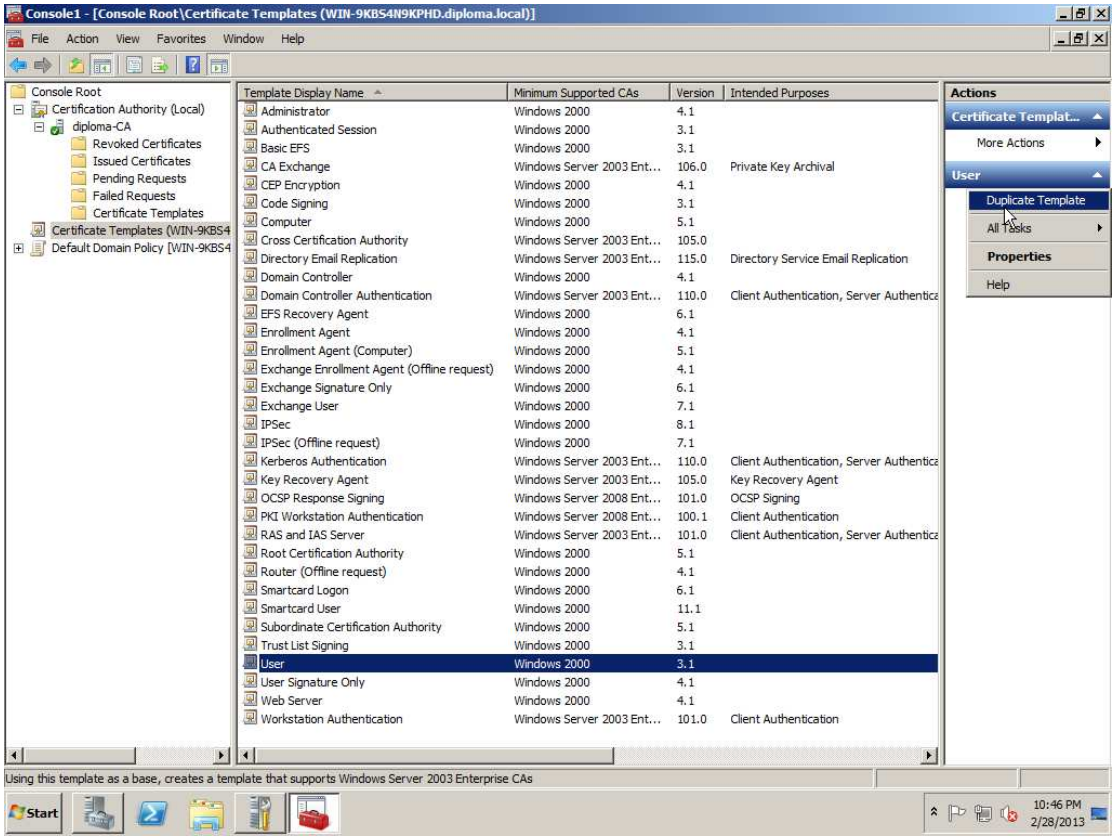


5.9 Δημιουργία πιστοποιητικών για τους χρήστες

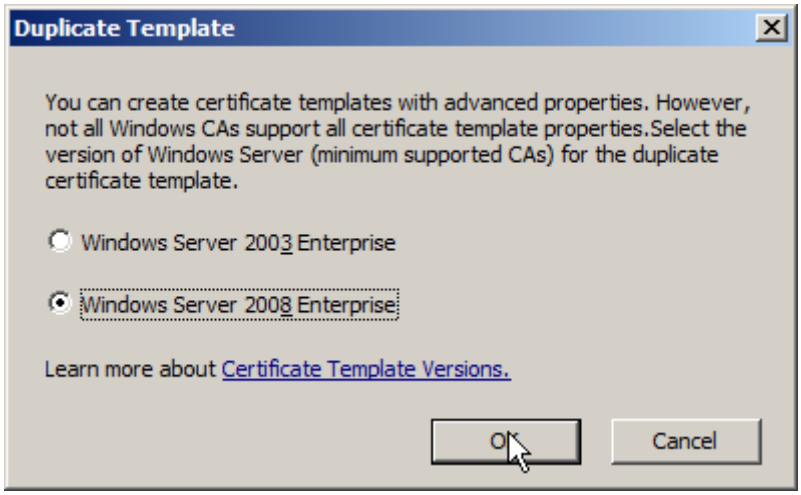
Όπως και για τους υπολογιστές του δικτύου η χειροκίνητη δημιουργία πιστοποιητικών για κάθε χρήστη δεν είναι πρακτική. Έτσι θα ρυθμίσουμε τον server να εκδίδει αυτόματα πιστοποιητικά για κάθε χρήστη που μπαίνει στο σύστημα.

Θα χρησιμοποιήσουμε την κονσόλα mmc της προηγούμενης ενότητας, δηλαδή μία κονσόλα στην οποία εισάγουμε τα snap-in στοιχεία Certificate Authority – Local, Certificate templates και Group Policy Editor – Default domain Policy.

