ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΛΕΤΗ ΚΑΙ ΥΛΟΠΟΙΗΣΗ ΥΠΟΔΟΜΩΝ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Των

ΒΑΡΛΟΚΩΣΤΑ ΠΑΝΑΓΙΩΤΗ
&
ΧΑΤΖΗΕΥΘΥΜΙΟΥ ΑΛΕΞΑΝΔΡΟΥ

Επιβλέπουσα : Κωνσταντίνου Ελισάβετ , Αναπληρώτρια Καθηγήτρια

Μέλη εξεταστικής επιτροπής: Βλάχου Ακριβή, Αναπληρώτρια Καθηγήτρια,
Δρ. Μπαρμπάτσαλου Κωσταντία

Σάμος, Σεπτέμβριος 2022

Η σελίδα αυτή είναι σκόπιμα λευκή.

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε την καθηγήτρια μας κα. Κωνσταντίνου για την εξαίρετη συνεργασία που είχαμε σε όλη την διάρκεια του Μεταπτυχιακού Προγράμματος και συγκεκριμένα στην Διπλωματική μας εργασία.

Τέλος θερμές ευχαριστίες στις οικογένειες μας και στους φίλους μας για την ψυχολογική στήριξη και την υπομονή που έδειξαν όλο αυτό το διάστημα.

Των
ΒΑΡΛΟΚΩΣΤΑ ΠΑΝΑΓΙΩΤΗ
&
ΧΑΤΖΗΕΥΘΥΜΙΟΥ ΑΛΕΞΑΝΔΡΟΥ
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα Σχημάτων

Ακρωνύμια

ΥΔΚ	Υποδομή Δημοσίου Κλειδιού
PKI	Public key infrastructure
RSA	Rivest - Shamir - Adleman
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ECC	Elliptic-curve cryptography
AES	Advanced Encryption Standard
DES	Data Encryption Standard
NIST	National Institute of Standards and Technology
3DES	Triple DES
SHA	Secure Hash Algorithm
eIDAS	electronic IDentification, Authentication και trust Services
SAML	Security Assertion Markup Language
PGP	Pretty Good Privacy
HSM	Hardware Security Module
PCI DSS	Payment Card Industry Data Security Standard
CA	Certificate Authority
CRL	Certificate Revocation List
RA	Registration Authority
VA	Validation Authority
CPS	Certification Practice Statement
CP	Certificate Policy
ΑΠ	Αρχή Πιστοποίησης

Περίληψη

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure, PKI) είναι ένας συνδυασμός διαδικασιών, λογισμικού και κρυπτογραφικών τεχνολογιών, όπου η κύρια λειτουργία της είναι η πιστοποίηση της εγκυρότητας όλων των μελών που εμπλέκονται σε μια ψηφιακή συναλλαγή.

Στη συγκεκριμένη διπλωματική εργασία πραγματοποιείται μελέτη και υλοποίηση Υποδομών Δημοσίου Κλειδιού πάνω στον τομέα έκδοσης, παραγωγής και χρήσης των ψηφιακών πιστοποιητικών για την εφαρμογή απομακρυσμένης ψηφιακής υπογραφής τόσο σε έγγραφα όσο και σε προγράμματα αποστολής και λήψης ηλεκτρονικών μηνυμάτων τα οποία βασίζονται στις αρχές της επιστήμης της Κρυπτογραφίας.

Επιπλέον μέσω της τεχνικής υλοποίησης στοχεύει στην διάδοση της τεχνικής γνώσης ώστε απλοί χρήστες ή οργανισμοί να μπορέσουν να ασχοληθούν και να αξιοποιήσουν την μελέτη της υποδομής και τα οφέλη των υπηρεσιών που προσφέρει.

Για την υλοποίηση της υποδομής χρησιμοποιήθηκαν δύο εμπορικές πλατφόρμες κατασκευής Υποδομών Δημόσιου Κλειδιού στις οποίες παρουσιάζονται αναλυτικά οι δυνατότητες , οι απαιτήσεις και οι παραμετροποιήσεις που χρειάζονται προκειμένου να διασφαλιστεί η ομαλή και παραγωγική λειτουργία τους.

Λέξεις Κλειδιά: *Υποδομή Δημοσίου Κλειδιού , πιστοποιητικά , ψηφιακές υπογραφές , κρυπτογραφία*

Abstract

Public Key Infrastructure (PKI) is a combination of processes, software and cryptographic technologies, where its main function is to authenticate the validity of all members involved in a digital transaction.

In this thesis, a study and implementation of Public Key Infrastructures on the field of issuing, producing and using digital certificates is carried out for the application of remote digital signatures both in documents and in programs for sending and receiving electronic messages, which are based on the principles of the science of Cryptography.

In addition, through the technical implementation, it aims to disseminate technical knowledge so that ordinary users or organizations can engage and exploit the study of the Infrastructure and the benefits of the services it offers.

For the implementation of the infrastructure, two commercial platforms for the construction of Public Key Infrastructures were used in which the capabilities, requirements and configurations needed to ensure their smooth and productive operation are presented in detail.

Keywords: *Public Key Infrastructure, certificates, digital signatures, cryptography*

1

Εισαγωγή

1.1 Εισαγωγή στην Υποδομή Δημοσίου Κλειδιού

Παρόλο που στις μέρες μας έχει αναπτυχθεί πληθώρα πρωτοκόλλων και μηχανισμών για την εξέταση ζητημάτων ασφαλείας των πληροφοριών που μεταβιβάζονται σε ένα ευρύ δίκτυο, παραμένει επιτακτική η ανάγκη για προστασία των δεδομένων, καθώς και για ασφαλή ηλεκτρονική επικοινωνία, η οποία καθίσταται απαραίτητη λόγω της ραγδαίας αύξησης των ηλεκτρονικών συναλλαγών στο διαδίκτυο. Για τους παραπάνω λόγους, δημιουργήθηκε η Υποδομή Δημοσίου Κλειδιού και η χρήση ψηφιακών πιστοποιητικών.

Ως Υποδομή Δημοσίου Κλειδιού (PKI- Public Key Infrastructure), ορίζεται ένας συνδυασμός προγραμμάτων, τεχνολογιών κρυπτογράφησης, διαδικασιών και υπηρεσιών που χρησιμοποιούνται για τη δημιουργία των ψηφιακών πιστοποιητικών, καθώς και για τη διαχείρηση, τη διανομή αλλά και την ανάκληση αυτών. Αναλυτικότερα, κάθε χρήστης, ο οποίος κατέχει ένα συγκεκριμένο ρόλο και μια μοναδική ταυτότητα, αντιστοιχίζεται με ένα δημόσιο κλειδί. Οι πόροι του δικτύου, στους οποίους κάθε χρήστης δύναται να έχει πρόσβαση, καθορίζονται από το ρόλο του, ενώ ως ταυτότητα θεωρείται το φυσικό πρόσωπο στο οποίο αντιστοιχεί ένα κλειδί. Κάθε χρήστης, ο οποίος αποτελεί συνδυασμό των δυο παραπάνω, έχει τη δυνατότητα απόκτησης ενός και μοναδικού πιστοποιητικού, το οποίο επιβεβαιώνει ότι του αντιστοιχεί ένα συγκεκριμένο δημόσιο κλειδί.

Ένα Σύστημα Υποδομής Δημοσίου Κλειδιού απαρτίζεται από τα εξής:

- Αρχή Πιστοποιητικών (CA- Certificate Authority), η οποία αποτελεί τον αξιόπιστο τρίτο υπεύθυνο για την επικύρωση μιας ταυτότητας

- Αρχή Καταχώρησης (RA- Registration Authority), η οποία αποτελεί στοιχείο ενός PKI υπεύθυνου για την αποδοχή αιτημάτων ψηφιακών πιστοποιητικών και την εξακρίβωση της ταυτότητας του ατόμου ή του οργανισμού που έχει υποβάλλει αίτημα.
- Αρχή Επιβεβαίωσης (VA- Validation Authority), η οποία παρέχει προαιρετικά στην Αρχή Πιστοποιητικών περαιτέρω πληροφορίες για την επιβεβαίωση της μοναδικής ταυτότητας του χρήστη
- Ασφαλή Κεντρικός Κατάλογος Πιστοποιητικών, στον οποίο αποθηκεύονται τα κλειδιά των χρηστών.

Ο κύριος ρόλος της Υποδομής Δημοσίου Κλειδιού είναι η συμβολή της στην αυθεντικοποίηση με την ενίσχυση της εμπιστοσύνης των συμβαλλόμενων μερών και στην εμπιστευτικότητα με την εξασφάλιση ότι οι ιδιωτικές πληροφορίες των χρηστών μεταβιβάζονται με ασφάλεια στο διαδίκτυο. Για την επίτευξη των παραπάνω στόχων, χρησιμοποιείται πληθώρα εργαλείων και τεχνικών τα οποία βασίζονται στη κρυπτογραφία.

1.2 Στόχος της Διπλωματικής Εργασίας

Στόχος της διπλωματικής εργασίας είναι να παρέχει μια συνολική αποτύπωση των μέχρι τώρα δεδομένων σε θεωρητικό και σε τεχνικό επίπεδο των σύγχρονων κανονιστικών και τεχνικών υποδομών που αφορούν τα ψηφιακά πιστοποιητικά και την βαρύτητα της χρήσης τους στην σύγχρονη καθημερινότητα.

Είναι γεγονός ότι τα τελευταία χρόνια υπάρχει ραγδαία αύξηση των ηλεκτρονικών συναλλαγών, όπως η είσοδος σε ένα ασφαλές δίκτυο, η αποστολή ηλεκτρονικών εγγράφων, οι ηλεκτρονικές πληρωμές αγαθών σε τρίτες οντότητες όπως κρατικές ή ιδιωτικές υπηρεσίες, έχουν καταστήσει επίκαιρα θέματα αναφορικά με την ασφάλεια και τις τεχνολογίες που πρέπει να εφαρμοστούν.

Επίσης ένας από τους σκοπούς είναι να διασφαλιστεί η ακεραιότητα και η αυθεντικότητα τέτοιων συναλλαγών μέσω της χρήσης ψηφιακών πιστοποιητικών που έχουν εκδοθεί από μια έμπιστη υποδομή δημοσίου κλειδιού.

Η Υποδομή Δημοσίου Κλειδιού (ΥΔΚ) είναι σε θέση να δημιουργήσει ένα «τεχνολογικό οικοσύστημα εμπιστοσύνης» με βάση την ικανοποίηση των απαιτήσεων ασφαλείας, θέτοντας ως στόχο την παροχή υπηρεσιών, πάντα με την εφαρμογή της «ασύμμετρης κρυπτογραφίας».

Η ΥΔΚ δύναται να διαχειρίζεται τον κύκλο ζωής των ψηφιακών πιστοποιητικών που εκδίδονται από την ίδια. Είναι μία ολοκληρωμένη και εφαρμοσμένη τεχνολογία, η οποία με την ανάπτυξη κάθε νέου ολοκληρωμένου πληροφοριακού συστήματος, διαδικτυακής υπηρεσίας ή εφαρμογής λογισμικού, αποτελεί θεμέλιο για την ασφάλεια των πληροφοριών.

Ως εκ τούτου, συμβάλει στην θωράκιση των επιχειρησιακών διαδικασιών, στην συμμόρφωση κανονιστικών πολιτικών ασφαλείας, καθώς και στην εκπλήρωση των στόχων του εκάστοτε οργανισμού.

1.3 Συνεισφορά και Δομή της Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία συνεισφέρει στην κατανόηση εφ'όλης της ύλης του τομέα έκδοσης, παραγωγής και χρήσης των ψηφιακών πιστοποιητικών βασιζόμενη στις αρχές της επιστήμης της Κρυπτογραφίας.

Επιπλέον μέσω των τεχνικών σεναρίων στοχεύει στην διάδοση της τεχνικής κατάρτισης, ώστε απλοί χρήστες ή οργανισμοί να μπορέσουν να ασχοληθούν και να αξιοποιήσουν την μελέτη της Υποδομή Δημόσιου Κλειδιού και τα

οφέλη των υπηρεσιών που προσφέρει . Η χρήση αυτών των υπηρεσιών μπορεί να διασφαλίσει την ακεραιότητα και την εμπιστευτικότητα των πληροφοριών τους, πράγμα που το καθιστά σημαντικό παράγοντα προσθήκης στην καθημερινή λειτουργία των διαδικασιών.

Επίσης προσφέρει τεχνική γνώση σε δύο εμπορικές πλατφόρμες κατασκευής Υποδομών Δημόσιου Κλειδιού η οποία είναι περιορισμένη ή μη κατανοητή ως προς την εγκατάσταση και την δημιουργία όλης της υποδομής.

Σκοπός της διπλωματικής εργασίας είναι να διευκρινισθούν οι παράμετροι που καθορίζουν την επιτυχία για την λειτουργία και ανάπτυξη μίας υποδομής για την δημιουργία, παραγωγή ψηφιακών πιστοποιητικών τόσο για υπογραφή μηνυμάτων ηλεκτρονικής αλληλογραφίας όσο και για την υπογραφή εγγραφών τελικών χρηστών.

Επίσης αναπτύσσεται ένα ολοκληρωμένο εικονικό εργαστηριακό περιβάλλον δύο διαφορετικών υποδομών, το οποίο στοχεύει στην μελέτη περίπτωσης σχετικά με τον σχεδιασμό και την λειτουργικότητα μίας υποδομής δημοσίου κλειδιού.

Για να επιτευχθούν οι ανωτέρω στόχοι, η μέθοδος που εφαρμόστηκε είναι η βιβλιογραφική ανασκόπηση τόσο από ακαδημαϊκές όσο και επιχειρησιακές πηγές. Στην συνέχεια αναλύθηκε το επιχειρησιακό και παραγωγικό μοντέλο ανάπτυξης και λειτουργίας μίας ΥΔΚ, για τη διαχείριση του κύκλου ζωής των ψηφιακών πιστοποιητικών χρησιμοποιώντας δύο διαφορετικά εμπορικά λογισμικά.

Αναλυτικότερα, στα πρώτα κεφάλαια παρουσιάζεται μία σύντομη εισαγωγή στο μαθηματικό υπόβαθρο και την θεωρητική δομή για την κρυπτογραφία και τις βασικές αρχές που απαρτίζουν τα συστήματα Δημοσίου κλειδιού .

Στο τρίτο κεφάλαιο παρουσιάζονται τα είδη κρυπτογράφησης σχετικά με την συμμετρική και ασύμμετρή κρυπτογραφία και κατ' επέκταση οι συναρτήσεις κατακερματισμού. Η θεωρητική δομή των σχημάτων ψηφιακών υπογραφών τεκμηριώνεται αναλυτικά στο τέταρτο κεφάλαιο, βασιζόμενο στο μαθηματικό υπόβαθρο των προηγούμενων κεφαλαίων .

Στο πέμπτο κεφάλαιο αναλύονται τα ψηφιακά πιστοποιητικά και τα μέσα αποθήκευσης τους , ο ρόλος τους και οι απαιτήσεις έκδοσής τους, ενώ στο έκτο κεφάλαιο περιγράφεται λεπτομερειακά το θεωρητικό υπόβαθρο της υποδομής δημοσίου κλειδιού.

Επιπροσθέτως, στο έβδομο κεφάλαιο περιγράφεται η υλοποίηση των τεχνικών σεναρίων, με την εγκατάσταση ενός ολοκληρωμένου εικονικού εργαστηριακού περιβάλλοντος δύο εμπορικών λογισμικών για την παραγωγή και χρήση των ψηφιακών πιστοποιητικών με την χρήση αλγόριθμων κρυπτογράφησης ελλειπτικής καμπύλης .

Καταλήγοντας στο όγδοο κεφάλαιο αναγράφονται τα συμπεράσματα της μελέτης και της υλοποίησης της παρούσας εργασίας.

2

Εισαγωγικές έννοιες

2.1 Βασικές Αρχές Θεωρίας Ελλειπτικών Καμπύλων

2.1.1 Ελλειπτικές Καμπύλες

Τα κρυπτοσυστήματα ελλειπτικών καμπυλών δεν αποτελούν καινούργια κρυπτοσυστήματα. Οι ελλειπτικές καμπύλες είναι ένα μαθηματικό εργαλείο το οποίο χρησιμοποιείται τα τελευταία χρόνια για την δημιουργία γνωστών κρυπτο συστημάτων δημόσιου κλειδιού. Αρχικά προτάθηκε η εφαρμογή τους στην κρυπτογραφία από τους Miller το 1986 και Koblitz το 1987 (Menezes, et al., 2004).

Οι ελλειπτικές καμπύλες ορίζονται σε πολλαπλά σώματα, όπως στο σώμα των μιγαδικών, των πραγματικών. Πιο συγκεκριμένα στην κρυπτογραφία, οι ελλειπτικές καμπύλες ορίζονται σε πεπερασμένα σώματα.

2.1.2 Οι ελλειπτικές καμπύλες ορισμένες modulo p

Η παρουσίαση των ελλειπτικών καμπυλών στο σώμα των πραγματικών αριθμών, είχε ως σκοπό τη γραφική απεικόνιση των καμπυλών, και την παρουσίαση των εξισώσεων της πρόσθεσης σημείων της καμπύλης. Οι ελλειπτικές καμπύλες οπού έχουν κρυπτογραφικό ενδιαφέρον είναι ορισμένες στο σώμα Z_p, όπου p είναι πρώτος και $p > 3$. Η πράξη της πρόσθεσης είναι επίσης εσωτερική στο Z_p, και μπορεί να οριστεί με τον ίδιο τρόπο (Κάτος & Στεφανίδης, 2003). Μας ενδιαφέρει επίσης η ελλειπτική καμπύλη να έχει τρεις διακριτές ρίζες (για $y = 0$), ώστε να καταλήξουμε στον ακόλουθο ορισμό:

ΟΡΙΣΜΟΣ : Η ελλειπτική καμπύλη που είναι ορισμένη στο Z_p, για κάποιον πρώτο ακέραιο $p > 3$, είναι το σύνολο των στοιχείων $(x, y) \in Z_p \times Z_p$ τα οποία ικανοποιούν την εξίσωση:

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

όπου

$$a,b \in Zp$$

και

$$4a^3 + 27b^2 \ 0 \pmod{p}$$

Η πρόσθεση δύο σημείων της ελλειπτικής καμπύλης στο *Zp* ορίζεται με τον ίδιο τρόπο όπως και στους πραγματικούς αριθμούς. Έστω δύο σημεία $P = (x_1, y_1)$ και $Q = (x_2, y_2)$, της ελλειπτικής καμπύλης $y^2 \equiv x^3 + ax + b \pmod{p}$.

Το σημείο $P + Q = (x_3, y_3)$ το οποίο είναι επίσης σημείο της καμπύλης, θα έχει συντεταγμένες:

$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod{p}$$

και

$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod{p}$$

όπου:

$$\lambda \equiv \begin{cases} \dfrac{(y_2 - y_1)}{(x_2 - x_1)} \pmod{p}, & \text{εάν } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} \pmod{p}, & \text{εάν } P = Q \end{cases}$$

Άλλη μια ιδιότητα στις ελλειπτικές καμπύλες στο ***Zp***, είναι ότι τα σημεία της , μαζί με το σημείο **O** ορίζουν κυκλική υποομάδα. Αυτό σημαίνει ότι οποιοδήποτε σημείο ανήκει στην ελλειπτική καμπύλη εκτός του **O,** είναι γεννήτορας αυτής (Κάτος & Στεφανίδης, 2003). Δηλαδή, εάν δοθεί κάποιο σημείο P της καμπύλης, η διαδοχική πρόσθεση του P στον εαυτό του, θα διατρέξει όλα τα σημεία της καμπύλης. Αν η καμπύλη αποτελείται από *n* σημεία, τότε θα είναι:

2P = P + P = Q

3P = P + 2P = R

…

nP = **O** ,

(n +1)P = P.