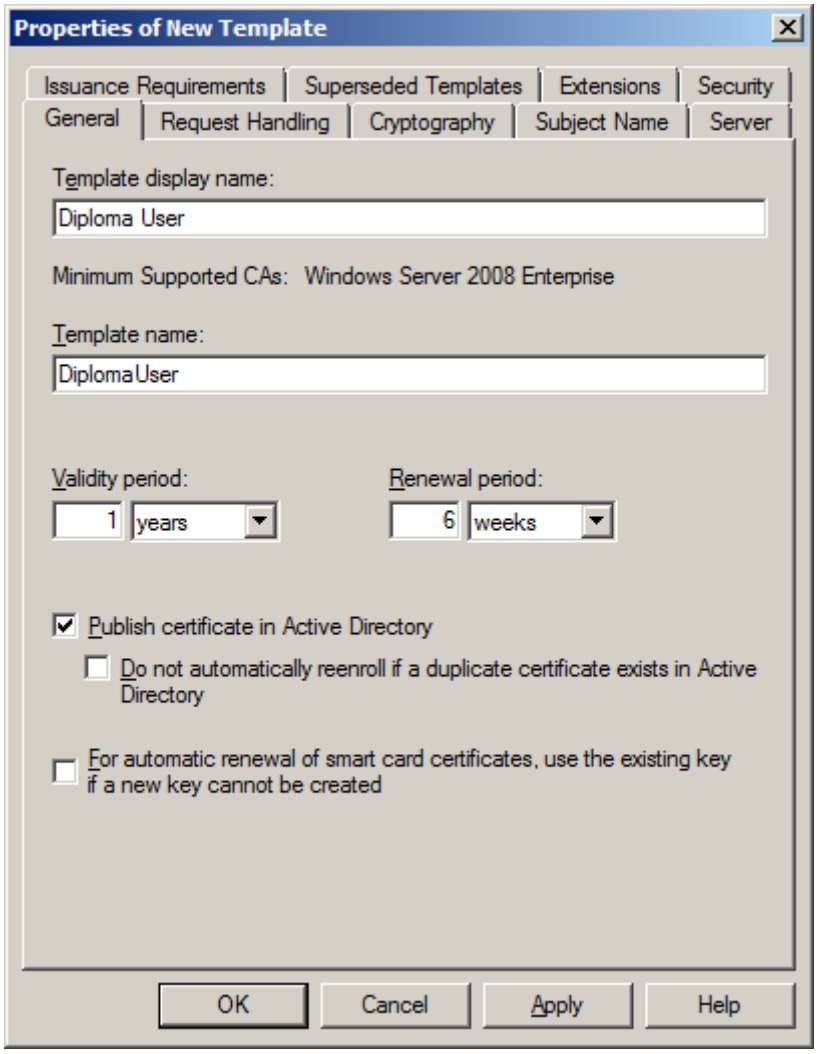
Από το δέντρο στα αριστερά επιλέγουμε Certificate Templates και από την λίστα το User. Έπειτα από το User, More Actions επιλέγουμε το Duplicate Template.



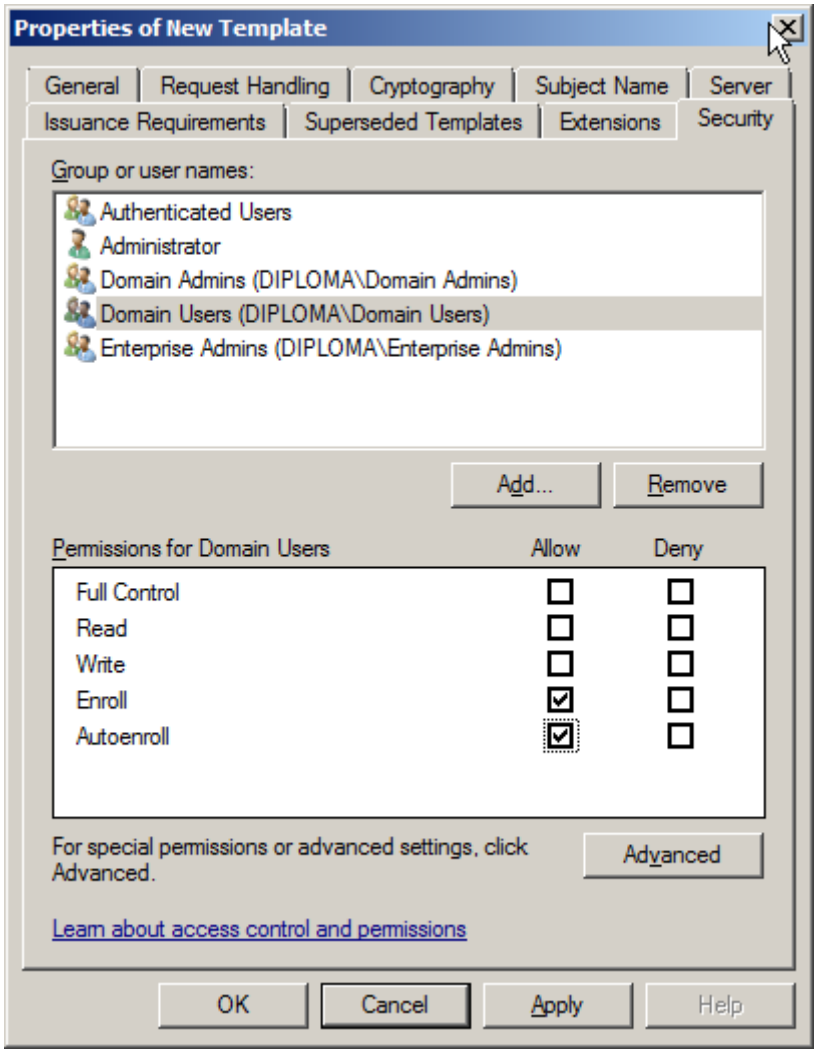
Στο παράθυρο επιλογής έκδοσης επιλέγουμε το Windows Server 2008 Enterprise.



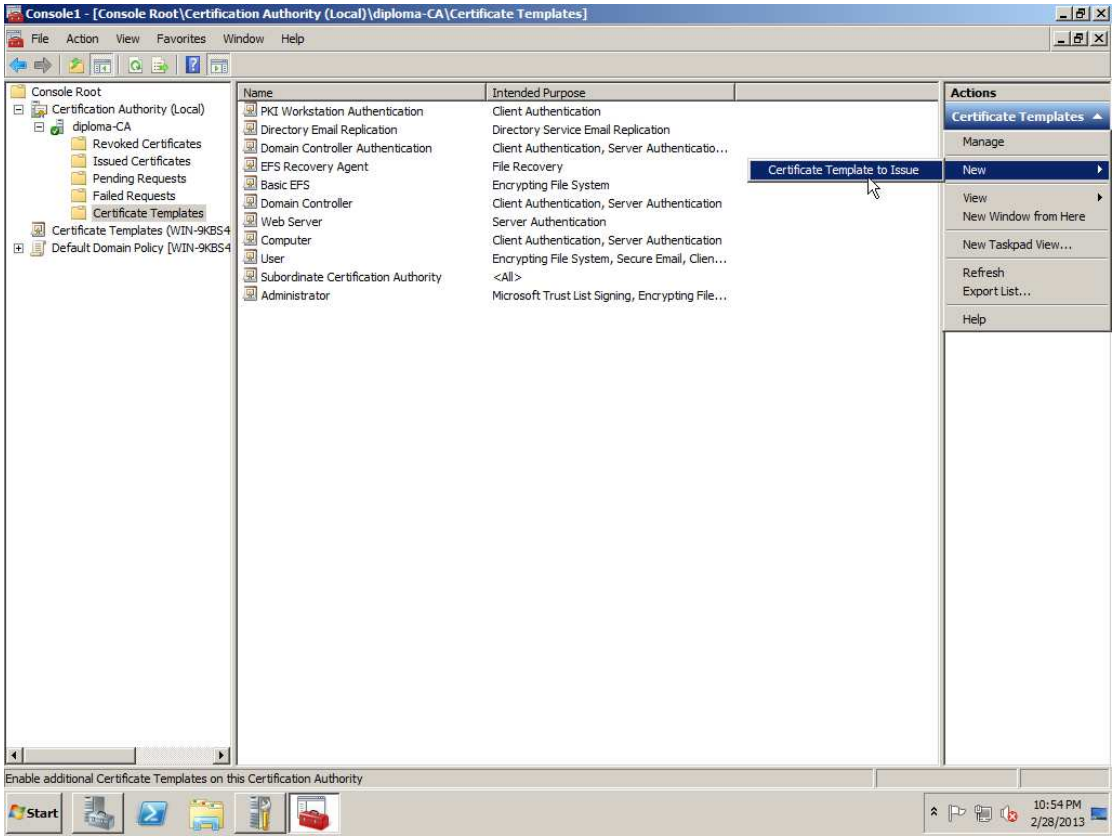
Στις επιλογές του νέου προτύπου αλλάζουμε από την καρτέλα General το όνομα του.



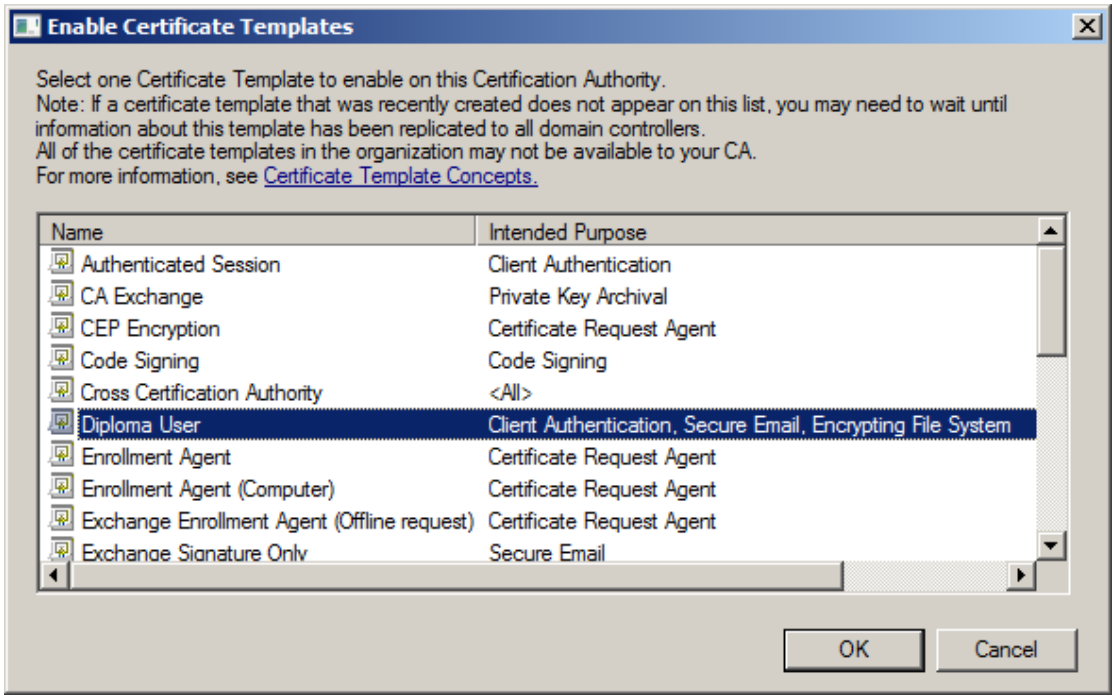
Έπειτα από την καρτέλα Security επιλέγουμε το Domain Users και ενεργοποιούμε το Allow στα Enroll και Autoenroll, και OK για να κλείσει το παράθυρο.