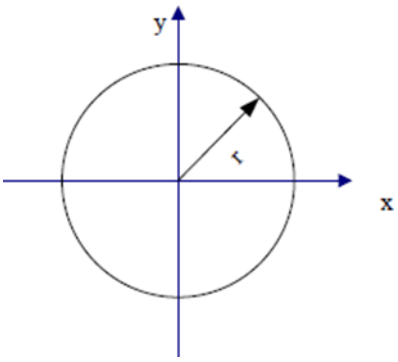
2.1.3 Ελλειπτικές καμπύλες στο σώμα των πραγματικών αριθμών

Αντίθετα από την αίσθηση που μας δημιουργεί ο όρος «καμπύλη», μια ελλειπτική καμπύλη στην πραγματικότητα μπορεί να αποτελείται από δύο καμπύλες και ένα σημείο που βρίσκεται εκτός των καμπυλών.

Ξεκινώντας από την εξίσωση του κύκλου, θα προσθέσουμε διαδοχικά όρους έως ότου καταλήξουμε στην εξίσωση της ελλειπτικής καμπύλης. Είναι γνωστό από την Αναλυτική Γεωμετρία, ένας κύκλος με κέντρο O(0, 0) ορίζεται από την εξίσωση:

$x^2 + y^2 = r^2$

όπου r η ακτίνα του κύκλου. Αν απεικονίσουμε όλα τα σημεία (x, y) ενός επιπέδου που ικανοποιούν την εξίσωση του κύκλου, τότε θα λάβουμε την κυκλική καμπύλη όπως εμφανίζεται στο παρακάτω σχήμα:

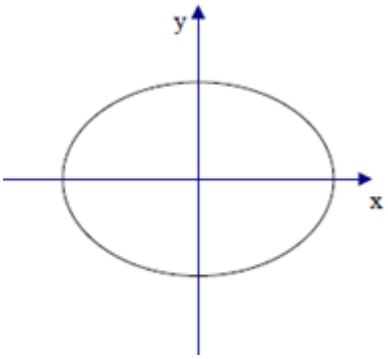


Σχήμα 1: $x^2 + y^2 = r^2$ στους πραγματικούς αριθμούς

Ο κύκλος είναι ειδική περίπτωση έλλειψης, όπου a = b:

$ax^2 + by^2 = c$

Οι τιμές που ικανοποιούν την εξίσωση έλλειψης για δοσμένα a και b σχηματίζουν την καμπύλη του παρακάτω σχήματος:



Σχήμα 2: $ax^2 + by^2 = c$ στους πραγματικούς αριθμούς

Τόσο στην εξίσωση κύκλου, όσο και στην εξίσωση έλλειψης, οι μεταβλητές συνδέονται με εξισώσεις δευτέρου βαθμού. Σαν αποτέλεσμα ότι σε μια δοσμένη τιμή του x να αντιστοιχούν δύο τιμές για το y, και αντίστροφα. Δοσμένα για διαφορετικά σημεία (x_1, y_1) και (x_2, y_2) της έλλειψης μπορεί να ορισθεί ευθεία η οποία διαπερνά από τα σημεία αυτά.

Η ευθεία θα τέμνει την έλλειψη μόνον σε αυτά τα δύο σημεία.

Στην περίπτωση της ελλειπτικής καμπύλης, η εξίσωση της καμπύλης είναι δευτέρου βαθμού ως προς y αλλά τρίτου βαθμού ως προς x.

Η εξίσωση της ελλειπτικής καμπύλης δίνεται από τη σχέση:

$y^2 = x^3 + ax + b,$

για σταθερές a και b. Θεωρούμε δύο διαφορετικά σημεία (x_1, y_1) και (x_2, y_2) της ελλειπτικής καμπύλης, και έστω η ευθεία:

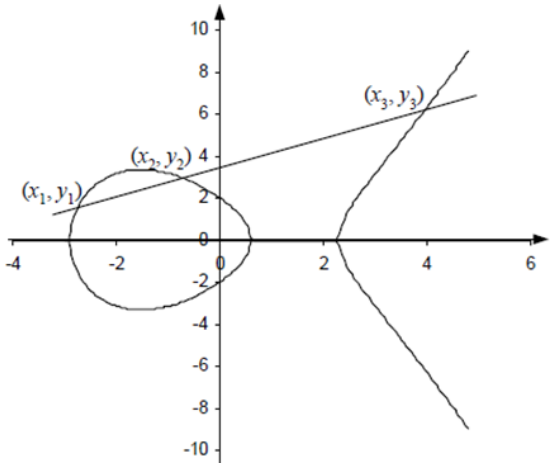
$y = \lambda x + c$

η οποία τέμνει την ελλειπτική καμπύλη στα σημεία αυτά. Αντικαθιστώντας την εξίσωση της ευθείας στην ελλειπτική καμπύλη, θα είναι:

$(\lambda x+c)^2 = x^3 + ax + b,$

η οποία είναι τρίτου βαθμού εξίσωση με δύο από τις ρίζες τα x_1 και x_2. Υπάρχει όμως και η τρίτη ρίζα x_3, που αντιστοιχεί στο σημείο της ευθείας $(x_3, \lambda x_3 + c)$. Συνεπώς η ευθεία τέμνει στην καμπύλη σε τρία σημεία.

Στο επόμενο σχήμα εμφανίζεται μια ελλειπτική καμπύλη και η ευθεία που τέμνει την καμπύλη σε τρία σημεία. Η ελλειπτική καμπύλη αποτελείται από τις καμπύλες του σχήματος και επιπλέον από ένα σημείου Ο που το ονομάζουμε «σημείο στο άπειρο» (point at infinity) (Κάτος & Στεφανίδης, 2003).

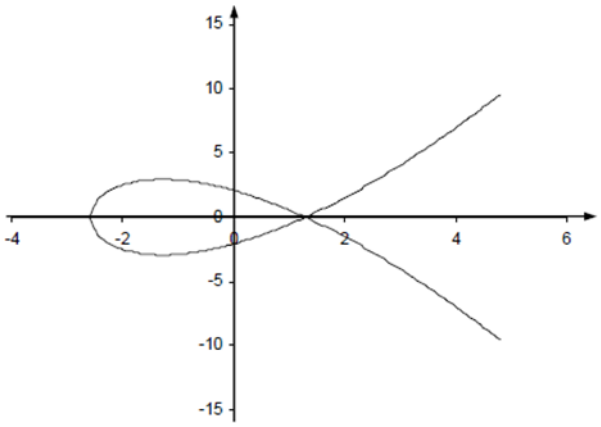


Σχήμα 3: Η ελλειπτική καμπύλη $y^2 = x^3 - 7x + 4$

Για κάποιον συνδυασμό των a και b, η εξίσωση της ελλειπτικής καμπύλης δεν έχει τρεις διαφορετικές ρίζες (για y = 0). Αυτό συμβαίνει όταν:

$4a^3 + 27b^2 = 0$

και η ελλειπτική καμπύλη είναι της μορφής του σχήματος που απεικονίζεται παρακάτω . Μια τέτοια ελλειπτική καμπύλη ονομάζεται ιδιάζουσα (singular).

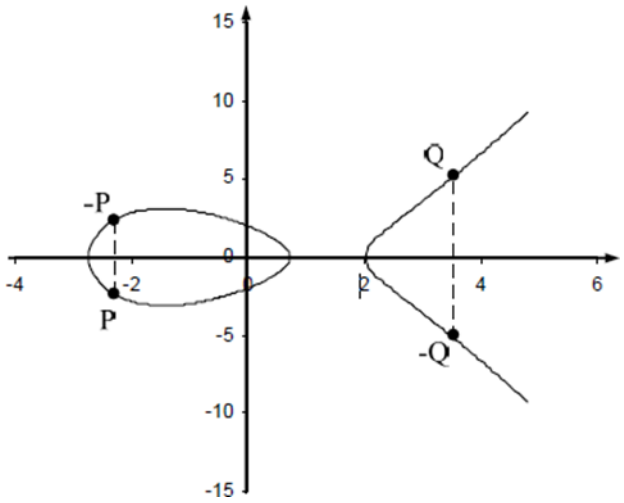


Σχήμα 4: Singular ελλειπτική καμπύλη

2.1.4 Πρόσθεση σημείων ελλειπτικής καμπύλης

Για αρχή θα παρουσιαστεί το πως ορίζεται γραφικά η πρόσθεση σημείων ελλειπτικής καμπύλης. Η πρόσθεση είναι βασισμένη στο γεγονός ότι μια ευθεία μπορεί να τέμνει μια ελλειπτική καμπύλη σε τρία σημεία το πολύ (Κάτος & Στεφανίδης, 2003).

Μια ελλειπτική καμπύλη εξ ορισμού είναι συμμετρική ως προς τον άξονα x. Μπορεί έτσι να ορίσουμε το αντίθετο σημείο (–P) ενός σημείου (P) της καμπύλης όπως φαίνεται παρακάτω :



Σχήμα 5: Ορισμός αντιθέτου

Παρατηρείται ότι αν P = (x, y), τότε –P = (x, –y).

Αυτό γεωμετρικά περιγράφεται ως εξής :

Υπολογίζουμε την ευθεία που διέρχεται από το σημείο P και το σημείο O (κατακόρυφη). Το τρίτο σημείο της καμπύλης είναι το –P. Το σημείο στο άπειρο είναι το σημείο εκείνο στο οποίο τέμνονται όλες οι παράλληλες με τον άξονα των y.

Επομένως το ουδέτερο στοιχείο στην πρόσθεση σημείων ελλειπτικής καμπύλης είναι το σημείο O:

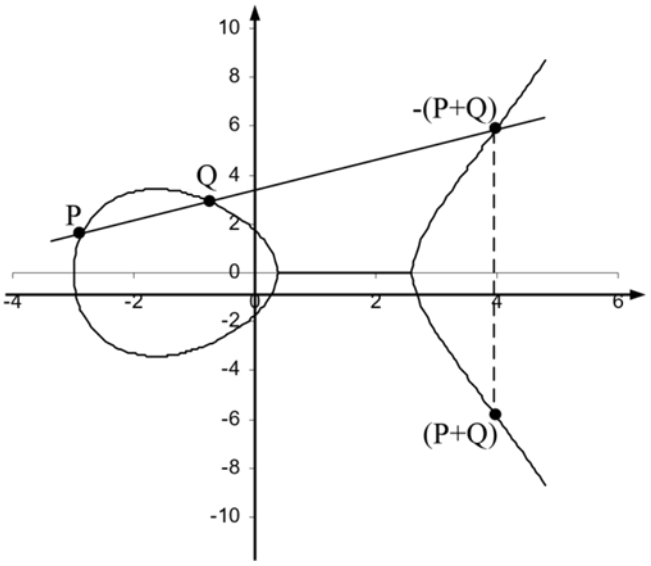
$$P + \mathbf{O} = \mathbf{O} + P = P,$$

και

$$P + (-P) = \mathbf{O}.$$

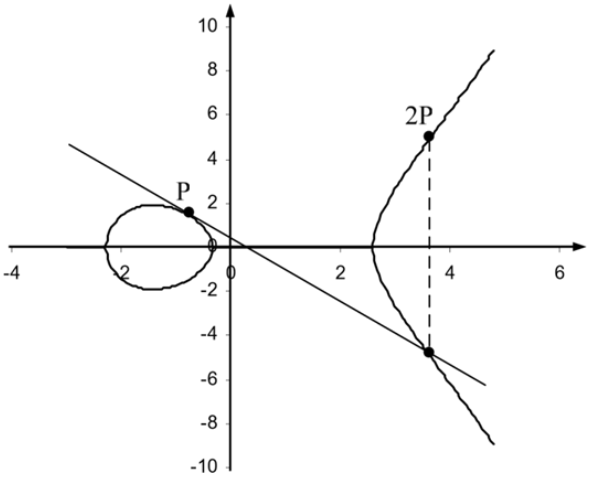
Έστω τα σημεία P και Q της ελλειπτικής καμπύλης όπως απεικονίζεται παρακάτω. Η ευθεία η οποία διέρχεται από τα P και Q, τέμνει την καμπύλη στο τρίτο σημείο το οποίο είναι το (P + Q).

Το σημείο (P + Q) θα είναι το συμμετρικό του –(P + Q) ως προς τον άξονα x.



Σχήμα 6: Πρόσθεση σημείων, P + Q

Στην περίπτωση που P = Q, θεωρούμε ότι τα δύο από τα τρία σημεία που τέμνουν την καμπύλη συμπίπτουν. Η ευθεία που ορίζεται είναι η εφαπτομένη στο σημείο P όπως φαίνεται παρακάτω



Σχήμα 7: P + P = 2P

Παρακάτω θα περιγράψουμε την πράξη της πρόσθεσης σημείων ελλειπτικής καμπύλης αλγεβρικά. Όπως είδαμε κατά τον γραφικό υπολογισμό, τα δύο σημεία καθώς και το αντίθετο του αθροίσματος αυτών βρίσκονται στην ίδια ευθεία.

Έστω τα δύο σημεία $P = (x_1, y_1)$ και $Q = (x_2, y_2)$. Τότε η ευθεία:

$y = \lambda x + c$, η οποία διέρχεται από τα σημεία αυτά θα έχει κλίση ίση με:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Αν στην εξίσωση της ελλειπτικής καμπύλης θέσουμε όπου *y* την εξίσωση ευθείας, οι συντεταγμένες του σημείου P + Q = (x_3, y_3) είναι:

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$

Οι σχέσεις παραπάνω προέκυψαν για διαφορετικά σημεία P και Q. Στην περίπτωση όπου Q = –P = (x_1, $-y_1$), η κλίση γίνεται άπειρη, γεγονός που μας οδηγεί στο σημείο **O**.

Τέλος, στην περίπτωση όπου P = Q, η πρόσθεση αντιστοιχεί με το διπλασιασμό του σημείου P. Η κλίση υπολογίζεται από την παραγώγιση της εξίσωσης της ελλειπτικής καμπύλης και είναι ίση με:

$$\lambda = \frac{3x_1^2 + a}{2y_1},$$

ενώ οι συντεταγμένες ορίζονται από τις σχέσεις που υπολογίσθηκαν για διαφορετικά P και Q.

2.1.5 Οι ελλειπτικές καμπύλες ορισμένες σε GF(2n)

Οι ελλειπτικές καμπύλες μπορούν να ορισθούν στο σώμα $GF(2^n)$. Μαζί με τις ελλειπτικές καμπύλες ορισμένες στο ***Zp***, οι οποίες καθορίστηκαν από το NIST. Ο κύριως λόγος της επιλογής του σώματος αυτού είναι η αποτελεσματική υλοποίηση των ελλειπτικών καμπυλών στο $GF(2^n)$ στις ψηφιακές τεχνολογίες.

Η εξίσωση της ελλειπτικής καμπύλης ορισμένης στο $GF(2^n)$ είναι η ακόλουθη:

$y^2 + xy = x^3 + ax^2 + b$, όπου $a\ b, \in GF(2^n)$.

Η πρόσθεση δύο σημείων P = (x_1, y_1)και Q = (x_2, y_2) ορίζεται από τις σχέσεις:

$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$

$y_3 = \lambda\ (x_1 + x_3) + x_3 + y_1$

Η πρόσθεση δύο σημείων P = (x_1, y_1)και Q = (x_2, y_2) ορίζεται από τις σχέσεις:

$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$

$y_3 = \lambda (x_1 + x_3) + x_3 + y_1$

όπου

$$\lambda = \frac{y_2 + y_1}{x_2 + x_1}.$$

Στην περίπτωση όπου P = Q, η πρόσθεση αντιστοιχεί στο 2P με:

$x_3 = \lambda^2 + \lambda + a$

$y_3 = (\lambda+1)\, x_1^2 + x_3$

όπου

$$\lambda = x_1 + \frac{y_1}{x_1}.$$

Το αντίθετο ενός σημείου P, έχει συντεταγμένες –P = (x_1, $x_1 + y_1$).

2.1.6 Ασφάλεια των ελλειπτικών καμπυλών

Έχει αναφερθεί ότι η πολυπλοκότητα των μεθόδων που προσπαθούν να επιλύσουν το πρόβλημα του διακριτού λογάριθμου στις ελλειπτικές καμπύλες είναι της μορφής n^a, $a > 0$.

Δηλαδή είναι εκθετικά πιο αργοί από την (λογαριθμική) πολυπλοκότητα του υπολογισμού βαθμωτών γινομένων του P.

Υπάρχει ωστόσο μια κατηγορία ελλειπτικών καμπυλών, οι υπεριδιάζουσες (supersingular) ελλειπτικές καμπύλες οι οποίες δεν θεωρούνται ασφαλείς, διότι είναι ευάλωτες σε επίθεση η οποία εκμεταλλεύεται έναν συγκεκριμένο ισομορφισμό μεταξύ των ελλειπτικών καμπυλών και των πεπερασμένων σωμάτων (Κάτος & Στεφανίδης, 2003).

Οι συγκεκριμένες ελλειπτικές καμπύλες συχνά μπορεί να προτιμηθούν λόγω της αποτελεσματικής ταχύτητας υλοποίησης των πράξεων, δεν συνιστώνται.

Άλλο ένα κριτήριο ασφάλειας των ελλειπτικών καμπυλών είναι το πλήθος των σημείων μιας ελλειπτικής καμπύλης. Όσο μεγαλύτερος είναι ο αριθμός των σημείων μιας καμπύλης, τόσο μεγαλύτερη θα είναι και η εξαντλητική αναζήτηση.

Ένας υπολογισμός σημείων μιας ελλειπτικής καμπύλης είναι δύσκολος. Διατυπώθηκε ένα θεώρημα από τον Hasse το οποίο θέτει τα όρια του πλήθους των στοιχείων της ελλειπτικής καμπύλης. Σύμφωνα λοιπόν με τον Hasse , μια καμπύλη ορισμένη στο $\boldsymbol{Z}p$, αναμένεται να έχει σημεία μεταξύ των ορίων (Stamatiou, et al., 2003):

$$p + 1 - 2\sqrt{p} \le |E| \le p + 1 + 2\sqrt{p}$$

2.2 Διακριτός λογάριθμος

2.2.1 Το πρόβλημα του διακριτού λογάριθμου (DLP)

Ο ορισμός του προβλήματος διακριτού λογαρίθμου :

Υποθέτοντας ότι (G, *) είναι μία κυκλική ομάδα πολλαπλασιασμού με βαθμό n και βάση g, τότε για κάθε a ∈ g υπάρχει ένας μοναδικός ακέραιος x με $0 \leq x \leq n-1$ τέτοιος ώστε $a = g^x$.

Το πρόβλημα της εύρεσης του x με δεδομένο ότι είναι γνωστά g και a ονομάζεται πρόβλημα του Διακριτού λογαρίθμου. Ο ακέραιος x καλείται διακριτός λογάριθμος του a ως προς την βάση g και συμβολίζεται με $\log_g a$.

Πρόβλημα διακριτού λογαρίθμου: Δοθέντος ενός πρώτου p, ενός γεννήτορα a του Z_p^* και ενός στοιχείου b του Z_p^*, να βρεθεί ακέραιος x, με $0 \leq x \leq p-2$, τέτοιος ώστε $a^x \equiv b \pmod p$ (Menezes, et al., 1996).