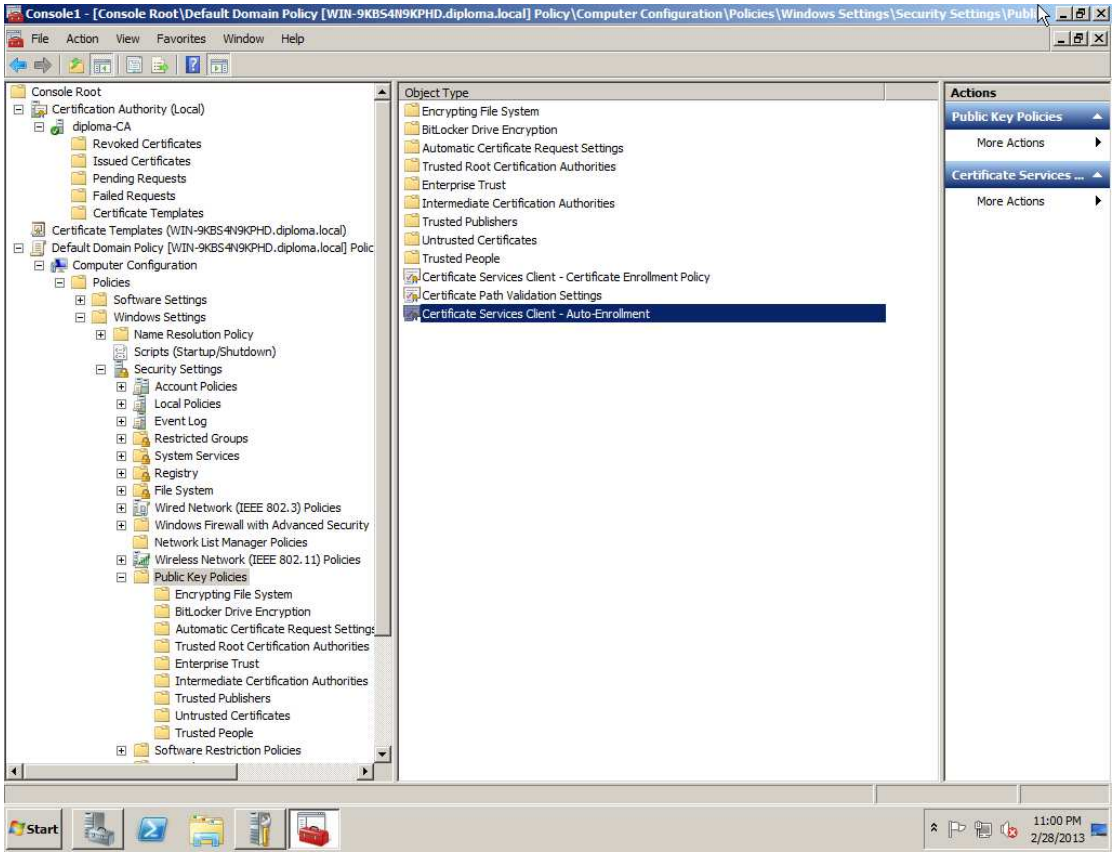
Έπειτα από το δέντρο στην αριστερή στήλη ανοίγουμε τα Certificate Authority, diploma-CA και επιλέγουμε το Certificate Templates. Με αυτό επιλεγμένο επιλέγουμε το More Actions, New την επιλογή Certificate Templates to Issue.



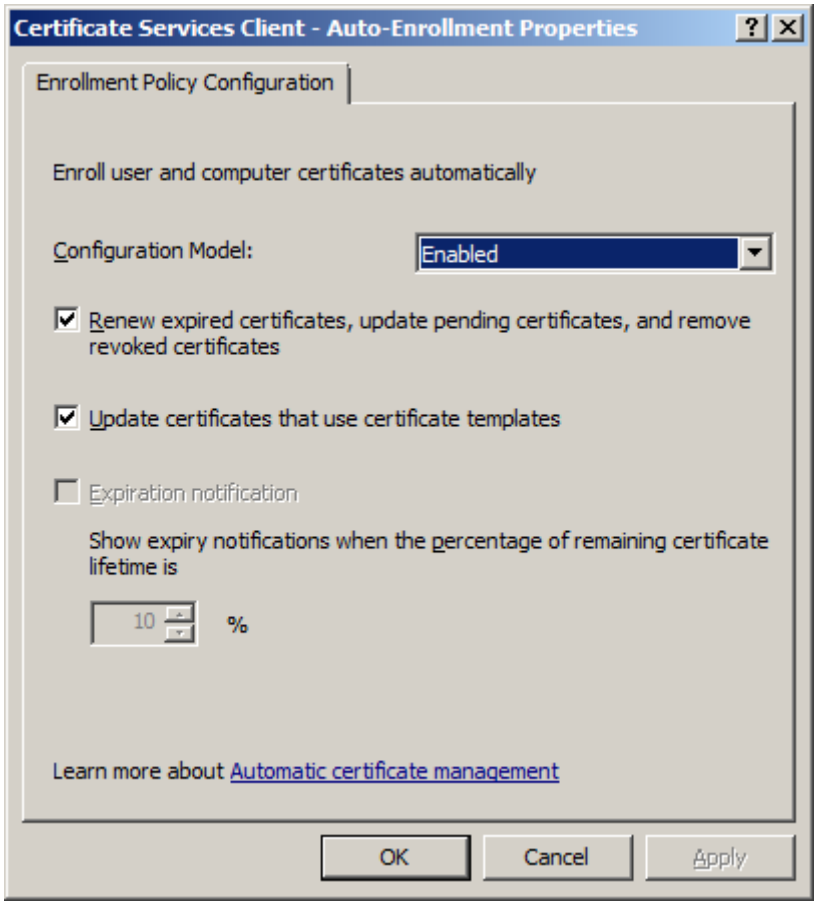
Από το νέο παράθυρο επιλέγουμε το template που δημιουργήσαμε προηγουμένως και πατάμε OK.



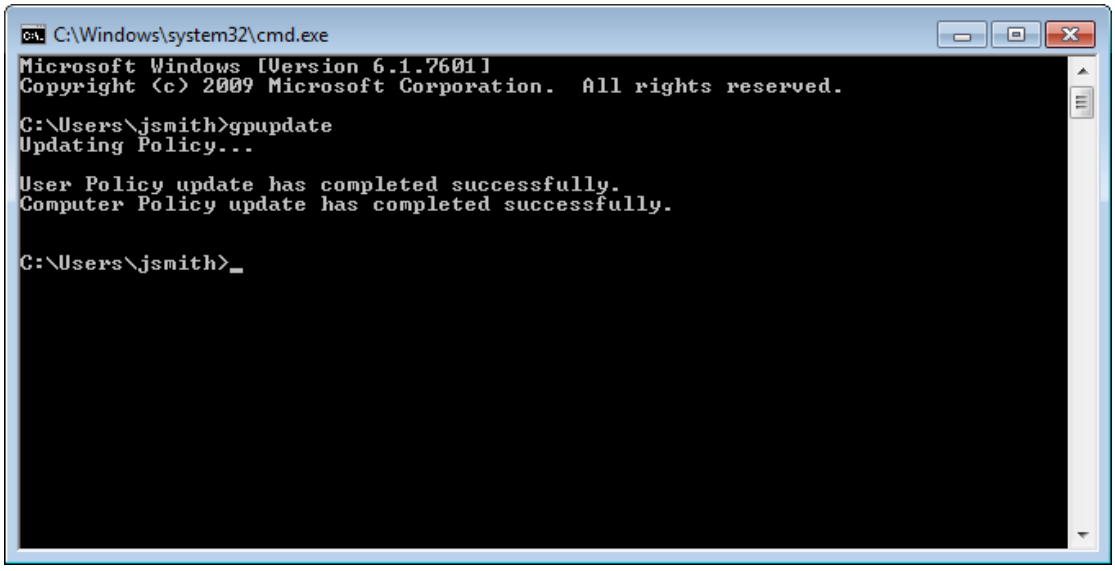
Μετά από το δέντρο στα αριστερά ανοίγουμε τα Default domain policy, User configuration, Policies, Windows Settings, Security Settings, Public Key Policies και επιλέγουμε το τελευταίο. Κάνουμε διπλό κλικ στο Certificate Services Client – Auto enrollment.



Από το παράθυρο που εμφανίζεται βεβαιωνόμαστε ότι το Configuration model είναι Enabled και οι δύο πρώτες επιλογές επιλεγμένες.



Για να ανανεωθούν οι ρυθμίσεις του client χρειάζεται να ανοίξουμε ένα command prompt και να τρέξουμε την εντολή grupdate.

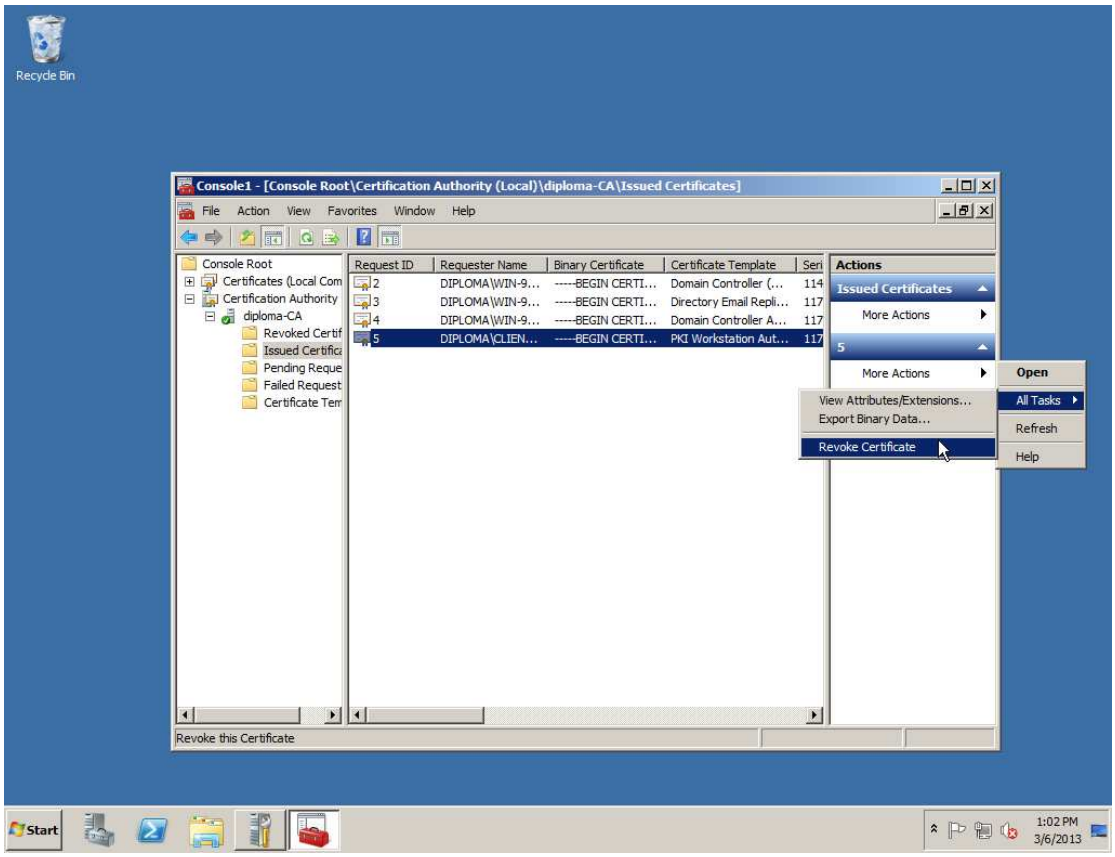


5.10 Ανάκληση πιστοποιητικού

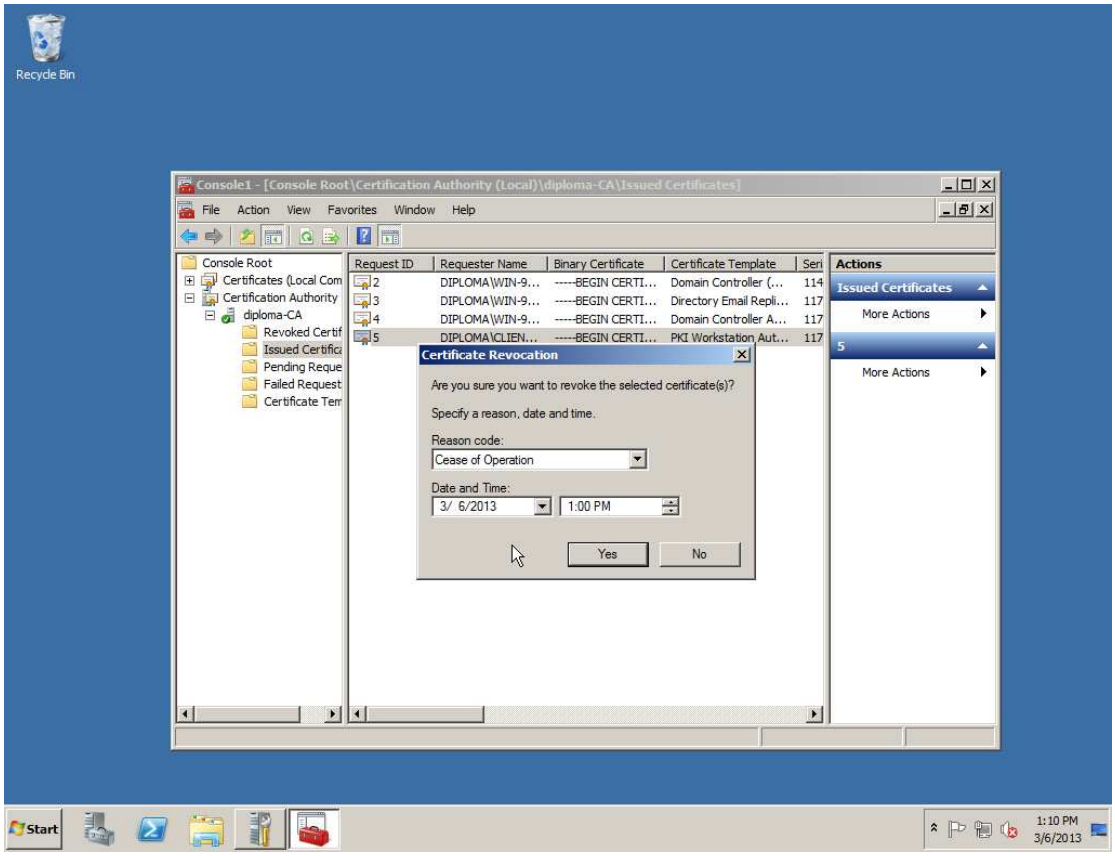
Μία τυπική διαδικασία διαχείρισης πιστοποιητικών είναι η ανάκληση του κλειδιού ενός μηχανήματος, η οποία μπορεί να γίνει σε περίπτωση που το συγκεκριμένο μηχάνημα πάψει να χρησιμοποιείται. Ένας