2.2.2 Γενικευμένο πρόβλημα διακριτού λογαρίθμου (GDLP)

Ο ορισμός του γενικευμένου προβλήματος διακριτού λογαρίθμου :

Έστω ότι δένεται μια πεπερασμένη κυκλικής ομάδας G τάξης n, ενός γεννήτορα a της G και ενός στοιχείου b ∈ G, το γενικευμένο πρόβλημα του διακριτού λογαρίθμου είναι να βρεθεί ο ακέραιος x, $0 \leq x \leq n-1$,τέτοιος ώστε $a^x = b$.

Να σημειωθεί ότι η δυσκολία του GDLP είναι ανεξάρτητη του γεννήτορα.

Έστω ότι a και c είναι δύο γεννήτορες μιας κυκλικής ομάδας G τάξης n, και έστω b ∈ G.

Έστω $x = \log_a b$, $c = \log_c b$ και $z = \log_a c$. Τότε $a^x = b = c^y = (a^z)^y$.

Συνεπώς, $x = z^y \bmod n$, και $\log_c b = (\log_a b)(\log_a c)^{-1} \bmod n$.

Αυτό σημαίνει ότι ένας αλγόριθμος ο οποίος υπολογίζει λογαρίθμους ως προς βάση το a μπορεί να χρησιμοποιηθεί για να υπολογίσει λογαρίθμους ως προς μια άλλη βάση c που είναι επίσης γεννήτορας της ομάδας G.

2.3 Η συνάρτηση φ του Euler

Για κάθε n ≥ 1, θεωρούμε την συνάρτηση φ(n) που συμβολίζει το πλήθος των ακεραίων στο διάστημα [1,n], οι οποίοι είναι σχετικά πρώτοι με το n (Menezes, et al., 1996).

Ιδιότητες της συνάρτησης φ του Euler:

1. $\phi(p) = p - 1$ όπου p πρώτος.
2. $\phi(p^a) = p^a (1 - \frac{1}{p})$ όπου p πρώτος
3. $\phi(mn) = \phi(m)\phi(n)$ για m,n σχετικά πρώτους

Παρατηρείται από τις ιδιότητες 2 και 3 ότι αν είναι γνωστή η ανάλυση ενός αριθμού n σε πρώτους παράγοντες τότε εύκολα υπολογίζεται το φ(n).

Επίσης ισχύει ότι:

- Για κάθε $n \in N$ ισχύει $\phi(n) = n \Pi_{p|n} (1 - \frac{1}{p})$.
- Έστω n = pq, p, q πρώτοι, $p \neq q$. Γνώση των δύο πρώτων p,q είναι ισοδύναμη με γνώση του φ(n).

Θεώρημα του Euler : Αν $a \in Z_n^*$ τότε $a^{\varphi(n)} \equiv 1 \bmod n$.

2.4 Μικρό θεώρημα του Fermat

Μία περίπτωση που μπορεί να χαρακτηριστεί και σαν ειδική είναι του θεωρήματος του Euler (Menezes, et al., 1996) είναι το μικρό θεώρημα του Fermat.

Κάθε φυσικός αριθμός $p \in N$, εάν ο p είναι πρώτος αριθμός, τότε για κάθε ακέραιο a, το $a^p - a$ διαιρείται με το p.

ΟΡΙΣΜΟΣ: Έστω p ένας πρώτος αριθμός. Αν gcd(a, p) = 1 για κάποιον ακέραιο αριθμό α, τότε $a^{p-1} \equiv 1 \bmod p$.

3

Είδη Κρυπτογράφησης

3.1 Ασύμμετρη Κρυπτογραφία

Η ασύμμετρη κρυπτογραφία, γνωστή και ως κρυπτογραφία δημόσιου κλειδιού (Basharat, et al., 2018), είναι μια διαδικασία που χρησιμοποιεί ένα ζεύγος κλειδιών που σχετίζονται μεταξύ τους, ένα δημόσιο και ένα ιδιωτικό κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση ενός μηνύματος και την προστασία του από μη εξουσιοδοτημένη πρόσβαση ή χρήση.

Ένα δημόσιο κλειδί είναι ένα κρυπτογραφικό κλειδί που μπορεί να χρησιμοποιηθεί από οποιοδήποτε άτομο για την κρυπτογράφηση ενός μηνύματος έτσι ώστε να μπορεί να αποκρυπτογραφηθεί μόνο από τον προβλεπόμενο παραλήπτη με το ιδιωτικό του κλειδί. Ένα ιδιωτικό κλειδί γνωστό και ως μυστικό κλειδί είναι γνωστό μόνο στον δημιουργό του.

Όταν κάποιος θέλει να στείλει ένα κρυπτογραφημένο μήνυμα, μπορεί να κατεβάσει το δημόσιο κλειδί του παραλήπτη από έναν δημόσιο κατάλογο και να το χρησιμοποιήσει για να κρυπτογραφήσει το μήνυμα πριν το στείλει. Ο παραλήπτης του μηνύματος μπορεί στη συνέχεια να αποκρυπτογραφήσει το μήνυμα χρησιμοποιώντας το σχετικό ιδιωτικό κλειδί.

Εάν ο αποστολέας κρυπτογραφήσει το μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί, το μήνυμα μπορεί να αποκρυπτογραφηθεί μόνο χρησιμοποιώντας το δημόσιο κλειδί αυτού του αποστολέα, επαληθεύοντας έτσι την ταυτότητα του αποστολέα. Αυτές οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης συμβαίνουν αυτόματα. Οι χρήστες δεν χρειάζεται να κλειδώσουν και να ξεκλειδώσουν φυσικά το μήνυμα.

Σχήμα 8 : Ασύμμετρη Κρυπτογράφηση με χρήση δημόσιου και ιδιωτικού κλειδιού

Πολλά πρωτόκολλα βασίζονται σε ασύμμετρη κρυπτογραφία, συμπεριλαμβανομένων των πρωτοκόλλων TLS (transport layer security) και SSL (secure sockets layer), τα οποία καθιστούν δυνατό το HTTPS.

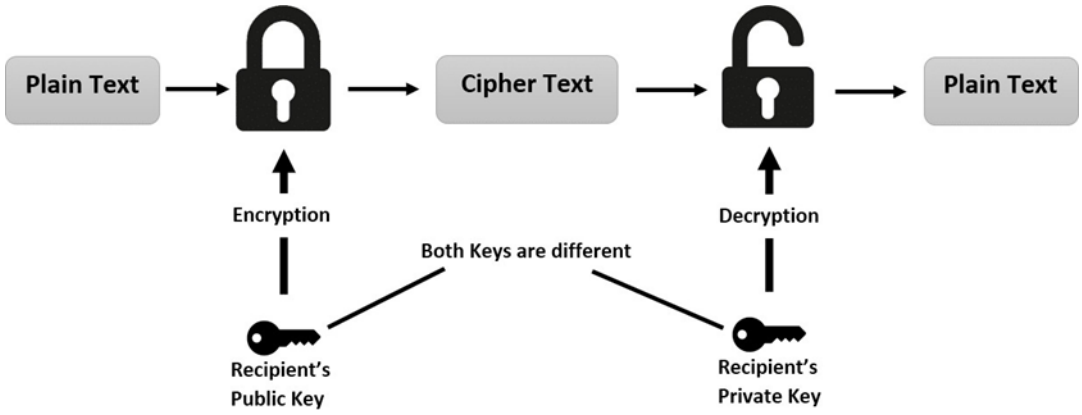
Η ασύμμετρη κρυπτογραφία μπορεί επίσης να εφαρμοστεί σε συστήματα στα οποία πολλοί χρήστες μπορεί να χρειαστεί να κρυπτογραφήσουν και να αποκρυπτογραφήσουν μηνύματα, όπως:

- **Κρυπτογραφημένο email**: Ένα δημόσιο κλειδί μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση ενός μηνύματος και ένα ιδιωτικό κλειδί μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση του.
- **Ψηφιακές υπογραφές**: Η ψηφιακή υπογραφή χρησιμοποιείται για την επικύρωση της αυθεντικότητας και της ακεραιότητας ενός μηνύματος, λογισμικού ή ψηφιακού εγγράφου.
- **SSL/TLS**: Η δημιουργία κρυπτογραφημένων συνδέσμων μεταξύ ιστοτόπων και προγραμμάτων περιήγησης χρησιμοποιεί επίσης ασύμμετρη κρυπτογράφηση.
- **Κρυπτονομίσματα**: Το Bitcoin όπως και άλλα κρυπτονομίσματα βασίζονται στην ασύμμετρη κρυπτογραφία .

Μερικοί γνωστοί αλγόριθμοι Κρυπτογράφησης Δημοσίου Κλειδιού είναι οι παρακάτω :

3.1.1 RSA (Rivest - Shamir - Adleman)

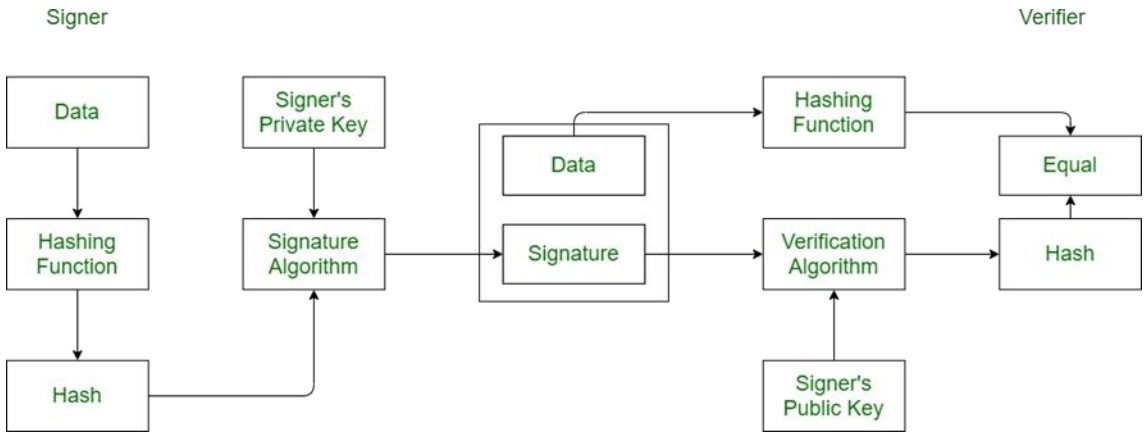
Το RSA, το οποίο κατοχυρώθηκε με δίπλωμα ευρεσιτεχνίας το 1983 και εξακολουθεί να είναι το πιο ευρέως χρησιμοποιούμενο σύστημα για την ψηφιακή ασφάλεια, κυκλοφόρησε το ίδιο έτος με το Diffie-Hellman και πήρε την ονομασία του από τους εφευρέτες, Ron Rivest, Adi Shamir & Leonard Adleman (Asaithambi, 2015). Το RSA λαμβάνει μεγάλο μέρος της πρόσθετης ασφάλειάς του συνδυάζοντας δύο αλγόριθμους: ο ένας εφαρμόζεται στην ασύμμετρη κρυπτογραφία και ο άλλος αλγόριθμος παρέχει ασφαλείς ψηφιακές υπογραφές. Ο αλγόριθμος RSA έχει τρεις κύριες διαδικασίες: δημιουργία ζεύγους κλειδιών, κρυπτογράφηση και αποκρυπτογράφηση. Τα ζεύγη κλειδιών περιλαμβάνουν τη δημιουργία του δημόσιου κλειδιού και του ιδιωτικού κλειδιού, το μέγεθος των ιδιωτικών κλειδιών προτείνεται να έχει τουλάχιστον μέγεθος 2048 bits.



Σχήμα 9 : RSA Αλγόριθμος

3.1.2 DSA (Digital Signature Algorithm)

Το 1991, η Εθνική Υπηρεσία Ασφάλειας (NSA) ανέπτυξε τον αλγόριθμο ψηφιακής υπογραφής (DSA) ως εναλλακτική λύση στον αλγόριθμο RSA. Όπως το RSA, έτσι και το DSA είναι ένα σύστημα ασύμμετρης κρυπτογράφησης, το οποίο δημιουργεί ένα ζεύγος κλειδιών (ιδιωτικό και δημόσιο) (Asaithambi, 2015).



Σχήμα 10 : DSA Αλγόριθμος

3.1.3 ECC & ECDSA

Η κρυπτογραφία ελλειπτικής καμπύλης (ECC) ή ο αλγόριθμος ψηφιακής υπογραφής ελλειπτικής καμπύλης (ECDSA) ήταν γνωστός και μελετήθηκε στον κόσμο των μαθηματικών για 150 χρόνια πριν εφαρμοστεί στην κρυπτογραφία. Οι Neal Koblitz (Koblitz, et al., 2000) και Victor S. Miller (Miller, 1985) το πρότειναν αρχικά το 1985. Ωστόσο, το 2005, η NSA κυκλοφόρησε ένα νέο σύνολο αλγορίθμων ασφαλείας που εγκρίθηκαν από την κυβέρνηση των ΗΠΑ.

Η κρυπτογραφία ελλειπτικής καμπύλης είναι ένας νέος αλγόριθμος κρυπτογραφίας που έχει αναπτυχθεί για αυξημένη ασφάλεια και πιο ισχυρή απόδοση δικτύου. Το ECDSA (Elliptic Curve Digital Signature Algorithm) βασίζεται στο DSA, αλλά χρησιμοποιεί ακόμη μια άλλη μαθηματική προσέγγιση για τη δημιουργία κλειδιών.

Το ECC είναι μια μαθηματική εξίσωση που λαμβάνεται από μόνη της, αλλά το ECDSA είναι ο αλγόριθμος που εφαρμόζεται στο ECC για να καταστεί κατάλληλος για κρυπτογράφηση ασφαλείας.

Ένα κύριο χαρακτηριστικό του ECDSA έναντι ενός άλλου δημοφιλούς αλγόριθμου, του RSA, είναι ότι το ECDSA παρέχει υψηλότερο βαθμό ασφάλειας με μικρότερα μήκη κλειδιών και λιγότερη υπολογιστική ισχύ.

NIST προτεινόμενα μεγέθη κλειδιών

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Σχήμα 11: Προτεινόμενα μεγέθη κλειδιών

3.2 Συμμετρική Κρυπτογραφία

Στη συμμετρική κρυπτογράφηση (Symmetric Cryptography ή Secret-Key Cryptography) χρησιμοποιείται ένα μυστικό κλειδί τόσο για κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Αυτή η προσέγγιση είναι το αντίστροφο της Ασύμμετρης Κρυπτογράφησης, η οποία χρησιμοποιεί ένα κλειδί για την κρυπτογράφηση και ένα άλλο για την αποκρυπτογράφηση (Ayushi, 2010). Τα δεδομένα μεταφράζονται σε μορφή που δεν μπορεί να ερμηνευθεί ή να επιθεωρηθεί από κάποιον που δεν έχει το μυστικό κλειδί που χρησιμοποιείται για την κρυπτογράφηση τους κατά τη διάρκεια αυτής της φάσης.

Η ισχύς της γεννήτριας τυχαίων αριθμών που χρησιμοποιείται για τη δημιουργία του μυστικού κλειδιού καθορίζει την αποτελεσματικότητα αυτής της μεθόδου. Η Symmetric Key Cryptography, που χρησιμοποιείται συνήθως στο Διαδίκτυο σήμερα, περιλαμβάνει δύο είδη αλγορίθμων:

- Block : Κρυπτογραφεί τα ψηφία ή τα γράμματα ενός μηνύματος ένα κάθε φορά.
- Stream cipher: Κρυπτογράφηση μιας ομάδα bit ως μια ενιαία οντότητα, εισάγοντας το απλό κείμενο για να γίνει πολλαπλάσιο του μεγέθους του μπλοκ.

Αυτός ο τύπος κρυπτογράφησης είναι συνήθως πολύ πιο γρήγορος από την ασύμμετρη κρυπτογράφηση, αλλά επιτρέπει τη διατήρηση του μυστικού κλειδιού τόσο από τον αποστολέα όσο και από τον παραλήπτη δεδομένων.

Σχήμα 12: Συμμετρική Κρυπτογράφηση

3.2.1 AES

Ο πιο συχνά χρησιμοποιούμενος συμμετρικός αλγόριθμος είναι ο Advanced Encryption Standard (AES) (Esparham, et al., 2018), ο οποίος αρχικά ήταν γνωστός ως Rijndael. Αυτό είναι το πρότυπο που ορίστηκε από το NIST το 2001 για την κρυπτογράφηση των ηλεκτρονικών δεδομένων που ανακοινώθηκε στο FIPS PUB 197 των ΗΠΑ. Αυτό το πρότυπο αντικαθιστά τον DES, το οποίο χρησιμοποιήθηκε από το 1977. Σύμφωνα με το NIST, ο κρυπταλγόριθμος AES έχει μέγεθος μπλοκ 128 bit , αλλά μπορεί να έχει τρία διαφορετικά μήκη κλειδιών όπως φαίνεται στα AES-128, AES-192 και AES-256.

Χαρακτηριστικά AES

- SP Network: Λειτουργεί σε μια δομή δικτύου SP αντί για μια δομή κρυπτογράφησης Feistel, όπως διακρίνεται στην περίπτωση του αλγόριθμου DES.
- Key Expansion: Απαιτείται μόνο ένα κλειδί κατά τη διάρκεια του πρώτου σταδίου, το οποίο αργότερα επεκτείνεται σε πολλαπλά κλειδιά που χρησιμοποιούνται σε μεμονωμένους γύρους.
- Byte Data: Ο αλγόριθμος κρυπτογράφησης AES εκτελεί λειτουργίες σε δεδομένα byte αντί για δεδομένα bit. Επομένως, αντιμετωπίζει το μέγεθος μπλοκ 128-bit ως 16 byte κατά τη διαδικασία κρυπτογράφησης.
- Key Length: Ο αριθμός των γύρων που πρέπει να πραγματοποιηθούν εξαρτάται από το μήκος του κλειδιού που χρησιμοποιείται για την κρυπτογράφηση δεδομένων. Το μέγεθος κλειδιού 128 bit έχει δέκα γύρους, το μέγεθος κλειδιού 192 bit έχει 12 γύρους και το μέγεθος κλειδιού 256 bit έχει 14 γύρους.

3.2.2 DES

Ο αλγόριθμος DES (Data Encryption Standard) είναι ένας αλγόριθμος κρυπτογράφησης συμμετρικού κλειδιού που δημιουργήθηκε στις αρχές της δεκαετίας του 1970 από μία ομάδα της IBM και υιοθετήθηκε από το NIST που βασίζεται σε ένα δίκτυο Feistel. Ο αλγόριθμος παίρνει το απλό κείμενο σε μπλοκ 64-bit και τα μετατρέπει σε κρυπτογραφημένο κείμενο χρησιμοποιώντας κλειδιά 48-bit.

Δεδομένου ότι είναι ένας αλγόριθμος συμμετρικού κλειδιού , χρησιμοποιεί το ίδιο κλειδί τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση των δεδομένων. Αντιθέτως εάν ήταν ένας ασύμμετρος αλγόριθμος, θα χρησιμοποιούσε διαφορετικά κλειδιά για κρυπτογράφηση και αποκρυπτογράφηση (Esparham, et al., 2018).

Υπάρχουν ορισμένα μηχανήματα που μπορούν να χρησιμοποιηθούν για να σπάσουν τον αλγόριθμο DES. Ο αλγόριθμος DES χρησιμοποιεί ένα κλειδί μεγέθους 56 bit. Χρησιμοποιώντας αυτό το κλειδί, το DES παίρνει ως είσοδο ένα μπλοκ απλού κειμένου 64 bit και δημιουργεί ένα μπλοκ κρυπτογραφημένου κειμένου 64 bit.