επιτιθέμενος μπορεί να ανακτήσει το παλιότερο πιστοποιητικό και προσπαθήσει να αποκτήσει πρόσβαση με αυτό στο δίκτυο. Γι' αυτό τον

λόγο είναι απαραίτητη η ανάκληση των πιστοποιητικών όλων των μηχανημάτων που αποσύρονται από το δίκτυο.

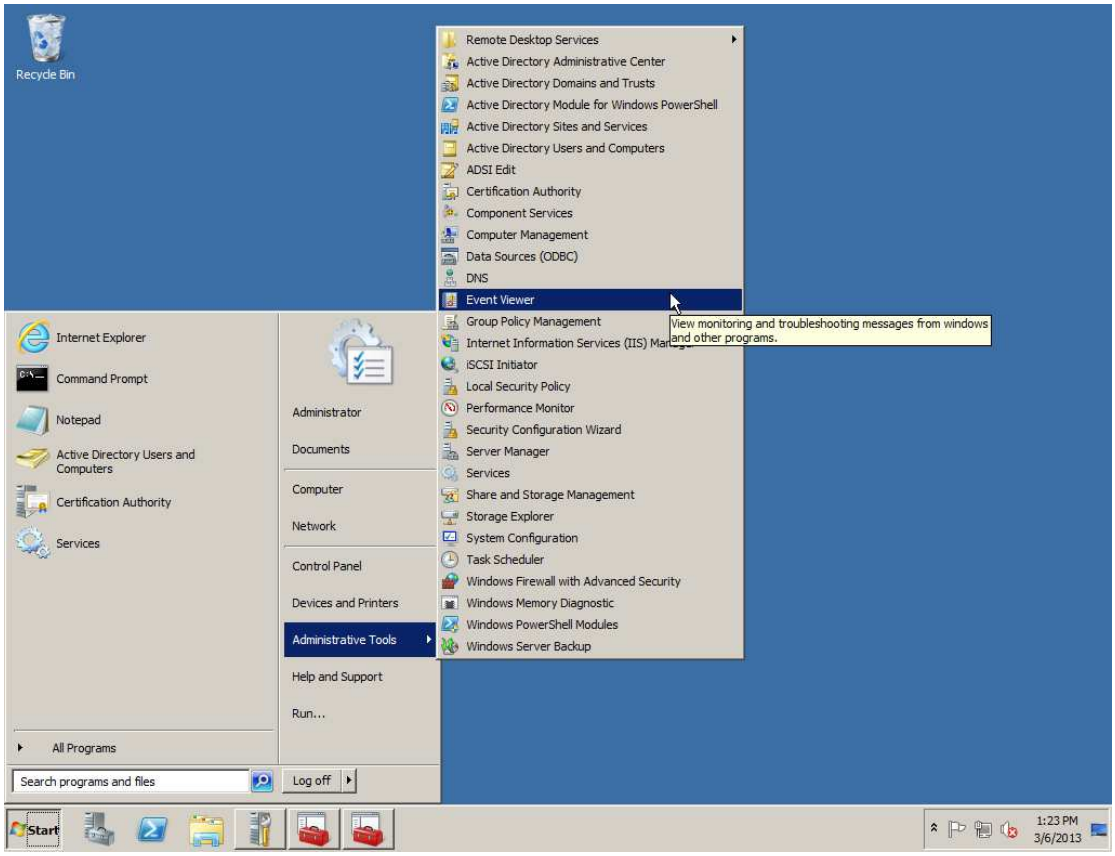
Για να εξομοιώσουμε αυτή τη διαδικασία θα ανακαλέσουμε το πιστοποιητικό του client. Χρησιμοποιούμε, από τον server, το παράθυρο Console που χρησιμοποιήσαμε και στις προηγούμενες διαδικασίες και από τα Issued Certificates επιλέγουμε το πιστοποιητικό ενός μηχανήματος και Revoke Certificate.