Η διαδικασία DES περιλαμβάνει πολλά βήματα, όπου κάθε βήμα ονομάζεται γύρος. Ανάλογα με το μέγεθος του κλειδιού που χρησιμοποιείται, ο αριθμός των γύρων ποικίλλει. Για παράδειγμα, ένα κλειδί 128 bit απαιτεί 10 γύρους, ένα κλειδί 192 bit απαιτεί 12 γύρους και ούτω καθεξής.

3.2.3 Triple DES

Το 3DES ή αλγόριθμος τριπλής κρυπτογράφησης δεδομένων (TDEA) (Singh & Supriya, 2013) είναι μια σειρά κρυπτογράφησης που βασίζεται στο πρότυπο κρυπτογράφησης δεδομένων που αναπτύχθηκε από την IBM στις αρχές της δεκαετίας του 1970 και υιοθετήθηκε από το NIST (με μικρές αλλαγές) το 1977. Το 3DES εισήχθη κατά τη διάρκεια μιας περιόδου μετάβασης μεταξύ δύο μεγάλων αλγορίθμων. Το 1997, το NIST ανακοίνωσε μια επίσημη αναζήτηση για υποψήφιους αλγόριθμους για να αντικαταστήσει το DES ενώ το 2001 κυκλοφόρησε τον AES με σκοπό να συνυπάρξει με το 3DES μέχρι το 2030, επιτρέποντας μια σταδιακή μετάβαση. Παρ' όλα αυτά Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) δημοσίευσε ένα προσχέδιο πρότασης λέγοντας ότι όλες οι μορφές 3DES θα καταργηθούν έως το 2023 και θα απαγορεύονται από το 2024 και μετά.

Ο 3DES αναπτύχθηκε για να αντιμετωπίσει τα προφανή ελαττώματα του DES χωρίς να σχεδιαστεί ένα εντελώς νέο κρυπτοσύστημα. Ο DES χρησιμοποιεί ένα κλειδί 56 bit και δεν θεωρείται επαρκές για την κρυπτογράφηση ευαίσθητων δεδομένων. Το 3-DES απλώς επεκτείνει το μέγεθος του κλειδιού του DES εφαρμόζοντας τον αλγόριθμο τρεις φορές διαδοχικά με τρία διαφορετικά κλειδιά. Το συνδυασμένο μέγεθος κλειδιού είναι 168 bits (3 φορές το 56). Ο TDEA περιλαμβάνει τη χρήση τριών κλειδιών DEA 64 bit (K1, K2, K3) σε λειτουργία κρυπτογράφησης-αποκρυπτογράφησης - κρυπτογράφησης (EDE), δηλαδή το απλό κείμενο κρυπτογραφείται με το κλειδί K1, στη συνέχεια αποκρυπτογραφείται με το K2, και στη συνέχεια κρυπτογραφείται ξανά με το K3.

3.2.4 RC2

Ο RC2 που είναι επίσης γνωστός ως ARC2 είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ο οποίος ήταν δημοφιλής στις αρχές της δεκαετίας του ‘90, με μήκος κλειδιού από 1 έως 128 byte και μήκος block να ισούται με 8 byte. Αναπτύχθηκε από την RSA Security και πιο συγκεκριμένα από τον Ron Rivest και η δημοσιοποίησή του έγινε το 1996.

Ο κρυπτογραφικός αλγόριθμος RC2 όπως προαναφέρθηκε έχει μήκος block 8 byte (64bit), που αυτό σημαίνει ότι τα δεδομένα εισόδου αρχικά χωρίζονται σε μπλοκ των 8 byte και στη συνέχεια το καθένα από αυτά υποβάλλεται σε επεξεργασία ξεχωριστά.

Κάθε μπλοκ δεδομένων αντιμετωπίζεται ως τέσσερις λέξεις, κάθε λέξη έχει 16 bit (2 byte). Ο πίνακας τεσσάρων λέξεων παρουσιάζεται ως R[0] R[1] R[2] R[3] . Τόσο η κρυπτογράφηση όσο και η αποκρυπτογράφηση λαμβάνουν αυτόν τον πίνακα ως είσοδο και τροποποιούν τις τέσσερις λέξεις. Η έξοδος επιστρέφεται στον ίδιο πίνακα (Charbathia & Sharma, 2014).

3.2.5 RC4

Ο κρυπτογραφικός αλγόριθμος RC4 που είναι επίσης γνωστός ως ARCFOUR ή ARC4 είναι ένας αλγόριθμος ροής που φημίζεται για την ταχύτητα και την απλότητα του, με μήκος κλειδιού έως και 2048 bit (Charbathia & Sharma, 2014). Ομοίως με τον RC2, ο RC4 σχεδιάστηκε από τον Ron Rivest της RSA Security το 1987 με την δημοσιοποίησή του να γίνεται το 1994 και χρησιμοποιήθηκε ευρέως σε δημοφιλή πρωτόκολλα και πρότυπα

κρυπτογράφησης όπως για παράδειγμα στο TLS (Transport Layer Security) και WEP (Wired Equivalent Privacy) για την προστασία της κυκλοφορίας στο Διαδίκτυο και την προστασία των ασύρματων δικτύων αντίστοιχα.

3.2.6 RC5

Ο κρυπτογραφικός αλγόριθμος RC5 δημοσιεύτηκε το 1994 από τον Ronald Rivest. Σε αντίθεση με τους προηγούμενους κρυπταλγόριθμους στον αλγόριθμο RC5, το μέγεθος του μπλοκ απλού κειμένου εισαγωγής, ο αριθμός των γύρων και 8 bits του κλειδιού μπορεί να είναι μεταβλητού μήκους. Μόλις αποφασιστούν οι τιμές αυτού, οι τιμές θα παραμείνουν οι ίδιες για μια συγκεκριμένη εκτέλεση του κρυπτογραφικού αλγορίθμου . Το μέγεθος του μπλοκ απλού κειμένου μπορεί να είναι 32 bit, 64 bit ή 128 bit ενώ το μήκος του κλειδιού μπορεί να είναι από 0 έως 2040 bit. Η έξοδος που δημιουργείται από το RC5 είναι το κρυπτογραφημένο κείμενο που έχει το ίδιο μέγεθος με το μέγεθος απλού κειμένου (Rivest, 1997).

Στο RC5, το απλό μήνυμα κειμένου χωρίζεται σε δύο μπλοκ A και B το καθένα των 32 bit. Στη συνέχεια δημιουργούνται δύο δευτερεύοντα κλειδιά S[0] και S[1]. Αυτά τα δύο δευτερεύοντα κλειδιά προστίθενται στο A και B αντίστοιχα. Αυτή η διαδικασία παράγει μπλοκ C και D αντίστοιχα και σηματοδοτεί το τέλος της εφάπαξ λειτουργίας και στη συνέχεια ξεκινά η διαδικασία του γύρου.

3.2.7 RC6

Ο κρυπτογραφικός αλγόριθμος RC6 προέρχεται από τον RC5 και σχεδιάστηκε από τους Ron Rivest , Yiqun Lisa Yin, Ray Sidney και Matt Robshaw . Ο RC6 είναι ένας παραμετροποιημένος αλγόριθμος όπου το μέγεθος του μπλοκ (128 bits), το μέγεθος του κλειδιού και ο αριθμός των γύρων είναι μεταβλητά. Το ανώτατο όριο στο μέγεθος του κλειδιού είναι 2040 bit (Charbathia & Sharma, 2014).

Στην πραγματικότητα, το RC6 θα μπορούσε να θεωρηθεί ως η διασύνδεση δύο παράλληλων διαδικασιών κρυπτογράφησης RC5, στην περίπτωση που ο RC6 χρησιμοποιεί μια πρόσθετη πράξη πολλαπλασιασμού που δεν υπάρχει στο RC5, προκειμένου να εξαρτηθεί η περιστροφή από κάθε bit σε μια λέξη, και όχι μόνο από τα λιγότερο σημαντικά bit.

Διαφορές μεταξύ Συμμετρικής και Ασύμμετρης Κρυπτογράφησης

Βασικές Διαφορές	Συμμετρική κρυπτογράφηση	Ασύμμετρη κρυπτογράφηση
Μέγεθος κρυπτογραφημένου κειμένου	Το μικρότερο κείμενο κρυπτογράφησης συγκρίνεται με το αρχικό αρχείο απλού κειμένου.	Μεγαλύτερο κείμενο κρυπτογράφησης σε σύγκριση με το αρχικό αρχείο απλού κειμένου.
Μέγεθος δεδομένων	Χρησιμοποιείται για τη μετάδοση μεγάλων δεδομένων.	Χρησιμοποιείται για τη μετάδοση μικρών δεδομένων.
Εκμετάλλευση πόρων	Η κρυπτογράφηση συμμετρικού κλειδιού λειτουργεί με χαμηλή χρήση πόρων.	Η ασύμμετρη κρυπτογράφηση απαιτεί υψηλή κατανάλωση πόρων.
Μήκη κλειδιών	Μέγεθος κλειδιού 128 ή 256 bit.	Μέγεθος κλειδιού RSA 2048 bit ή μεγαλύτερο.
Ασφάλεια	Λιγότερο ασφαλές λόγω της χρήσης ενός μόνο κλειδιού για κρυπτογράφηση.	Πολύ πιο ασφαλές καθώς δύο κλειδιά εμπλέκονται στην κρυπτογράφηση και την αποκρυπτογράφηση.
Αριθμός κλειδιών	Η Συμμετρική Κρυπτογράφηση χρησιμοποιεί ένα μόνο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση.	Η Ασύμμετρη κρυπτογράφηση χρησιμοποιεί δύο κλειδιά για κρυπτογράφηση και αποκρυπτογράφηση
Τεχνικές	Είναι παλιά τεχνική.	Είναι μια σύγχρονη τεχνική κρυπτογράφησης.
Εμπιστευτικότητα	Χρησιμοποιείται ένα μόνο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση, συνεπώς υπάρχουν περισσότερες πιθανότητες να παραβιαστεί το κλειδί.	Δύο κλειδιά ξεχωριστά κατασκευασμένα για κρυπτογράφηση και αποκρυπτογράφηση που αφαιρεί την ανάγκη κοινής χρήσης ενός κλειδιού.
Ταχύτητα	Η συμμετρική κρυπτογράφηση είναι γρήγορη τεχνική	Η ασύμμετρη κρυπτογράφηση είναι πιο αργή όσον αφορά την ταχύτητα.
Αλγόριθμοι	RC4, AES, DES, 3DES και QUAD.	Αλγόριθμοι RSA, Diffie-Hellman, ECC.

3.3 Συνάρτηση κατακερματισμού

Με τον όρο συνάρτηση κατακερματισμού (hash function) h υποδηλώνουμε ένα μετασχηματισμό ο οποίος παίρνει ως είσοδο ένα μήνυμα m οποιουδήποτε μήκους και επιστρέφει στην έξοδο μία ακολουθία χαρακτήρων h(m) περιορισμένου μήκους η οποία καλείται ως τιμή κατακερματισμού (hash value). Ως σύνοψη μηνύματος καλείται η τιμή κατακερματισμού στην οποία εμφανίζει το μεγαλύτερο μήνυμα ή έγγραφο συνοπτικά. Θα μπορούσε να θεωρηθεί η σύνοψη του μηνύματος ως «ψηφιακό αποτύπωμα» (digital fingerprint) ενός εγγράφου.

Ο συνδυασμός συναρτήσεων κατακερματισμού με ασύμμετρη κρυπτογραφία παρέχει δυνατότητες επαλήθευσης και αναγνώρισης. Ένας έλεγχος ακεραιότητας διασφαλίζει ότι τα δεδομένα δεν έχουν τροποποιηθεί, καθώς και μια διαβεβαίωση για το ποιος πραγματικά δημιούργησε το hash. Μαζί αυτοί οι δύο μηχανισμοί παρέχουν αυτό που ονομάζεται ψηφιακή υπογραφή.

Το Hashing χρησιμοποιείται για τη λήψη ενός στιγμιότυπου δεδομένων σε μια χρονική στιγμή. Για να προσδιοριστεί εάν τα δεδομένα έχουν αλλάξει, θα γίνει σύγκριση μεταξύ του αρχικού αποτελέσματος κατακερματισμού και του αποτελέσματος κατακερματισμού που λήφθηκε αργότερα. Εάν τα αποτελέσματα κατακερματισμού είναι πανομοιότυπα, τα δεδομένα δεν έχουν αλλάξει. Αν εφαρμοστεί έστω και μια μικρή ασήμαντη αλλαγή στα δεδομένα, τα αποτελέσματα κατακερματισμού θα είναι διαφορετικά.

Η δημιουργία μια ψηφιακής υπογραφής βασίζεται στις συναρτήσεις κατακερματισμού και τους αλγόριθμους δημόσιου κλειδιού. Πιο συγκεκριμένα, τα δεδομένα περνούν μέσω μιας συνάρτησης κατακερματισμού για να παράγουν μια μαθηματική περίληψη η οποία μπορεί αργότερα να συγκριθεί με μια νέα περίληψη για να ελεγχθεί η ακεραιότητα των δεδομένων. Αυτό το αποτέλεσμα κατακερματισμού κρυπτογραφείται στη συνέχεια από τον δημιουργό των δεδομένων για να παρέχει έναν μηχανισμό ταυτοποίησης.

Μόλις ένα αρχείο έχει υπογραφεί ψηφιακά, τυχόν αλλαγές που γίνονται στο αρχείο θα οδηγήσουν σε σφάλμα όταν ένας χρήστης επιχειρήσει να επαληθεύσει την υπογραφή. Η επαλήθευση μιας ψηφιακής υπογραφής καθορίζει επίσης ποιος υπέγραψε αρχικά το αρχείο.

3.3.1 Συναρτήσεις Κατακερματισμού SHA

Οι ασφαλής συναρτήσεις κατακερματισμού γνωστοί και ως SHA (Secure Hash Algorithm) είναι μια οικογένεια κρυπτογραφικών λειτουργιών που έχουν σχεδιαστεί για να διατηρούν τα δεδομένα ασφαλή και δημοσιοποιήθηκαν για πρώτη φορά το 1993 από το NIST.

Μερικοί αλγόριθμοι ενδιαφέροντος είναι οι SHA-1, SHA-2 και SHA-3, καθένας από τους οποίους σχεδιάστηκε διαδοχικά με ολοένα και ισχυρότερη κρυπτογράφηση ως απάντηση σε επιθέσεις από κακόβουλους χρήστες.

Οι συναρτήσεις κατακερματισμού παράγουν μια συμβολοσειρά σταθερού μεγέθους που δεν μοιάζει καθόλου με την αρχική. Αυτοί οι αλγόριθμοι έχουν σχεδιαστεί για να είναι μονόδρομες συναρτήσεις, που σημαίνει ότι μόλις μετατραπούν στις αντίστοιχες τιμές κατακερματισμού τους, είναι σχεδόν αδύνατο να μετατραπούν ξανά στα αρχικά δεδομένα.

Μερικοί γνωστές Συναρτήσεις κατακερματισμού είναι οι παρακάτω:

3.3.1.1 SHA-1

Το SHA-1 δημιουργήθηκε από την NSA και προτάθηκε το 1993 από το NIST. Είναι η πιο ευρέως χρησιμοποιούμενη από τις υπάρχουσες συναρτήσεις κατακερματισμού SHA και θεωρείται πλέον επισφαλής από το 2005. Χρησιμοποιείται σε πολλές ευρέως χρησιμοποιούμενες εφαρμογές και πρωτόκολλα, συμπεριλαμβανομένων των TLS, SSL , IPsec, S/MIME , SSH , και PGP.

Λειτουργεί τροφοδοτώντας ένα μήνυμα ως συμβολοσειρά bit με μήκος μικρότερο από 2^{64} bit και παράγει μια τιμή κατακερματισμού 160 bit γνωστή ως σύνοψη μηνυμάτων.

3.3.1.2 SHA-2

Ο αλγόριθμος SHA-2 δημιουργήθηκε από την NSA των ΗΠΑ το 2001 και απέκτησε πρότυπο από τον NIST. Στην πράξη αντικατέστησε τον SHA-1 και αποτελείται από τέσσερις εκδόσεις παράγοντας συνόψεις των 224, 256, 384, ή 512-bit με αντίστοιχη ονομασία SHA-224/256/384 και 512. Επιπλέον, δύο άλλες εκδόσεις, ο SHA-512/224 και ο SHA-512/256, παρέχουν συνόψεις 224-bit και 256-bit, αντίστοιχα, με περικοπή του αποτελέσματος του SHA-512. Στην εποχή μας χρησιμοποιείται ως επί το πλείστων ο SHA-256, ο οποίο παρέχει τα ελάχιστα 128-bit ασφαλείας που απαιτούνται για τις τρεις ιδιότητες ασφαλείας.

3.3.1.3 SHA-3

Το 2007 ο NIST διοργάνωσε ανοικτό διαγωνισμό για ένα νέο πρότυπο συνάρτησης κατακερματισμού, το SHA-3. Το 2015 εκδόθηκε το πρότυπο της νέας συνάρτησης-νικητή του διαγωνισμού. Η συνάρτηση SHA-3 δεν έχει προκαθορισμένο μήκος εξόδου (όπως ούτε και εισόδου). Προσφέρει τις παραλλαγές SHA-3-224/256/384 και 512. Ο SHA-3 είναι ένας κρυπτογραφικός αλγόριθμος που βασίζεται σε μία μετάθεση (permutation) η οποία ονομάζεται keccak-f.

Για να εξηγήσουμε πως λειτουργεί, μία συνάρτηση επανάληψης λαμβάνει 1600-bit δεδομένων και στη συνέχεια τα τοποθετεί σε 24 γύρους μετάθεσης χρησιμοποιώντας έναν συγκεκριμένο αλγόριθμο. Μετά από αυτό, περνά στο επόμενο στάδιο ως block 1600-bit. Αυτό συνεχίζεται μέχρι να ολοκληρωθεί η φάση απορρόφησης. Με την ολοκλήρωση της φάσης απορρόφησης, το τελευταίο block των 1600- bit περνά στη φάση συμπίεσης.

4

Σχήματα Ψηφιακών υπογραφών

Μία ψηφιακή υπογραφή μηνυμάτων είναι λειτουργικά ισοδύναμη με μια φυσική υπογραφή, η οποία είναι εξίσου ανθεκτική στην πλαστογράφηση όσο και μία αντίστοιχη φυσική υπογραφή. Τα συστήματα που παρέχουν αυτή τη λειτουργικότητα ονομάζονται Σχήματα Ψηφιακών Υπογραφών. Ένα σχήμα ψηφιακής υπογραφής έχει δύο συστατικά, έναν ιδιωτικό αλγόριθμο υπογραφής που επιτρέπει σε έναν χρήστη να υπογράψει με ασφάλεια ένα μήνυμα και έναν δημόσιο αλγόριθμο επαλήθευσης που επιτρέπει σε οποιονδήποτε να επαληθεύσει ότι η υπογραφή είναι αυθεντική. Η υπογραφή του αλγορίθμου πρέπει να "δεσμεύει" μια υπογραφή σε ένα μήνυμα με τέτοιο τρόπο ώστε η υπογραφή να μην μπορεί να αφαιρεθεί και να χρησιμοποιηθεί για την υπογραφή άλλου έγγραφου, ή αν τροποποιηθεί το αρχικό μήνυμα η υπογραφή να μην παραμένει έγκυρη.

Υπάρχουν πολλά σχήματα ψηφιακών υπογραφών που ανταποκρίνονται σε αυτά τα κριτήρια και τις προϋποθέσεις, αλλά θα εξετάσουμε μόνο μερικά από τα πιο δημοφιλή από αυτά.

4.1 Σχήμα Ψηφιακής Υπογραφής RSA

Το κρυπτοσύστημα δημόσιου κλειδιού RSA παρέχει ένα κρυπτογραφικά ασφαλές σχήμα ψηφιακής υπογραφής (υπογραφή και επαλήθευση), το οποίο βασίζεται στα μαθηματικά των modular exponentiations, των διακριτών λογαρίθμων και στη δυσκολία του προβλήματος παραγοντοποίησης ακεραίων αριθμών. Η διαδικασία υπογραφής και επαλήθευσης λειτουργεί ως εξής:

Ο αλγόριθμος υπογραφής RSA υπολογίζει έναν κατακερματισμό μηνύματος και στη συνέχεια κρυπτογραφεί τον κατακερματισμό με τον εκθέτη του ιδιωτικού κλειδιού για να αποκτήσει την υπογραφή. Η λαμβανόμενη υπογραφή είναι ένας ακέραιος αριθμός.

Ο αλγόριθμος επαλήθευσης RSA υπολογίζει πρώτα το κατακερματισμό του μηνύματος, στη συνέχεια αποκρυπτογραφεί την υπογραφή του μηνύματος με τον εκθέτη του δημόσιου κλειδιού και συγκρίνει τον αποκτηθέντα αποκρυπτογραφημένο κατακερματισμό με τον κατακερματισμό του υπογεγραμμένου μηνύματος για να εξασφαλίσει ότι η υπογραφή είναι έγκυρη.

Οι υπογραφές RSA είναι ντετερμινιστικές που σημαίνει ότι το ίδιο μήνυμα με το ίδιο ιδιωτικό κλειδί παράγουν την ίδια υπογραφή.

Για την δημιουργία ενός ζεύγους κλειδιών (δημοσίου και ιδιωτικού) στον RSA μια οντότητα Α πρέπει:

Δημιουργία Κλειδιών

Επιλέγουμε δυο μεγάλους πρώτους αριθμούς p και q με (κατά προσέγγιση) ίδιο μήκος.

- Υπολογίζουμε το γινόμενο τους $n = pq$.
- Υπολογίζουμε $t = (p - 1)(q - 1)$.
- Διαλέγουμε τυχαία έναν ακέραιο e που είναι σχετικά πρώτος με τον t, δηλαδή $1 < e < t$ και $\gcd(e, t) = 1$.
- Υπολογίζουμε, κάνοντας χρήση του εκτεταμένου αλγόριθμου του Ευκλείδη, τον (μοναδικό) ακέραιο d, τέτοιον ώστε $1 < d < t$ και $ed = 1 \bmod t$.

Το δημόσιο κλειδί του Α είναι το ΕΑ = (n, e) και το DA = d αντίστοιχα ιδιωτικό του κλειδί. Οι e και d καλούνται σαν εκθέτες κρυπτογράφησης και αποκρυπτογράφησης, ο n είναι το υπόλοιπο (modulus), και οι d και n είναι σχετικά πρώτοι. Εφόσον πραγματοποιηθεί η δημιουργία των κλειδιών, τα p, q δεν είναι πλέον αναγκαίοι και χρειάζεται να διαγραφούν μόλις είναι διαθέσιμα τα ΕΑ και DA. Αν δυο οντότητες Α και Β χρειαστεί να διασφαλίσουν την επικοινωνία τους, η Α πρέπει να βρει το ΕΒ, το δημόσιο κλειδί της Β, και αντίθετα (Παπαδημητράτος, n.d.).

Η οντότητα Α κρυπτογραφεί ένα μήνυμα m για την οντότητα Β με τον εξής τρόπο:

Κρυπτογράφηση

- Αναπαράστησε το m ως ακέραιο(ους) στο διάστημα [0, n − 1], κόβοντας το m σε ένα αριθμό από τμήματα, m_i , τέτοια ώστε $0 < m_i < n - 1$. Αν $m < n - 1$, προφανώς, το m είναι το μόνο τμήμα.
- Χρησιμοποιώντας το $E_B = (n, e)$, υπολόγισε το κρυπτογράφημα $c_i = m^e_i \bmod n$ για κάθε m_i.
- Στείλε κάθε ένα από τα κρυπτογραφήματα c_i στην B.

Στην συνέχεια, η B οντότητα αποκρυπτογραφεί κάθε ένα από τα c_i που λαμβάνει χρησιμοποιώντας το $D_B = d$:

Αποκρυπτογράφηση

Υπολόγισε το $c^d_i \bmod n = m_i$.

Η δημιουργία και επιβεβαίωση μιας υπογραφής RSA για το m είναι στην ουσία ίδια με την κρυπτογράφηση και αποκρυπτογράφηση του m. Σε αυτό που διαφέρει είναι ότι ο υπογράφων κρυπτογραφεί το m κάνοντας χρήση του ιδιωτικού του κλειδιού , και η άλλη οντότητα επιβεβαιώνει την υπογραφή πάνω στο m χρησιμοποιώντας το δημόσιο κλειδί του υπογράφοντος. Όπως προαναφέρθηκε οι υπογραφές είναι ντετερμινιστικές επιτρέποντας την ανάκτηση του μηνύματος. Πρακτικά όμως, το σχήμα RSA χρησιμοποιείται ως υπογραφή με προσθήκη, δηλαδή η υπογραφή υπολογίζεται όχι πάνω στο m αλλά σε μια σύνοψη του m. Ο υπογράφων, A, εκτελεί τα παρακάτω βήματα για να υπολογίσει την υπογραφή του, SA, πάνω σε ένα μήνυμα m, χρησιμοποιώντας μια μονόδρομη συνάρτηση σύνοψης h (με εξόδους στο διάστημα [0, n − 1]):

Δημιουργία Υπογραφής

- Υπολογίζουμε το $H = h(m)$.
- Υπολογίζουμε το $SA = H^d \bmod n$.

Οποιαδήποτε οντότητα, B, η οποία γνωρίζει το δημόσιο κλειδί του υπογράφοντος, EA, μπορεί να επιβεβαιώσει την υπογραφή SA πάνω στο m:

Επιβεβαίωση Υπογραφής

- Υπολογίζουμε το $S^e \bmod n = H$.
- Υπολογίζουμε το $H' = h(m)$.
- Συγκρίνουμε το H' με το H.
- Αν είναι ίσα, αποδεχόμαστε την SA.
- Αν όχι, την απορρίπτουμε .

4.2 Σχήμα Ψηφιακής Υπογραφής ElGamal

Το σχήμα υπογραφής ElGamal είναι ένα από τα πρώτα σχήματα ψηφιακών υπογραφών που βασίζεται σε ένα αριθμητικό modulo ενός πρώτου αριθμού. Μπορεί να θεωρηθεί ως πρόγονος του προτύπου ψηφιακής υπογραφής και του σχήματος υπογραφής Schnorr. Οι υπογραφές ElGamal είναι πολύ μεγαλύτερες από τις υπογραφές DSS και Schnorr. Ως αποτέλεσμα, αυτό το σχήμα υπογραφών δεν χρησιμοποιείται συχνά και παρουσιάζει ενδιαφέρον κυρίως για ιστορικούς λόγους.

Για να επιτευχθεί η δημιουργία κλειδιών, κάθε οντότητα, A, τρέχει τον παρακάτω βασικό αλγόριθμο για του σχήματος ElGamal:

Δημιουργία κλειδιών

- Επιλέγουμε έναν μεγάλο μεγέθους πρώτο αριθμό, p, και ένα γεννήτορα, g, για μια ομάδα Z^*_p.
- Επιλέγουμε ένα τυχαίο αριθμό x, τέτοιον ώστε $1 \leq x \leq p - 2$.
- Υπολογίζουμε $y = g^x \bmod p$.

Το δημόσιο κλειδί του A είναι το $E_A = (p, g, y)$ και το ιδιωτικό του κλειδί είναι το $D_A = x$.

Για να επιτευχθεί η κρυπτογράφηση ενός μνήματος, m, για την B, η A αποκτά το E_B και εκτελεί τον παρακάτω αλγόριθμο:

Κρυπτογράφηση

- Αναπαράστησε το m με ένα σύνολο από τμήματα m_i το καθένα στο διάστημα $[0,p-1]$. Διαλέγουμε ένα τυχαίο ακέραιο, k, τέτοιον ώστε $1 \leq k \leq p-2$.
- Υπολογίζουμε τα $a = g^k \bmod p$ και $b = my^k \bmod p$.

Το κρυπτογράφημα για την B είναι το (a,b). Η B αποκρυπτογραφεί το (a,b), το οποίο είναι δυο φορές το μέγεθος του αρχικού μηνύματος, χρησιμοποιώντας το D_B και εκτελώντας:

Αποκρυπτογράφηση

- Υπολογίζουμε το $a^{p-1-x} \bmod p$.
- Υπολογίζουμε το $m = a^{-x}b \bmod p$.

Το "σπάσιμο" της κρυπτογράφησης ElGamal ισοδυναμεί με το να λυθεί το πρόβλημα του διακριτού λογάριθμου. Εκτός από αυτά, ο τυχαίος αριθμός k πρέπει να επιλεχθεί διαφορετικός και ανεξάρτητα για διαφορετικές κρυπτογραφήσεις. Αλλιώς, η πιθανή γνώση του μηνύματος μπορεί να οδηγήσει στην ανάκτηση άλλων μηνυμάτων που κρυπτογραφηθήκαν με το ίδιο k (Παπαδημητράτος, n.d.).

Η υπογραφή ElGamal είναι ένα τυχαίο σχήμα, και δημιουργεί υπογραφές με προσθήκη, χρησιμοποιώντας μονόδρομη συνάρτηση σύνοψης $h : \{0,1\}^* \longrightarrow Z_p$. για να υπογράψει ένα μήνυμα m οποιουδήποτε μήκους, ο A εκτελεί το παρακάτω αλγόριθμο με το ιδιωτικό του κλειδί, D_A:

Δημιουργία Υπογραφής

Επιλέγουμε ένα τυχαίο ακέραιο k, τέτοιον ώστε $1 \leq k \leq p-2$ και $\gcd(k,p-1) = 1$. Ο k πρέπει να κρατηθεί μυστικός.

- Υπολογίζουμε $r = g^k \bmod p$. Υπολόγισε $k-1 \bmod (p-1)$.
- Υπολογίζουμε $s = k^{-1}(h(m) - xr) \bmod (p-1)$.

Το ζεύγος (r,s) είναι η υπογραφή του A στο m. Οποιαδήποτε άλλη οντότητα που έχει το E_A μπορεί να επιβεβαιώσει την υπογραφή με τα βήματα παρακάτω:

Επιβεβαίωση Υπογραφής

- Επιβεβαιώνουμε ότι $1 \leq r \leq p-1$, αλλιώς, απέρριψε την υπογραφή. Υπολόγισε $u_1 = y^r r^s \bmod p$.
- Υπολογίζουμε $h(m)$.
- Υπολογίζουμε $u_2 = g^h(m) \bmod p$.
- Λέγουμε αν $u_1 = u_2$. Αν ναι, αποδεχόμαστε την υπογραφή.

Η επιβεβαίωση μιας υπογραφής ElGamal είναι σχετικά πιο αργή από αυτή μιας υπογραφής RSA με μικρό εκθέτη.

4.3 Σχήμα Ψηφιακής Υπογραφής DSA

Ο DSA (Digital Signature Algorithm) είναι ένα κρυπτογραφικά ασφαλές πρότυπο για ψηφιακές υπογραφές (υπογραφή μηνυμάτων και επαλήθευση υπογραφής), που βασίζεται στα μαθηματικά των modular exponentiations, των διακριτών λογαρίθμων και στη δυσκολία επίλυσης του προβλήματος του διακριτού λογαρίθμου (DLP). Αποτελεί εναλλακτική λύση του RSA και χρησιμοποιείται αντί αυτού. Το DSA αποτελεί παραλλαγή του σχήματος υπογραφής ElGamal.

Δημιουργία Κλειδιού

- Επιλέγουμε έναν πρώτο q τέτοιον ώστε $2^{N-1} < q < 2^N$.
- Επιλέγουμε έναν πρώτο p μήκους L bits, τέτοιον ώστε $q|p-1$.
- Επιλέγουμε ένα στοιχείο $h \in Z^*_p$ και υπολόγισε $g = h^{(p-1)/q} \bmod p$. Επαναλαμβάνουμε μέχρι $g \neq 1$ (δηλαδή, να είναι ο γεννήτορας του μοναδικής κυκλικής ομάδας τάξης q).
- Επιλέγουμε ένα τυχαίο ακέραιο x στο διάστημα $[1, q-1]$.
- Υπολογίζουμε το $y = g^x \bmod p$

Οι παράμετροι N και L μπορούν να πάρουν ένα από τέσσερα ζεύγη τιμών που προσδιορίζει η τυποποίηση, π.χ., $N = 160$ και $L = 1024$. Το δημόσιο κλειδί είναι $E_A = (p,q,g,y)$ και το ιδιωτικό είναι $D_A = x$. Οι *παράμετροι πεδίου του DSA*, p, q, g, δεν χρειάζεται να είναι μέρος του δημόσιου κλειδιού. Ο αλγόριθμος απαιτεί την δημιουργία ζεύγους κλειδιών με βάση τις παραμέτρους πεδίου, οι οποίες είναι δημόσια γνωστές. Όλες οι οντότητες πρέπει να είναι διασφαλισμένες ότι αυτές οι παράμετροι είναι έγκυρες. Με δημόσιες παραμέτρους πεδίου, μπορούμε να πούμε ότι $E_A = y$. Για να υπογράψει ένα μήνυμα m, μια οντότητα A που χρησιμοποιεί την SHA-1 συνάρτηση, την οποία συμβολίζουμε εδώ ως H, πρέπει:

Δημιουργία Υπογραφής

- Επιλέγουμε ένα τυχαίο ακέραιο, k, στο διάστημα $[1,q-1]$.
- Υπολογίζουμε το $r = (g^k \bmod p) \bmod q$.
- Υπολογίζουμε το $k^{-1} \bmod q$.
- Υπολογίζουμε το $s = k^{-1}(H(m) + xr) \bmod q$.
- Αν $s = 0$, τότε πηγαίνουμε στο αρχικό βήμα (επειδή $s = 0$ συνεπάγεται ότι το $s^{-1} \bmod q$, το οποίο χρειάζεται για την επιβεβαίωση της υπογραφής, δεν υπάρχει).

Η υπογραφή στο m είναι το ζεύγος ακεραίων (r,s). Πρέπει να σημειωθεί ότι , αν το k επιλεγεί εκ των προτέρων, πριν το m προς υπογραφή, τα k^{-1} και r (που είναι μέρη της υπογραφής) μπορούν να προ-υπολογιστούν. αλλά είναι απολύτως απαραίτητο να προστατευτούν με τον ίδιο τρόπο που διαφυλάσσεται το ιδιωτικό κλειδί (Παπαδημητράτος, n.d.).

Κάθε οντότητα, B, που ξέρει το E_A μπορεί να επιβεβαιώσει την υπογραφή (r,s) πάνω στο m ως εξής:

Επιβεβαίωση Υπογραφής

- Επιβεβαιώνουμε ότι τα r και s είναι ακέραιοι στο διάστημα $[1,q-1]$. Αν όχι, απέρριψε την υπογραφή.
- Υπολογίζουμε το $w = s^{-1} \bmod q$ και $H(m)$.
- Υπολογίζουμε το $u_1 = H(m)w \bmod q$ και $u_2 = rw \bmod q$.
- Υπολογίζουμε το $v = (g^{u_1}y^{u_2} \bmod p) \bmod q$.
- Αποδεχόμαστε την υπογραφή αν και μόνο αν $v = r$.

Το ιδιωτικό κλειδί για τον DSA έχει το ίδιο μέγεθος με το q, ενώ και τα r και s μέρη της υπογραφής έχουν και αυτά, το καθένα, το ίδιο μέγεθος. Το δημόσιο κλειδί έχει το ίδιο μέγεθος με το p.

4.4 Σχήμα Ψηφιακής Υπογραφής ECDSA

Ο αλγόριθμος ECDSA (αλγόριθμος ψηφιακής υπογραφής ελλειπτικής καμπύλης) είναι ένα κρυπτογραφικά ασφαλές σχήμα ψηφιακής υπογραφής, που βασίζεται στην κρυπτογραφία ελλειπτικής καμπύλης (ECC). Ο ECDSA βασίζεται στα μαθηματικά των κυκλικών ομάδων ελλειπτικών καμπυλών πάνω σε πεπερασμένα πεδία και στη δυσκολία του προβλήματος ECDLP.

Ο ECDSA αποτελεί τροποποίηση του κλασικού αλγορίθμου DSA, ο οποίος προέρχεται από το σχήμα υπογραφής ElGamal. Πιο συγκεκριμένα, ο αλγόριθμος ECDSA είναι μια παραλλαγή της υπογραφής ElGamal, με ορισμένες αλλαγές και βελτιστοποιήσεις για τον χειρισμό της αναπαράστασης των στοιχείων της ομάδας (τα σημεία της ελλειπτικής καμπύλης).

Όπως κάθε άλλος αλγόριθμος κρυπτογράφησης ελλειπτικής καμπύλης, ο ECDSA χρησιμοποιεί μια ελλειπτική καμπύλη , ιδιωτικό κλειδί (τυχαίος ακέραιος αριθμός εντός του μήκους κλειδιού της καμπύλης, για την υπογραφή μηνυμάτων) και ένα δημόσιο κλειδί (σημείο EC, που υπολογίζεται από το ιδιωτικό κλειδί πολλαπλασιάζοντάς το με το σημείο γεννήτριας της καμπύλης για την επαλήθευση υπογραφών).

Μια οντότητα, *A*, πρέπει να:

Δημιουργία Κλειδιών

- Επιλέγουμε μια ελλειπτική καμπύλη, *E*, ορισμένη πάνω στο Z_p, τέτοια ώστε ο αριθμός των σημείων στην $E(Z_p)$ να διαιρείται έναν μεγάλο πρώτο αριθμό *n*.
- Επιλέγουμε ένα σημείο $P \in E(Z_p)$ τάξης *n*.
- Επιλέγουμε ένα τυχαίο ακέραιο $d \in [1, n-1]$.
- Υπολογίζουμε το $Q = dP$.

Το δημόσιο κλειδί είναι το $E_A = (E,P,n,Q)$ και το ιδιωτικό κλειδί είναι το $D_A = d$. Με *E, P, n* δημόσια γνωστές παραμέτρους, το δημόσιο κλειδί είναι το $E_A = Q$.

Να σημειωθεί ότι το *d* και το *k* χρειάζονται για την δημιουργία υπογραφής και δεν είναι απλώς τυχαίοι αλλά ονομάζονται, για την ακρίβεια, στατιστικά μοναδικοί και απρόβλεπτοι. Για την υπογραφή ενός μηνύματος *m*, μια οντότητα *A* κάνει τα παρακάτω (με το *H* να είναι η SHA-1):

Δημιουργία Υπογραφής

- Επιλέγουμε ένα τυχαίο ακέραιο, k, στο διάστημα $[1,n-1]$.
- Υπολογίζουμε το $kP = (x_1,y_1)$ και το $r = x_1 \bmod n$. Αν $r = 0$ πήγαινουμε στο αρχικό βήμα (Αν $r = 0$, η εξίσωση υπογραφής (Βήμα 4) δεν περιλαμβάνει το ιδιωτικό κλειδί).
- Υπολογίζουμε το $k^{-1} \bmod n$.
- Υπολογίζουμε το $s = k^{-1}(H(m) + dr) \bmod n$.
- Αν $s = 0$, πήγαινουμε στο αρχικό βήμα (Επειδή $s = 0$ σημαίνει ότι το $s^{-1} \bmod n$, που χρειάζεται για την επιβεβαίωση της υπογραφής, δεν υπάρχει).
- Η υπογραφή στο m είναι το ζεύγος (r,s). Κάθε οντότητα B που ξέρει το E_A κάνει τα παρακάτω για να επιβεβαιώσει την (r,s) για το m:

Επιβεβαίωση Υπογραφής

- Επιβεβαιώνουμε ότι τα r και s είναι ακέραιοι στο $[1,n-1]$. Αν όχι, απορρίπτουμε την υπογραφή.
- Υπολογίζουμε το $w = s^{-1} \bmod n$ και το $H(m)$.
- Υπολογίζουμε το $u_1 = H(m)w \bmod n$ και το $u_2 = rw \bmod n$.
- Υπολογίζουμε το $u_1P + u_2Q = (x_0,y_0)$ και το $v = x_0 \bmod n$.
- Αποδεχόμαστε την υπογραφή αν και μόνο αν $v = r$.