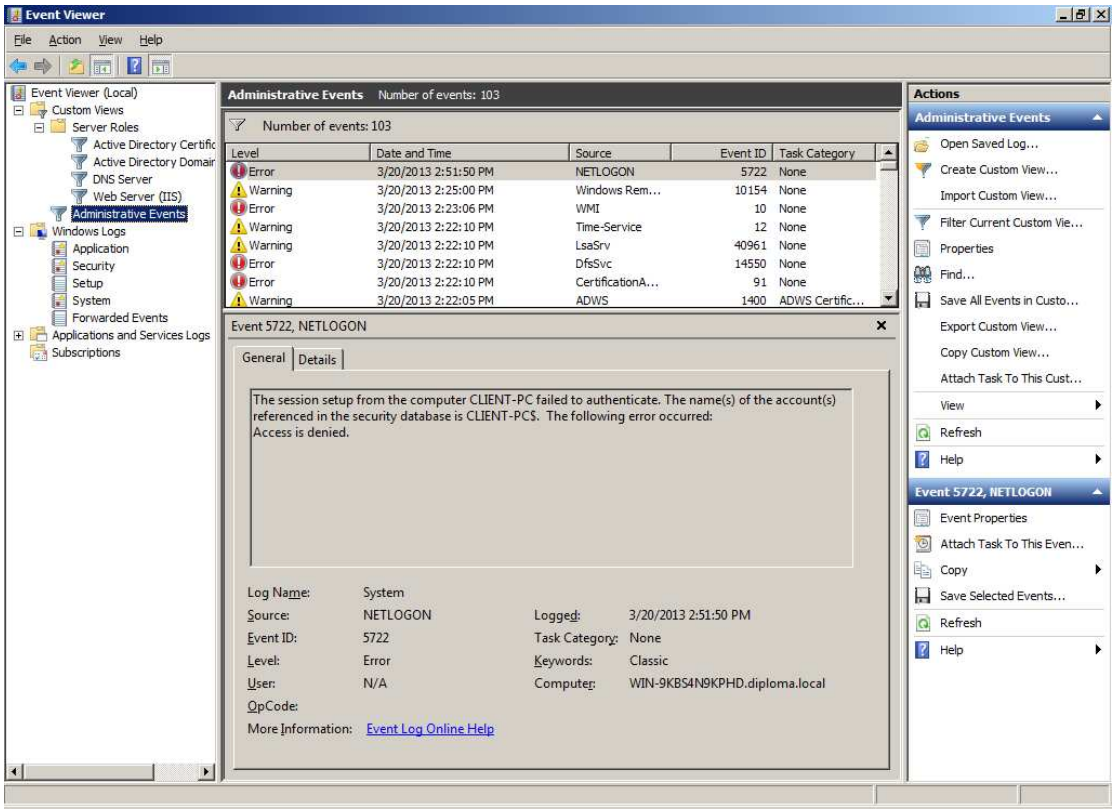
Στο επόμενο παράθυρο εισάγουμε τον λόγο της ανάκλησης και την ημερομηνία που έγινε αυτή.



Έπειτα προσπαθούμε να κάνουμε login με τον client. Ανάλογα με τις ρυθμίσεις στα group policies ο server θα δεχθεί ή θα αρνηθεί την σύνδεση. Για να δούμε το συμβάν χρειάζεται να ανοίξουμε το Event Viewer και να δούμε το συμβάν. Από το μενού Start Administrative Tools και Event Viewer.



Έπειτα από το δέντρο στα αριστερά επιλέγουμε Custom Views, Server Roles και Active Directory Domain Services. Στην λίστα με τα συμβάντα φαίνεται ένα Warning το οποίο προειδοποιεί πως δεν μπορεί να δημιουργηθεί σύνδεση SSL γιατί δεν βρέθηκε το κατάλληλο Certificate.



6 Συμπεράσματα

Η διαδικασία της μελέτης της υποδομής δημόσιου κλειδιού οδήγησε σε μερικές αρκετές ενδιαφέρουσες παρατηρήσεις.

Η κρυπτογράφηση δημόσιου κλειδιού αποτέλεσε ένα σημαντικό βήμα στην επιστήμη της κρυπτογραφίας ανοίγοντας πολλές ενδιαφέροντες δυνατότητες. Η υποδομή δημόσιου κλειδιού είναι η εφαρμογή της με έναν τρόπο που επιτρέπει την συνολική διαχείριση των κλειδιών που δημιουργούνται.

Αρχικά χρειάζεται να τονιστεί η χρησιμότητά της σε ένα δίκτυο. Τα πλεονεκτήματα που υπάρχουν σε επίπεδο ασφαλείας, διαχείρισης και δυνατοτήτων κάνουν μία εγκατάσταση PKI σημαντικό κομμάτι του δικτύου. Με αυτό είναι δυνατόν να πιστοποιούνται με μεγαλύτερη ασφάλεια οι υπολογιστές και οι χρήστες που έχουν πρόσβαση, ενώ προσφέρεται δυνατότητα υπογραφής εγγράφων από τους χρήστες και, σε μεγαλύτερους οργανισμούς, είναι εφικτή η πιστοποίηση δύο συνιστωσών με την χρήση έξυπνων καρτών πρόσβασης.

Η διαδικασία εγκατάστασης σε ένα απλό δίκτυο με διακομιστή Windows Server 2008 που μελετήσαμε παραπάνω δεν περιείχε ιδιαίτερα προβλήματα ούτε ζήταγε σε κάποιο σημείο εξεζητημένες τεχνικές πληροφορίες. Όμως η εξαγωγή αυτού του συμπεράσματος είναι αρκετά βιαστική γιατί δεν λαμβάνεται υπόψη το γεγονός ότι επιλέξαμε ένα απλό σενάριο χρήσης.