Για να εξασφαλίσουμε επίπεδο ασφάλειας παρόμοιο με του DSA (με N = 160-bit q και L = 1024- bit p), το n για τον ECDSA πρέπει να είναι 160 bits με μέγεθος.

Τότε, οι υπογραφές του DSA και του ECDSA θα έχουν το ίδιο μέγεθος, δηλαδή 320 bits. Κάνοντας σύγκριση με το DSA, παρατηρούμε ότι το ECDSA έχει την ίδια εξίσωση για την δημιουργία υπογραφής, και ότι και οι τα δυο σχήματα χρησιμοποιούν SHA-1 (Παπαδημητράτος, n.d.).

5

Ψηφιακά πιστοποιητικά

5.1 Ο ρόλος των ψηφιακών πιστοποιητικών

Το ψηφιακό πιστοποιητικό είναι ένα αρχείο ή ηλεκτρονικός κωδικός πρόσβασης που αποδεικνύει την αυθεντικότητα μιας συσκευής, διακομιστή ή χρήστη μέσω της χρήσης κρυπτογραφίας και της υποδομής δημόσιου κλειδιού (PKI).

Ο έλεγχος ταυτότητας ψηφιακού πιστοποιητικού βοηθά τους οργανισμούς να διασφαλίζουν ότι μόνο αξιόπιστες συσκευές και χρήστες μπορούν να συνδεθούν στα δίκτυά τους. Μια άλλη κοινή χρήση των ψηφιακών πιστοποιητικών είναι η επιβεβαίωση της αυθεντικότητας ενός ιστότοπου σε ένα πρόγραμμα περιήγησης ιστού, το οποίο είναι επίσης γνωστό ως στρώμα ασφαλών υποδοχών ή πιστοποιητικό SSL.

Ένα ψηφιακό πιστοποιητικό περιέχει αναγνωρίσιμες πληροφορίες, όπως όνομα χρήστη, εταιρεία ή τμήμα και διεύθυνση πρωτοκόλλου Internet (IP) ή σειριακό αριθμό συσκευής. Τα ψηφιακά πιστοποιητικά περιέχουν ένα αντίγραφο ενός δημόσιου κλειδιού από τον κάτοχο του πιστοποιητικού, το οποίο πρέπει να αντιστοιχιστεί με ένα αντίστοιχο ιδιωτικό κλειδί για να επαληθευτεί ότι είναι αληθινό.

Ένα πιστοποιητικό δημόσιου κλειδιού εκδίδεται από τις αρχές έκδοσης πιστοποιητικών (CA), οι οποίες υπογράφουν πιστοποιητικά για να επαληθεύσουν την ταυτότητα της συσκευής ή του χρήστη που ζητά.

Ψηφιακά πιστοποιητικά μπορούν να ζητηθούν από άτομα, οργανισμούς και ιστότοπους. Για να γίνει αυτό, παρέχουν τις πληροφορίες που πρέπει να επικυρωθούν και ένα δημόσιο κλειδί μέσω ενός αιτήματος υπογραφής πιστοποιητικού. Οι πληροφορίες επικυρώνονται από μια δημόσια αξιόπιστη ΑΠ (αρχή πιστοποίησης), η οποία τις υπογράφει με ένα κλειδί που παρέχει μια αλυσίδα εμπιστοσύνης στο πιστοποιητικό.

Αυτό επιτρέπει στο πιστοποιητικό να αξιοποιείται ως αποδεικτικό γνησιότητας σε ένα έγγραφο, για τον έλεγχο ταυτότητας πελάτη ή για την παροχή απόδειξης των διαπιστευτηρίων ενός ιστότοπου.

Υπάρχουν τρεις διαφορετικοί τύποι πιστοποιητικών δημόσιου κλειδιού: ένα πιστοποιητικό ασφάλειας επιπέδου μεταφοράς (TLS)/πιστοποιητικό SSL, ένα πιστοποιητικό υπογραφής κώδικα και ένα πιστοποιητικό πελάτη.

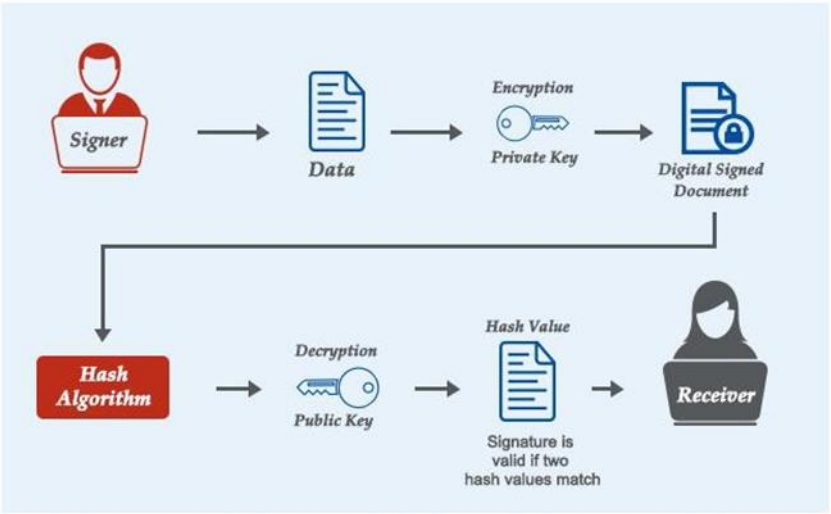
5.2 Είδη Ψηφιακών υπογραφών

Στο ψηφιακό κόσμο, οι ψηφιακές υπογραφές κάνουν χρήση της κρυπτογραφίας δημοσίου κλειδιού, στην οποία αποστολέας και παραλήπτης κατέχουν έκαστος από ένα ιδιωτικό και ένα δημόσιο κλειδί.

Στα κλειδιά μεταξύ τους υπάρχει ένας μαθηματικός συσχετισμός, το δημόσιο κλειδί χρησιμοποιείται στην επαλήθευση της υπογραφής και το ιδιωτικό στην δημιουργία της και αυτή είναι και η κύρια διαφορά σε σχέση με τη κρυπτογράφηση. Στη περίπτωση όπου ένας τρίτος γνωρίζει το ένα κλειδί θεωρείται ανέφικτο να γίνει ο υπολογισμός του δεύτερου.

Η έννοια της συνάρτησης κατακερματισμού σχετίζεται με τη διαδικασία δημιουργίας αλλά και με την διαδικασία επαλήθευσης της υπογραφής. Η εφαρμογή της συγκεκριμένης συνάρτησης έχει ως αποτέλεσμα την παραγωγή της «σύνοψης» ενός μηνύματος ανεξάρτητου μεγέθους, όπου η σύνοψη αποτελεί μια ακολουθία από bits με συγκεκριμένο μέγεθος. Η σύνοψη ενός μηνύματος αποτελεί μια μοναδική ψηφιακή αναπαράσταση του μηνύματος που το αντιπροσωπεύει.

Από την σύνοψη η οποία δημιουργείται δεν καθίσταται δυνατόν να πραγματοποιηθεί η εξαγωγή του αρχικού μηνύματος , οπότε η συνάρτηση κατακερματισμού θεωρείται μονόδρομη. Υπάρχει εξαιρετικά μικρή πιθανότητα μεταξύ δύο μηνυμάτων να προκύψει η ίδια σύνοψη. Αυτό υποδηλώνει ότι στην περίπτωση που υπάρχει διαφορά κατά την διαδικασία σύνοψης μεταξύ του αποστολέα και του παραλήπτη χρησιμοποιώντας πάντα την ίδια συνάρτηση κατακερματισμού, τότε το μήνυμα αλλοιώνεται κατά τη μετάδοση του, συνεπώς δεν υπάρχει ακεραιότητα. Η ηλεκτρονική υπογραφή ουσιαστικά αποτελεί την σύνοψη του αποστολέα κρυπτογραφημένη με το ιδιωτικό του κλειδί. Αντίθετα με τις ιδιόχειρες υπογραφές η ψηφιακή υπογραφή διαφέρει για κάθε μήνυμα.



Σχήμα 13: Ψηφιακή υπογραφή

Στη παραπάνω εικόνα βλέπουμε το σενάριο στο οποίο η ψηφιακή υπογραφή λειτουργεί ως ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος. Έστω ότι ο αποστολέας έχει στην κατοχή του ένα συγκεκριμένο ζεύγος κλειδιών, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί την ταυτότητα του αποστολέα.

5.2.1 Ψηφιακή Υπογραφή Φυσικού Προσώπου

Ο συγκεκριμένος τύπος ηλεκτρονικής υπογραφής εκδίδεται εξολοκλήρου για φυσικά πρόσωπα και έχει νομική ισχύ ισάξια με αυτή της ιδιόχειρης υπογραφής. Για να πραγματοποιηθεί η έκδοση της ταυτοποιούνται τα στοιχεία του φυσικού προσώπου και μπορεί να τη χρησιμοποιεί σε οποιαδήποτε ηλεκτρονική συναλλαγή επιθυμεί ή απαιτείται να δεσμεύεται νομικά. Επίσης μπορεί να ανακληθεί κατόπιν αιτήματος του φυσικού προσώπου.

5.2.2 Ψηφιακή Υπογραφή Φυσικού Προσώπου που σχετίζεται με Νομικό Πρόσωπο

Ο συγκεκριμένος τύπος ηλεκτρονικής υπογραφής εκδίδεται σε νόμιμους εκπροσώπους εταιρειών ή σε εξουσιοδοτημένα από τον νόμιμο εκπρόσωπο φυσικά πρόσωπα τα οποία μπορούν να υπογράφουν ηλεκτρονικά έγγραφα που σχετίζονται με την εταιρεία.

Ταυτοποιείται το Νομικό πρόσωπο, ο νόμιμος εκπρόσωπος (Συνδρομητής) καθώς και το υποκείμενο (αν είναι διαφορετικό πρόσωπο). Το Νομικό Πρόσωπο κατέχει τα πλήρη δικαιώματα του πιστοποιητικού το οποίο εκδίδεται ή ανακαλείται κατόπιν αιτήματος του ή και του Υποκειμένου. Σε περίπτωση αποχώρησης ενός υπαλλήλου του νομικού προσώπου, μπορεί εύκολα να ανακληθεί από το νομικό πρόσωπο και να εκδοθεί για λογαριασμό κάποιου άλλου υπαλλήλου.

5.2.3 Ψηφιακή σφραγίδα για Νομικά Πρόσωπα

Ο συγκεκριμένος τύπος ηλεκτρονικής υπογραφής όπου στην πραγματικότητα είναι ψηφιακή σφραγίδα εκδίδεται σε μόνο για εταιρείες ή νομικές οντότητες με το συγκεκριμένο πιστοποιητικό μπορεί να υπογράφει κάθε νόμιμος εκπρόσωπος ή εξουσιοδοτημένος υπάλληλός.

Ταυτοποιείται το Νομικό πρόσωπο, ο νόμιμος εκπρόσωπος (Συνδρομητής) καθώς και το υποκείμενο (αν είναι διαφορετικό πρόσωπο), επίσης θα πρέπει να προσκομισθούν ηλεκτρονικά έγγραφα που σχετίζονται με την εταιρεία. Το Νομικό Πρόσωπο κατέχει τα πλήρη δικαιώματα του πιστοποιητικού το οποίο εκδίδεται ή ανακαλείται κατόπιν αιτήματος του ή του Νόμιμου Εκπροσώπου.

5.3 Ευρωπαϊκός Κανονισμός eIDAS

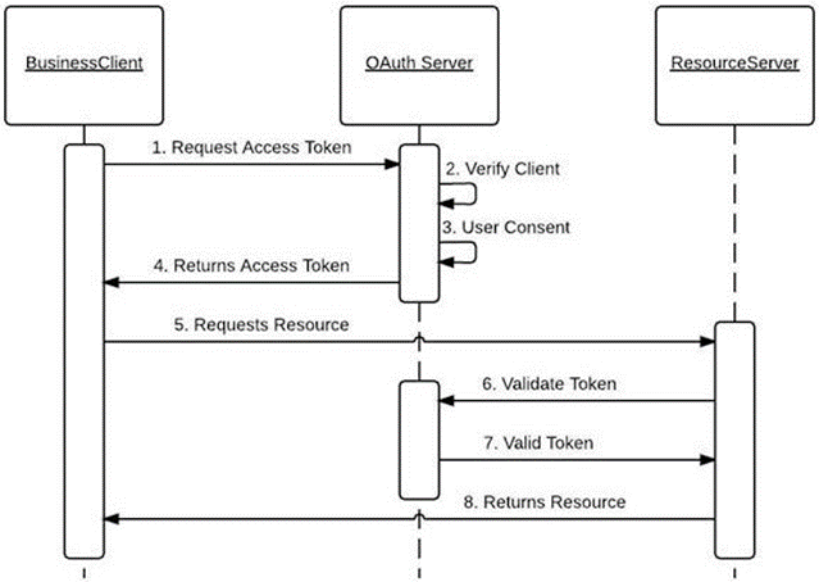
Ο όρος eIDAS σημαίνει «Ηλεκτρονική Ταυτοποίηση» (eID) και «Υπηρεσίες Εμπιστοσύνης» (AS). Πρόκειται για έναν ευρωπαϊκό κανονισμός ο οποίος εγκρίθηκε το 2014, κύριο μέλημα του είναι η εισαγωγή ενός ενιαίου πλαισίου τόσο για τις υπηρεσίες ηλεκτρονική ταυτοποίησης αλλά και τις υπηρεσίες εμπιστοσύνης. Καθιστώντας πιο απλή την παροχή επιχειρηματικών υπηρεσιών σε ολόκληρη την ΕΕ, θεσπίζοντας έτσι τη διαλειτουργικότητα μεταξύ των 28 χωρών της ΕΕ και την διασφάλιση ότι οι χώρες αμοιβαία αναγνωρίζουν η μία την άλλη όσο αφορά τις υπηρεσίες ηλεκτρονικής ταυτοποίησης και εμπιστοσύνης διασυνοριακά.

Ηλεκτρονική Ταυτοποίηση – eID

Η ηλεκτρονική ταυτοποίηση (ή eID) αποτελεί μια ψηφιακή λύση, η οποία παρέχει απόδειξη ταυτότητας σε πολίτες ή οργανισμούς, για την πρόσβαση σε διαδικτυακές υπηρεσίες ή τη διεξαγωγή διαδικτυακών συναλλαγών. Αυτό προαπαιτεί την ύπαρξη ενός πλαισίου ελέγχου ταυτότητας και αξιοπιστίας. Μερικές τεχνολογίες και πρωτόκολλα που χρησιμοποιούνται για αυτό το σκοπό είναι τα παρακάτω,

OAuth 2.0 - Το OAuth 2.0 είναι ένα πρωτόκολλο ανοιχτού προτύπου βασισμένο σε διακριτικά (tokens) για εξουσιοδότηση μέσω διαδικτύου. Το συγκεκριμένο πρωτόκολλο παρέχει στις εφαρμογές των πελατών ασφαλή εξουσιοδοτημένη πρόσβαση. Το OAuth λειτουργεί μέσω πρωτοκόλλου μεταφοράς υπερκειμένου (HTTP) και εξουσιοδοτεί συσκευές, API, διακομιστές και εφαρμογές με διακριτικά πρόσβασης και όχι διαπιστευτήρια. Η συγκεκριμένη τεχνολογία επιτρέπει στους χρήστες να εξουσιοδοτούν την ταυτότητά τους σε υπηρεσίες τρίτων, χωρίς να χρειάζεται να κάνουν κοινή χρήση των διαπιστευτηρίων τους. Το OAuth 2.0 υποθέτει ότι ο χρήστης έχει πιστοποιηθεί ήδη από την εφαρμογή στην οποία είχε δημιουργηθεί ο λογαριασμός του και δεν καθορίζεται ο τρόπος με τον οποίο πρέπει να πραγματοποιείται ο έλεγχος ταυτότητας. Όταν ένας χρήστης έχει πρόσβαση σε υπηρεσίες με ένα διακριτικό OAuth, οι υπηρεσίες δεν χρειάζεται να γνωρίζουν ποιος είναι ο χρήστης. Ο πάροχος ταυτότητας το καθιστά δυνατό, εκδίδοντας ένα διακριτικό στην εφαρμογή τρίτου μέρους με το έγκριση του χρήστη.

Το User – Managed Access (UMA) είναι μια επέκταση OAuth 2.0 που καθορίζει τον τρόπο ελέγχου των δεδομένων των χρηστών. Οι χρήστες έχουν την δυνατότητα να επιλέξουν ποιος θα μπορεί να έχει προσβασιμότητα στα δεδομένα του, τι είδους δεδομένα πρόκειται να μοιραστεί και για πόσο χρονικό διάστημα η πρόσβαση θα είναι δυνατή στα συγκεκριμένα δεδομένα.



Σχήμα 14: OAuth 2.0

Τα θετικά σημεία για τη συγκεκριμένη λύση είναι τα παρακάτω:

- Τα διακριτικά OAuth 2.0 επιτρέπουν την εύκολη ενσωμάτωση υπηρεσιών ιστού μέσω APIs χωρίς την ανάγκη χρήσης των διαπιστευτηρίων πελατών. Ο μηχανισμός επιτρέπει στους χρήστες να μοιράζονται τα στοιχεία του λογαριασμού τους με εφαρμογές ή ιστότοπους τρίτων.

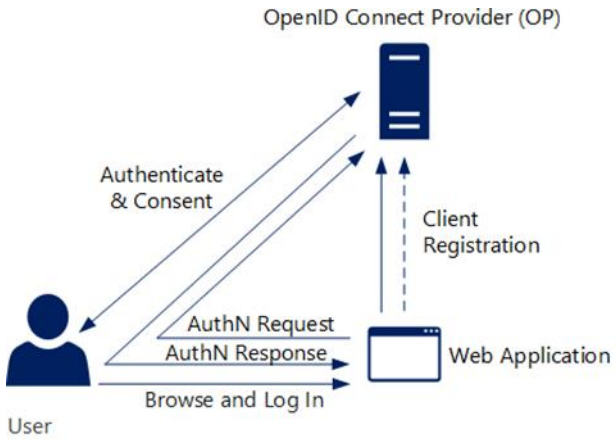
- Η συγκεκριμένη λύση δεν αποθηκεύει δεδομένα και διαπιστευτηρίων χρηστών/πελατών.

Τα αρνητικά σημεία είναι τα παρακάτω:

- Η απόδοση της λύσης αναλογικά με τον αριθμό των αιτημάτων που είναι σε θέση να χειριστεί εξαρτάται από την διαμόρφωση του διακομιστή. Επιπλέον υπάρχει εξάρτηση με την αποδοτικότητα διαχείρισης αιτημάτων από τρίτου μέρους διακομιστές.

- Σχετικά με την ασφάλεια, το OAuth2.0 επικυρώνει μόνο την προέλευση και την ακεραιότητα του διακριτικού, για παράδειγμα στην περίπτωση ενός «κλεμμένου» διακριτικού η διαδικασία μπορεί να συνεχιστεί κανονικά

OpenID Connect - Το OpenID Connect παρέχει ένα πλαίσιο για τη δημιουργία λειτουργικών και ασφαλών συστημάτων ελέγχου ταυτότητας. Είναι ένα ανοιχτό πρότυπο για έλεγχο ταυτότητας, το οποίο είναι σχεδιασμένο να λειτουργεί συνδυαστικά με τις δυνατότητες εξουσιοδότησης του OAuth 2.0. Στην ουσία είναι ένα επίπεδο ασφάλειας ταυτότητας χτισμένο πάνω από το OAuth 2.0, επιτρέποντας την επαλήθευση της ταυτότητας ενός τελικού χρήστη καθώς και τη λήψη βασικών πληροφοριών προφίλ για τον χρήστη. Αυτό επιτυγχάνεται προσθέτοντας ένα διακριτικό ταυτότητας στην εξουσιοδότηση OAuth 2.0. Η διαφορά μεταξύ του OAuth 2.0 και του OpenID Connect είναι ότι το OAuth 2.0 είναι πρωτίστως ένα πρωτόκολλο ανάθεσης πρόσβασης, μέσω του οποίου οι χρήστες παρέχουν άδεια ή δικαιώματα πρόσβασης στον αιτούντα πελάτη. Το πρωτόκολλο OpenID Connect βασίζεται στις προδιαγραφές OAuth 2.0, με ένα πρόσθετο διακριτικό ID που παρέχει πληροφορίες σχετικά με τον χρήστη (όπως πώς και πότε έγινε έλεγχος ταυτότητας του χρήστη).



Σχήμα 15: OpenID

Τα θετικά σημεία για τη συγκεκριμένη λύση είναι τα παρακάτω:

• Το OpenID Connect επιτρέπει στους προγραμματιστές να πραγματοποιούν έλεγχο ταυτότητας ατόμων σε ιστότοπους και εφαρμογές χωρίς να χρειάζεται οι προγραμματιστές και οι εφαρμογές να κατέχουν και να διαχειρίζονται κωδικούς πρόσβασης. Η τεχνολογία επιτρέπει έτσι την εύκολη χρήση ψηφιακών ταυτοτήτων σε ιστότοπους και εφαρμογές μέσω οποιασδήποτε πληροφορικής ή κινητή συσκευή.

• Επειδή το OpenID Connect διαθέτει ένα ενσωματωμένο επίπεδο ασφαλείας πάνω από το διακριτικό OAuth 2.0, αναιρεί την εξάρτηση από εξουσιοδοτήσεις τρίτων- αυξάνοντας τον αριθμό των αιτημάτων που η τεχνολογία μπορεί να χειριστεί.

Τα αρνητικά σημεία είναι τα παρακάτω:

• Η δημιουργίας μια υποδομής βασισμένη στο OpenID Connect προϋποθέτει ένα διακομιστή δεδομένων μαζί με ένα ισχυρό σύστημα ασφάλειας με απώτερο σκοπό την ασφάλιση αποθήκευση των δεδομένων αυτών. Αυτό ισοδυναμεί με κόστος λογισμικού και υλικού, επομένως είναι ένας σημαντικός παράγοντας.

SAML - Το SAML (Security Assertion Markup Language), εντάσσεται στα ανοιχτά πρότυπα και είναι βασισμένο στο Extensible Markup Language (XML). Αυτό το πρωτόκολλο υποστηρίζει την ανταλλαγή πληροφοριών εξουσιοδότησης και ελέγχου ταυτότητας μέσω διαδικτυακών υπηρεσιών (Web Services). Πρόσβαση μπορούν να έχουν οι τελικοί χρήστες σε αποκλειστικό περιεχόμενο σε πολλούς ιστότοπους ή εφαρμογές. Το οικοσύστημα SAML συντίθεται από δύο μέρη, το υποστηρικτικό μέρος και το επικουρικό μέρος SAML.

Η τεχνολογία SAML περιλαμβάνει τα ακόλουθα στοιχεία:

- Ισχυρισμός (Assertion). Το υποστηρικτικό μέρος επιβεβαιώνει πληροφορίες ασφαλείας με τη μορφή δηλώσεων σχετικά με ένα θέμα. Ένας ισχυρισμός περιέχει κάποιες βασικές απαιτούμενες και προαιρετικές πληροφορίες που ισχύουν για όλες τις δηλώσεις και συνήθως περιέχει το θέμα και τις προϋποθέσεις που χρησιμοποιούνται για την επικύρωση του ισχυρισμού.

- Πρωτόκολλα (Protocols). Αυτά περιλαμβάνουν κανόνες αιτήματος/απόκρισης για την εκτέλεση εργασιών, όπως έλεγχο ταυτότητας, αποσύνδεση, ερώτημα επιβεβαίωσης κ.α.

Δεσμεύσεις (Bindings). Αυτά περιγράφουν πώς μπορούν να μεταφερθούν μηνύματα πρωτοκόλλου SAML στα υποκείμενα πρωτόκολλα μεταφοράς

Σχήμα 16: SAML

Τα θετικά σημεία για τη συγκεκριμένη λύση είναι τα παρακάτω:

• Η τεχνολογία χρησιμοποιείται εδώ και λίγο καιρό και έχει εφαρμοστεί με επιτυχία σε πολλές κυβερνητικές και εταιρικές υλοποιήσεις , αποδεικνύοντας ευρεία αποδοχή αυτού του πρωτοκόλλου.
• Εύκολη υιοθέτηση

Τα αρνητικά σημεία είναι τα παρακάτω:

• Η τεχνολογία είναι ευάλωτη σε πολλές διαφορετικές απειλές (spoofing DNS, hijack SAML Token)

5.4 Υπηρεσίες Εμπιστοσύνης – Trust Services

Σύμφωνα με τον κανονισμό eIDAS, οι υπηρεσίες εμπιστοσύνης είναι ηλεκτρονικές υπηρεσίες που στοχεύουν στην ενίσχυση της εμπιστοσύνης των οργανισμών και των πολιτών της ΕΕ κατά την πραγματοποίηση ηλεκτρονικών συναλλαγών. Ιδίως εκείνων που πραγματοποιούνται μεταξύ επιχειρήσεων και πελατών που βρίσκονται σε άλλη χώρα της ΕΕ (Enisa, 2014).

Σύμφωνα με τον κανονισμό eIDAS, οι υπηρεσίες εμπιστοσύνης περιλαμβάνουν:

- **Ηλεκτρονική υπογραφή (eSignature):** είναι η έκφραση σε ηλεκτρονική μορφή της συμφωνίας ενός ατόμου για το περιεχόμενο ενός εγγράφου ή συνόλου δεδομένων. Οι πιστοποιημένες ηλεκτρονικές υπογραφές έχουν το ίδιο νομικό αποτέλεσμα με τις χειρόγραφες υπογραφές.

- **Ηλεκτρονική σφραγίδα (eSeal):** είναι ισοδύναμο μιας σφραγίδας που εισάγεται σε ένα έγγραφο για να πιστοποιήσει την ακεραιότητα και την προέλευσή του.

- **Ηλεκτρονική χρονική σήμανση (eTimestamp):** αποδεικνύει ότι ένα έγγραφο υπήρχε σε μια χρονική στιγμή

- **Ηλεκτρονική Καταχωρημένη Υπηρεσία Παράδοσης (eDelivery):** μια υπηρεσία που επιτρέπει την ηλεκτρονική μεταφορά δεδομένων μεταξύ επιχειρήσεων, δημόσιων διοικήσεων και πολιτών. Παρέχει απόδειξη αποστολής και λήψης των δεδομένων και προστατεύει από τον κίνδυνο απώλειας, κλοπής, ζημιάς ή μη εξουσιοδοτημένων αλλαγών

- **Πιστοποιητικά ελέγχου ταυτότητας ιστότοπου (WAC):** ηλεκτρονικά πιστοποιητικά που εκδίδονται για να αποδείξουν στους χρήστες (π.χ. πολίτες και ΜΜΕ) ότι ένα φυσικό ή νομικό πρόσωπο κατέχει έναν ισότοπο.

5.4.1 Εγκεκριμένες και μη- Εγκεκριμένες Υπηρεσίες Εμπιστοσύνης

Με τον όρο, 'εγκεκριμμένος' ορίζουμε ένα πιστοποιημένο πάροχο υπηρεσιών εμπιστοσύνης ο οποίος είναι διαπιστευμένος να εκδίδει υπηρεσίες εμπιστοσύνης που πληρούν τις απαιτήσεις του κανονισμού eIDAS. Αντίθετα με τον όρο 'μη-εγκεκριμένος' ορίζονται οι παρόχοι που συχνά προσφέρουν λύσεις παρόμοιες με τους εγκεκριμμένους αλλά δεν έχουν περάσει από την επίσημη διαδικασία για να διασφαλίσουν ότι οι υπηρεσίες που παρέχονται από τους ίδιους πληρούν τις απαιτήσεις που καθορίζονται στον Κανονισμό eIDAS. Δεν είναι απαραίτητα λιγότερο αξιόπιστα, αλλά δεν είναι εγγυημένη η κανονιστική εποπτεία από το eIDAS.

5.5 Pretty Good Privacy (PGP)

Το Pretty Good Privacy (PGP) αναφέρεται σε ένα κρυπτογραφικό πρόγραμμα που σχεδιάστηκε για την προστασία των απόρρητων και εμπιστευτικών μηνυμάτων ηλεκτρονικού ταχυδρομείου από χάκερ και ακούσιους παραλήπτες.

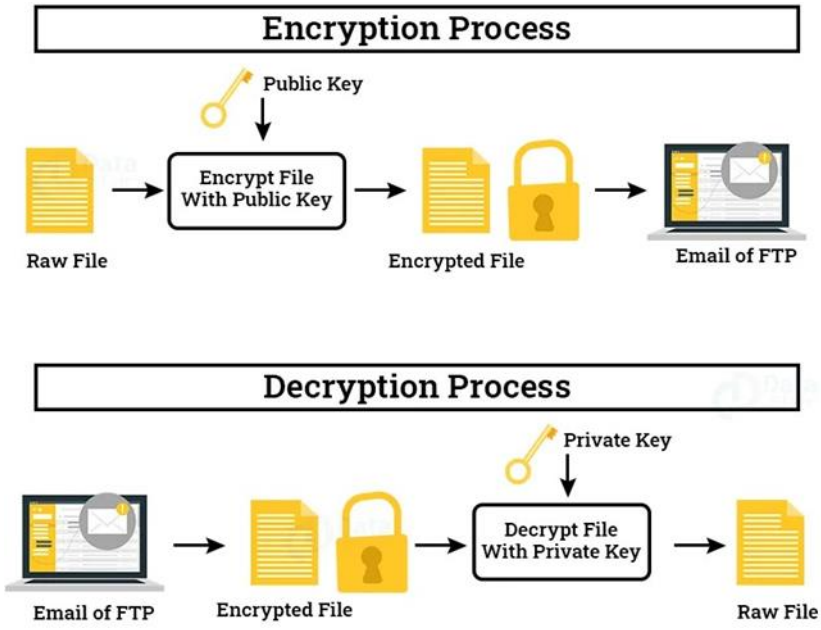
Το PGP διασφαλίζει ότι μόνο το άτομο στο οποίο στέλνετε το email και κανείς άλλος δεν θα μπορεί να το ανοίξει και να κοιτάξει το περιεχόμενό του.

Επιπλέον το PGP κάνει τη δουλειά του χρησιμοποιώντας δύο κλειδιά ή μαθηματικές εξισώσεις που χρησιμοποιούνται συνήθως στην κρυπτογραφία. Το πρώτο κλειδί (δημόσιο κλειδί), μεταφράζει το ακατέργαστο αρχείο ή το μήνυμα σε ακατάληπτο κώδικα. Το δεύτερο κλειδί (ιδιωτικό κλειδί), γνωστοποιείται μόνο στον παραλήπτη, το οποίο χρησιμοποιεί για να ανοίξει το αρχείο ή το μήνυμα.

Το PGP λειτουργεί ως εξής , οι χρήστες και στις δύο πλευρές (αποστολείς και παραλήπτες) πρέπει να διασφαλίσουν ότι χρησιμοποιούν συμβατά συστήματα, τηρούν τους συμφωνηθέντες κανόνες εμπιστευτικότητας και διατηρούν το ίδιο επίπεδο ασφάλειας. Η διαδικασία κρυπτογράφησης PGP έχει δύο μέρη - κρυπτογράφηση και αποκρυπτογράφηση. Στην πλευρά της κρυπτογράφησης, οι αποστολείς μηνυμάτων δημιουργούν πρώτα ένα τυχαίο κλειδί.

Στη συνέχεια χρησιμοποιούν αυτό το τυχαίο κλειδί για να κρυπτογραφήσουν τα δεδομένα και το δημόσιο κλειδί των παραληπτών. Τα κρυπτογραφημένα δεδομένα και το κρυπτογραφημένο κλειδί παραλήπτη συνδυάζονται, με αποτέλεσμα το κρυπτογραφημένο μήνυμα. Από την πλευρά της αποκρυπτογράφησης, εν τω μεταξύ, οι παραλήπτες αποκρυπτογραφούν το κρυπτογραφημένο κλειδί. Στη συνέχεια χρησιμοποιούν το αποκρυπτογραφημένο κλειδί για να αποκρυπτογραφήσουν τα δεδομένα, το οποίο τους επιτρέπει να διαβάσουν το μήνυμα.

Ακολουθεί ένα διάγραμμα που δείχνει πώς λειτουργεί οπτικά η διαδικασία PGP:



Σχήμα 17: PGP

5.6 Μέσα αποθήκευσης ψηφιακών πιστοποιητικών

5.6.1 HSM

Το HSM σημαίνει Hardware Security Module και είναι ένα πολύ ασφαλές αποκλειστικό υλικό για την ασφαλή αποθήκευση κρυπτογραφικών κλειδιών. Μπορεί να κρυπτογραφήσει, να αποκρυπτογραφήσει, να δημιουργήσει, να αποθηκεύσει και να διαχειριστεί ψηφιακά κλειδιά και να χρησιμοποιηθεί για υπογραφή και έλεγχο ταυτότητας. Σκοπός είναι η προστασία και προστασία ευαίσθητων δεδομένων.

Ο κύριος λόγος που χρειάζεται ένα HSM είναι ότι παρέχει ασφάλεια σε όλα τα επίπεδα.

Σε κλάδους όπως ο κλάδος πληρωμών όπου χειρίζεστε δεδομένα καρτών, τα δεδομένα πρέπει να είναι κρυπτογραφημένα προκειμένου να συμμορφώνονται με το Payment Card Industry Data Security Standard (PCI DSS). Από τεχνικής άποψη, ένα HSM είναι ένας πολύ ασφαλής τρόπος αποθήκευσης κρυπτογραφικών κλειδιών. Το υλικό προστατεύεται φυσικά και δεν μπορεί παραβιαστεί και προειδοποιεί εάν κάτι δεν πάει καλά.

Εάν ένα HSM κλαπεί και απενεργοποιηθεί, τα κρυπτογραφικά κλειδιά μπορούν να διαγραφούν αυτόματα από τη μνήμη του. Επομένως, είναι μια ασφαλής λύση εάν χρειάζεται να προστατευτούν εξαιρετικά ευαίσθητες πληροφορίες.

Τα κύρια οφέλη του είναι η ασφάλεια, απλότητα και απόδοση. Ένα HSM προστατεύει με ασφάλεια τα κρυπτογραφικά κλειδιά των χρηστών , αλλά ταυτόχρονα τα καθιστά εύκολα προσβάσιμα από την εφαρμογή της εκάστοτε πλατφόρμας και παρέχει υψηλή διαθεσιμότητα και απόδοση λειτουργιών κρυπτογράφησης.

Χρησιμοποιώντας ένα HSM, απαλλάσσουμε τους διακομιστές και τις εφαρμογές ως βασική λειτουργία σε μια κρυπτογράφηση, η κρυπτογράφηση γίνεται μέσω υλικού HSM αντί του διακομιστή του εκάστοτέ οργανισμού ή επιχείρησης.

Επίσης να πρέπει να αναφερθεί ότι υπάρχουν αυστηρά πρότυπα και διαδικασίες πιστοποίησης για μονάδες HSM. Υπάρχουν συγκεκριμένα πρότυπα ασφαλείας που πρέπει να τηρεί το ίδιο το υλικό – το FIPS-140 (Ομοσπονδιακά πρότυπα επεξεργασίας πληροφοριών) είναι ένα από αυτά. Το Συμβούλιο PCI έχει αφιερώσει επίσης ένα έγγραφο στο HSM , το οποίο καθορίζει τις απαιτήσεις για τη συσκευή. Η χρήση ενός HSM είναι μια σφραγίδα ασφαλείας για έναν οργανισμό ή επιχείρηση και για όσους αξιολογούν τη συμμόρφωσή με τα πρότυπα ασφαλείας, σηματοδοτεί ότι η εταιρεία λαμβάνει σοβαρά υπόψη την ασφάλεια των πληροφοριών και την κρυπτογράφηση.

Σχήμα 18 : HSM

5.6.1.1 CLOUD HSM

Η συμβατή με πρότυπα υπηρεσία cloud που επιτρέπει να προστατευτούν τα κρυπτογραφικά κλειδιά για τις εφαρμογές στο cloud, χρησιμοποιώντας επικυρωμένα HSM FIPS 140-2 Επίπεδο 3 .

Προσφέρει πλήθος υπηρεσιών όπως αυτοί που αναφέρονται παρακάτω

- **Κεντρική διαχείριση κλειδιών :** ο χρήστης μπορεί να διαχειριστεί κρίσιμα κλειδιά υψηλής αξίας για ολόκληρο τον οργανισμό σε ένα μέρος. Με τα αναλυτικά δικαιώματα ανά κλειδί, ελέγχει την πρόσβαση σε κάθε κλειδί με την αρχή της «λιγότερης προνομιακής πρόσβασης».

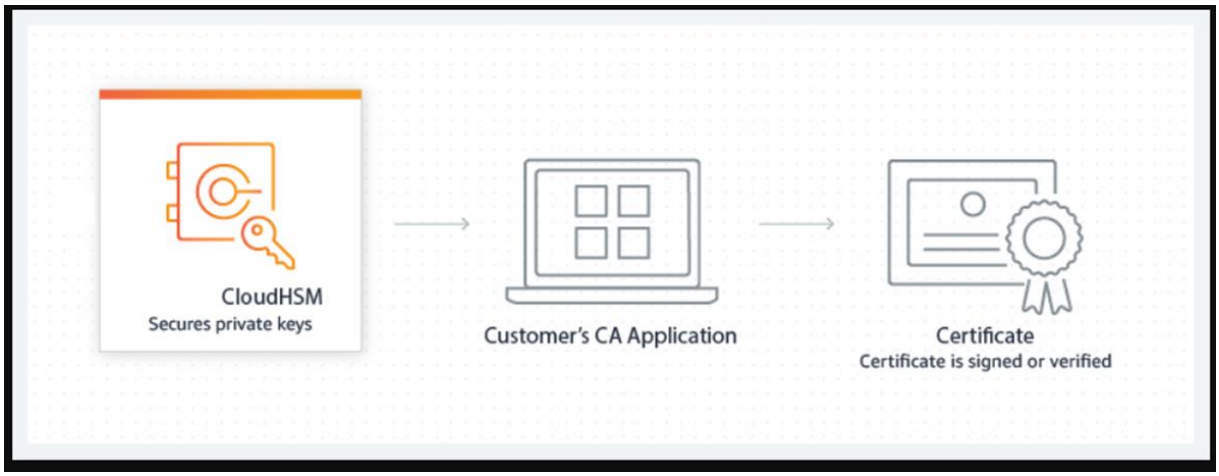
- **Έλεγχος απομονωμένης πρόσβασης :** Το διαχειριζόμενο μοντέλο ελέγχου πρόσβασης "τοπικό RBAC" HSM επιτρέπει στους καθορισμένους διαχειριστές HSM να έχουν πλήρη έλεγχο των HSM που ακόμη και οι διαχειριστές ομάδας διαχείρισης πόρων δεν μπορούν να παρακάμψουν.