Είναι προφανές πως για την εγκατάσταση του PKI είναι απαραίτητη η εξοικείωση με τις βασικές έννοιες της κρυπτογράφησης δημοσίου κλειδιού. Επιπλέον πριν ξεκινήσει η εγκατάσταση χρειάζεται να γίνει ο σχεδιασμός του δικτύου με τέτοιο τρόπο ώστε να καλύπτονται οι τωρινές και οι μελλοντικές ανάγκες τόσο σε επίπεδο ασφαλείας όσο και δυνατοτήτων. Ακόμη χρειάζεται να καθοριστεί με ακρίβεια η πολιτική έκδοσης και ανάκλησης κλειδιών.

Η ίδια η εγκατάσταση, αν και γίνεται με την χρήση πεδίων διαλόγου των Windows δεν είναι τετριμμένη από την άποψη ότι αρχικά χρειάζεται να γίνει η σωστή ρύθμιση του δικτύου και του Active Directory, διαδικασία που περιλαμβάνει την απόδοση διευθύνσεων IP και την ρύθμιση του DNS και του DHCP, αν αυτά χρησιμοποιηθούν.

Όμως το μεγαλύτερο πρόβλημα είναι το πλήθος φαινομενικά απλών επιλογών κατά την διάρκεια της εγκατάστασης που μπορούν να δημιουργήσουν προβλήματα και επιπλοκές στην συνέχεια. Το πιο τυπικό παράδειγμα είναι οι εκδόσεις των κρυπτογραφικών πρωτοκόλλων, που μπορούν να προκαλέσουν ασυμβατότητες με τις διάφορες εκδόσεις των Windows. Ακόμη και στην εγκατάσταση που πραγματοποιήσαμε, η οποία συμπεριλάμβανε μηχανήματα με δυο σύγχρονες εκδόσεις, Windows 7 και Windows Server 2008 συναντήσαμε δυσκολίες.

Παρόλα αυτά με κατάλληλη προετοιμασία, θεωρητική γνώση του αντικειμένου και προσοχή στις λεπτομέρειες είναι δυνατή η σωστή εγκατάσταση ενός δικτύου με υποδομή δημοσίου κλειδιού το οποίο θα παρέχει αυξημένη ασφάλεια και δυνατότητα πιστοποίησης των χρηστών και των συσκευών που συνδέονται σε αυτό.

7 Βιβλιογραφία

Digital Signature Standard. (2000). *Federal Information Processing Standards Publication 186-2*.

Semantic Web and semantic Web services: father and son or. (2006). *Internet Computing, IEEE Volume 10, Issue 2*.

Active Directory. (n.d.). Ανάκτηση από Wikipedia: http://en.wikipedia.org/wiki/Active_Directory

Active Directory Domain Services (Windows). (n.d.). Ανάκτηση από MSDN: http://msdn.microsoft.com/en-us/library/windows/desktop/aa362244%28v=vs.85%29.aspx

Cryptographic hash function. (n.d.). Ανάκτηση από wikipedia.org: http://en.wikipedia.org/wiki/Cryptographic_hash_function

Cryptography. (n.d.). Ανάκτηση από wikipedia.org: http://en.wikipedia.org/wiki/Cryptography

Deploy Client Computer Certificates. (n.d.). Ανάκτηση από TechNet: http://technet.microsoft.com/en-us/library/cc731242.aspx

Encryption. (n.d.). Ανάκτηση από wikipedia.org: http://en.wikipedia.org/wiki/Encryption

Greek Research and Technology Network - Public Key Infrastructure. (n.d.). Ανάκτηση από pki.grnet.gr: http://pki.grnet.gr/help

Hand Ciphers . (n.d.). Ανάκτηση από http://users.telenet.be/d.rijmenants/en/handciphers.htm

Information security. (n.d.). Ανάκτηση από wikipedia.org: http://en.wikipedia.org/wiki/Information_security

Introduction to Cryptography. (n.d.). Ανάκτηση από williamstallings.com: http://williamstallings.com/Extras/Security-Notes/lectures/classical.html

Koblitz, N. (2007, Σεπτέμβριος). The Uneasy Relationship Between Mathematics and Cryptography. *Notices of the AMS*, σσ. 972-979.

Microsoft Product Lifecycle Search. (n.d.). Ανάκτηση από microsoft.org: http://support.microsoft.com/lifecycle/search/default.aspx?sort=PN&alpha=windows+server+2008&Filter=FilterNO

PKI Framework for Supporting the Security of Mobile Communication from its Core. (n.d.). Ανάκτηση από tweenpath.net: http://tweenpath.net/?p=1022

Public-key infrastructure. (n.d.). Ανάκτηση από wikipedia.org: http://en.wikipedia.org/wiki/Public-key_infrastructure

What Are Security Principals? (n.d.). Ανάκτηση από TechNet: http://technet.microsoft.com/en-us/library/cc780957%28WS.10%29.aspx

What are shadow passwords? (n.d.). Ανάκτηση από Indiana University: http://kb.iu.edu/data/aezz.html

Windows Server 2008. (n.d.). Ανάκτηση από wikipedia.org: https://en.wikipedia.org/wiki/Windows_Server_2008

Windows Server 2008 R2. (n.d.). Ανάκτηση από wikipedia.org: https://en.wikipedia.org/wiki/Windows_Server_2008_R2

Windows Server 2012. (n.d.). Ανάκτηση από wikipedia.org: https://en.wikipedia.org/wiki/Windows_Server_2012

(2005). Σημειώσεις για το μάθημα Ασφάλεια Πληροφοριακών Συστημάτων. Στο Δ. Πολέμη.

Συνάρτηση κατατεμαχισμού. (n.d.). Ανάκτηση από wikipedia.org: http://el.wikipedia.org/wiki/%CE%A3%CF%85%CE%BD%CE%AC%CF%81%CF%84%CE%B7%CF%83%CE%B7_%CE%BA%CE%B1%CF%84%CE%B1%CF%84%CE%B5%CE%BC%CE%B1%CF%87%CE%B9%CF%83%CE%BC%CE%BF%CF%8D

Το Πρότυπο Κρυπτογράφησης AES. (n.d.). Ανάκτηση από http://students.ceid.upatras.gr/~mprokala/techarticles/cryptography/AES/aes.htm