- **Ιδιωτικά τελικά σημεία :** Χρησιμοποιήστε ιδιωτικά τελικά σημεία για ασφαλή και ιδιωτική σύνδεση στο Διαχειριζόμενο HSM από την εφαρμογή που εκτελείται σε εικονικό δίκτυο.

- **Επικυρωμένα HSM FIPS 140-2 Επίπεδο 3 :** Προστατεύονται τα δεδομένα των χρηστών και πληρούνται οι απαιτήσεις συμμόρφωσης με το FIPS (Ομοσπονδιακό Πρότυπο προστασίας πληροφοριών) 140-2 Επίπεδο 3 επικυρωμένα HSM. Τα διαχειριζόμενα HSM χρησιμοποιούν προσαρμογείς Marvell LiquidSecurity HSM.

- **Παρακολούθηση και έλεγχος :** Ο διαχειριστής λαμβάνει πλήρη αρχεία καταγραφής όλων των δραστηριοτήτων μέσω του κεντρικού Monitor.

- **Διανομή δεδομένων :** Το διαχειριζόμενο HSM δεν αποθηκεύει/επεξεργάζεται δεδομένα πελατών εκτός της περιοχής στην οποία ο διαχειριστής έχει αναπτύξει την παρουσία του HSM.



Σχήμα 19 : Cloud HSM

5.6.2 SMART CARD

Οι έξυπνες κάρτες, που περιστασιακά ονομάζονται κάρτες chip ή κάρτες ολοκληρωμένων κυκλωμάτων (IC ή ICC), είναι μια ευρεία οικογένεια φυσικών ηλεκτρονικών συσκευών ελέγχου ταυτότητας. Πιο πρακτικά, είναι φυσικά ασφαλείς μικροεπεξεργαστές που η χρήση τους γίνεται για ελεγχόμενη πρόσβαση σε πόρους. Από τις ταυτότητες έως τα κλειδιά ασφαλείας, οι έξυπνες κάρτες σε όλο τον κόσμο χρησιμοποιούνται σε μια μεγάλη ποικιλία εφαρμογών.

Οι έξυπνες κάρτες αναπτύσσονται για ένα ευρύ φάσμα εφαρμογών, οι πιο πολλές από αυτές να σχετίζονται με **τη Διαχείριση Ταυτότητας & Πρόσβασης** (IAM). Στην ουσία, είναι χρήσιμα για την επικοινωνία **ποιος** (είτε ποιο

άτομο είτε ποια συσκευή) προσπαθεί να αποκτήσει πρόσβαση σε έναν πόρο. Ο «πόρος» θα μπορούσε να είναι σχεδόν οτιδήποτε: ο λογαριασμός ενός ταμιευτηρίου , η πόρτα του συγκροτήματος διαμερισμάτων σας, η πρόσβαση Wi-Fi στον υπολογιστή εργασίας σας ή ίσως τα στοιχεία ασφάλισης υγείας σας.

Οι κοινές εφαρμογές έξυπνων καρτών περιλαμβάνουν:

- Κάρτες ATM (χρεωστικές και πιστωτικές κάρτες)
- ταυτότητες
- διαβατήρια
- Κάρτες PIV/CAC
- κάρτες SIM
- Περάσματα λεωφορείων
- Ηλεκτρονικά πορτοφόλια
- Security Tokens
- Κλειδιά ασφαλείας υλικού
- Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA)
- Ενιαία σύνδεση (SSO)

Σχήμα 20 : Smart Card

5.6.3 USB TOKEN

Ένα USB token είναι μια φυσική συσκευή που χρησιμοποιείται για τον καθορισμό προσωπικής ταυτότητας χωρίς τη χρήση κωδικού πρόσβασης για πρόσβαση σε ένα δίκτυο.

Χρησιμοποιείται ένα διακριτικό USB για την ηλεκτρονική απόδειξη της ταυτότητας του χρήστη, ενισχύοντας έτσι την ψηφιακή ασφάλεια. Παρέχει ασφαλή και ισχυρό έλεγχο ταυτότητας για πρόσβαση στο δίκτυο.

Σχήμα 21 : USB Token

6

Υποδομή Δημόσιου Κλειδιού

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure, PKI) αποτελεί ένα ολοκληρωμένο σύστημα πολιτικής, διαδικασιών και τεχνολογιών όπου τα κλειδιά και τα ψηφιακά πιστοποιητικά έχουν τον τρόπο να παρέχουν δυνατότητες αναγνώρισης, επαλήθευσης, εμπιστευτικότητας και διαχείρισης ασφάλειας σε ένα δίκτυο. Η υποδομή δημόσιου κλειδιού καθιστά δυνατή τη χρήση αυτών των κλειδιών και πιστοποιητικών εντός ενός συστήματος ασφαλείας, παράλληλα είναι υπεύθυνη για το κύκλο ζωής των πιστοποιητικών/κλειδιών αλλά και για την διαχείριση των πολιτικών ασφαλείας. Επιπλέον διατηρεί καταλόγους με τα πιστοποιητικά που είναι έγκυρα, έχουν ανακληθεί ή έχουν λήξει, διαφορετικά τα κλειδιά και τα πιστοποιητικά θα ήταν μη διαχειρίσιμα και το περιβάλλον δικτύωσης θα ήταν αναξιόπιστο.

6.1 Βασικές έννοιες της Υποδομής Δημοσίου Κλειδιού (PKI)

Μια πλήρης υποδομή δημόσιου κλειδιού (PKI) αποτελείται από πολλά στοιχεία, τα κύρια μέρη που την απαρτίζουν είναι τα παρακάτω:

Ρίζα Αρχής Πιστοποίησης (Root CA) Η Ρίζα Αρχής Πιστοποίησης είναι η κορυφή σε μια ιεραρχία ΥΔΚ και λειτουργεί ως το σημείο εμπιστοσύνης για πιστοποιητικά που εκδίδονται από Αρχές Πιστοποίησης στο περιβάλλον. Σε ένα περιβάλλον δύο ή τριών επιπέδων, η Ρίζα Αρχής Πιστοποίησης εκδίδει μόνο πιστοποιητικά σε δευτερεύοντες CA. Η Ρίζα Αρχής Πιστοποίησης πρέπει να δημιουργηθεί και να συντηρείται εκτός σύνδεσης, χωρίς να συνδέεται ποτέ σε δίκτυο.

Ενδιάμεση Αρχή Πιστοποίησης (Intermediate CA – Certificate Authority) η κύρια λειτουργία της είναι η έκδοση των ψηφιακών πιστοποιητικών και η επαλήθευσή τους. Ονομάζεται επίσης Εκδότης Πιστοποιητικού, όπου χρησιμοποιείται για την έκδοση των πιστοποιητικών και των καταλόγων ανάκλησης. Το πιστοποιητικό είναι μια δομή δεδομένων που αποτελείται τόσο από την τιμή του δημόσιου κλειδιού όσο και από τις πιστοποιημένες πληροφορίες που ανήκουν στον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού.

Το πιστοποιητικό δημόσιου κλειδιού εκδίδεται σε ένα άτομο και κάθε πιστοποιητικό είναι ψηφιακά υπογεγραμμένο από την CA έκδοσης. Τα πιστοποιητικά έχουν διάρκεια ζωής ενός ή δύο ετών και μπορεί να ανακληθούν για διάφορους λόγους, όπως απώλεια ιδιωτικού κλειδιού, συμβιβαστικό κλειδί ή λήξη της διάρκειας ζωής του πιστοποιητικού κ.λπ. Στην περίπτωση που προκύψει κάτι από τα προαναφερθέντα, η οντότητα που εξέδωσε το πιστοποιητικό ζητείται να ακυρώσει (ανακαλέσει) το πιστοποιητικό δημοσίου κλειδιού.

Υπάρχουν πολλοί μηχανισμοί για την ανάκληση του πιστοποιητικού και που επιτρέπουν και στον χρήστη να μπορεί να ελέγχει την εγκυρότητα του πιστοποιητικού (το πιστοποιητικό εξακολουθεί να ισχύει ή έχει ανακληθεί). Όλοι οι μηχανισμοί ανάκλησης πρέπει να είναι έγκαιροι και αποτελεσματικοί. Ένας από τους μηχανισμούς ανάκλησης είναι το CRL (Certificate Revocation List) που είναι μια λίστα η οποία περιέχει πιστοποιητικά που έχουν υπογραφεί ψηφιακά και ανακληθεί από την οντότητα που είχε εκδώσει αυτά τα πιστοποιητικά προηγουμένως.

Αρχή Εγγραφής (**RA – Registration Authority**), παρέχει τη λειτουργική επικοινωνία και διεπαφή ανάμεσα στον αιτούμενο και του παρόχου του. Έχει την ευθύνη της πιστοποίησης και του ελέγχου των στοιχείων ή των ρόλων μιας οντότητας. Συνήθως η RA διαθέτει μόνο έναν υπερ-διαχειριστή (Master Admin) ο οποίος μπορεί να έχει προσβασιμότητα εξ ολοκλήρου στις λειτουργίες που παρέχει η RA ο οποίος μπορεί να προσθέσει περισσότερους διαχειριστές εάν χρειάζεται. Συνήθως κάθε διαχειριστής που θέλει να έχει πρόσβαση στο σύστημα πρέπει να χρησιμοποιήσει τη δική του smart card (έξυπνη κάρτα) για να εμποδίσει μη εξουσιοδοτημένα άτομα να κάνουν οποιεσδήποτε ενέργειες στην RA.

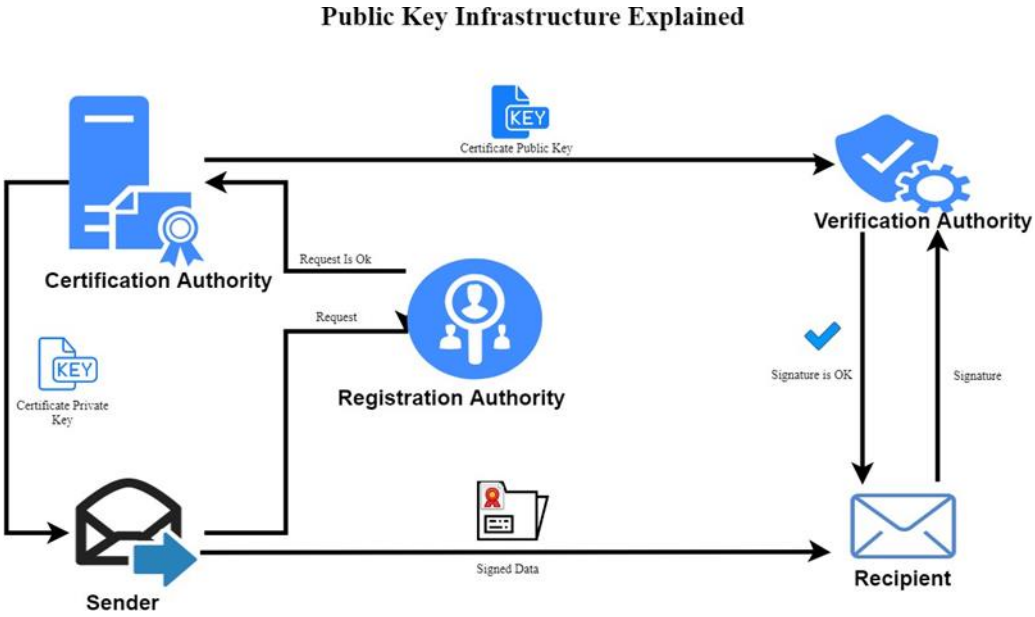
Αρχής Επιβεβαίωσης (VA - Validation Authority), πρόκειται για μία οντότητα που σύμφωνα με το πρότυπο RFC 5280 παρέχει επικύρωση των πιστοποιητικών έχοντας πρόσβαση σε λίστες ανάκλησης πιστοποιητικών (CRL), πρωτόκολλο κατάστασης πιστοποιητικού στο διαδίκτυο (OCSP) και λήψεις πιστοποιητικών αλυσίδας CA.

Αποθετήριο (**Repository**), μόλις δημιουργηθούν τα πιστοποιητικά και τα αντίστοιχα δημόσια κλειδιά, αποθηκεύονται σε μια δημόσια προσβάσιμη τοποθεσία γνωστή ως αποθήκη πιστοποιητικών . Τα αποθετήρια πιστοποιητικών συνήθως εκτός από πιστοποιητικά αποθηκεύουν αρχεία καταγραφής, λίστες ανάκλησης και κλειδιά.

Οντότητα-πελάτης, είναι ο τελικός χρήστης (φυσικό πρόσωπο ή σύστημα) που αιτείται και παραλαμβάνει πιστοποιητικά τα οποία εκδίδονται από την αρχή έκδοσης πιστοποιητικών. Δεσμεύεται ένα δημόσιο κλειδί με ορισμένες πληροφορίες αναγνώρισης το οποίο χρησιμοποιείται για κρυπτογράφηση, έλεγχο ταυτότητας, ψηφιακές υπογραφές και άλλους σκοπούς. Ο υπογράφων της δήλωσης είναι ο εκδότης και η οντότητα που αναφέρεται στο πιστοποιητικό είναι το υποκείμενο.

Λίστα ανάκλησης πιστοποιητικών (Certificate Revocation List - CRL) είναι μια υπογεγραμμένη, χρονικά σφραγισμένη λίστα με τους σειριακούς αριθμούς πιστοποιητικών και τους κωδικούς αιτίας των ανακληθέντων πιστοποιητικών από την Αρχή Πιστοποίησης. Οι λίστες ανάκλησης συνήθως δημοσιεύονται σε έναν δημόσια διαθέσιμο ιστότοπο για έλεγχο ανάκλησης. Μόλις ανακληθεί ένα πιστοποιητικό είναι άκυρο πριν από τη λήξη του.

Μονάδα Ασφάλειας Υλικού (Hardware Security Module – HSM) είναι μια φυσική υπολογιστική συσκευή που προστατεύει και διαχειρίζεται ψηφιακά κλειδιά για ισχυρό έλεγχο ταυτότητας και παρέχει επεξεργασία κρυπτογραφικών λειτουργιών. Είναι τυπικά πιστοποιημένα για φυσική ασφάλεια σε διάφορα επίπεδα ασφάλειας FIPS 140-2. Τα HSM συνιστώνται στις περισσότερες υλοποιήσεις PKI, δεδομένου ότι τα ιδιωτικά κλειδιά CA δεν βασίζονται σε λογισμικό και ως εκ τούτου είναι ανασφαλή, αλλά βασίζονται σε υλικό και διατίθενται μόνο από το ίδιο το HSM.



Σχήμα 22 : PKI

Οι υπηρεσίες μιας Υποδομής Δημοσίου Κλειδιού σύμφωνα με το PKIX είναι οι εξής:

- **Εγγραφή (Registration)**: Είναι μια διαδικασία όπου η τελική οντότητα εγγράφεται σε μια CA. Συνήθως, η εγγραφή γίνεται μέσω της RA.
- **Αρχικοποίηση (Initialization)**: Ασχολείται με βασικά προβλήματα, όπως η μεθοδολογία επαλήθευσης ότι η τελική οντότητα συνομιλεί με τη σωστή CA.
- **Πιστοποίηση (Certification)**: Είναι μια διαδικασία όπου η CA δημιουργεί ένα ψηφιακό πιστοποιητικό για την τελική οντότητα και το επιστρέφει στην τελική οντότητα. Η CA διατηρεί επίσης ένα αντίγραφο πιστοποιητικού για τα αρχεία της. Εάν απαιτείται, η CA το αντιγράφει επίσης σε δημόσιους καταλόγους.
- **Ανάκτηση ζεύγους κλειδιών (Key pair recovery)**: Τα κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση εγγράφων ενδέχεται να χρειαστεί να ανακτηθούν αργότερα για την αποκρυπτογράφηση των ίδιων παλαιών εγγράφων. Οι υπηρεσίες αρχειοθέτησης και ανάκτησης κλειδιών μπορούν να παρέχονται από την CA ή από ένα ανεξάρτητο σύστημα ανάκτησης κλειδιών.
- **Δημιουργία κλειδιού (Key generation)**: Το μοντέλο PKIX καθορίζει ότι η τελική οντότητα θα πρέπει να μπορεί να δημιουργήσει τα ζεύγη δημόσιου και ιδιωτικού κλειδιού ή η CA θα πρέπει να μπορεί να το κάνει αυτό για την τελική οντότητα.
- **Ενημέρωση κλειδιού (Key update)**: Είναι μια διαδικασία κατά την οποία το κλειδί του ψηφιακού πιστοποιητικού που έχει λήξει ανανεώνεται αυτόματα και αντικαθίσταται από ένα νέο ζεύγος κλειδιών. Ωστόσο, υπάρχει πρόβλεψη για μη αυτόματη ανανέωση ψηφιακών πιστοποιητικών.
- **Διασταυρούμενη πιστοποίηση (Cross certification)**: Είναι μια διαδικασία όπου οι τελικές οντότητες που έχουν επαναπιστοποιηθεί από διαφορετικές CA, μπορούν να αλληλοεπιβεβαιωθούν. Βοηθά στη δημιουργία μοντέλων εμπιστοσύνης.
- **Ανάκληση (Revocation)**: Το μοντέλο PKIX παρέχει υποστήριξη για έλεγχο της κατάστασης του πιστοποιητικού σε δύο λειτουργίες, online με χρήση OCSP και εκτός σύνδεσης με χρήση CRL.

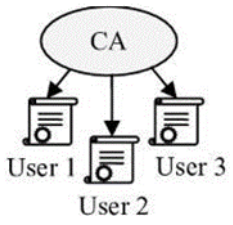
6.2 Μοντέλα Εμπιστοσύνης ΥΔΚ

Ένα μοντέλο εμπιστοσύνης αποτελείται από ένα σύνολο κανόνων, παρέχοντας έτσι ένα πλαίσιο για τη δημιουργία και την διαχείριση σχέσεων εμπιστοσύνης μεταξύ διαφόρων οντοτήτων μιας ΥΔΚ.

Οι σχέσεις εμπιστοσύνης επαληθεύονται μέσω της διαδικασίας επικύρωσης της διαδρομής πιστοποίησης, η οποία περιλαμβάνει: ανακάλυψη διαδρομής (path discovery), επαλήθευση υπογραφής (signature verification) και έλεγχο κατάστασης ανάκλησης (revocation status). Όταν οι σχέσεις εμπιστοσύνης είναι αμφίδρομες, μπορεί να υπάρχουν πολλαπλές διαδρομές μεταξύ δύο οντοτήτων, οι οποίες αυξάνουν τον χρόνο εκτέλεσης της διαδικασίας ανακάλυψης διαδρομής.

6.2.1 Μοντέλο μονής αρχής πιστοποίησης (Single CA Model)

Στη συγκεκριμένη περίπτωση όλοι οι χρήστες μιας ΥΔΚ, εμπιστεύονται την μοναδική Αρχή Πιστοποίησης της υποδομής, όπως φαίνεται στο παρακάτω σχήμα.



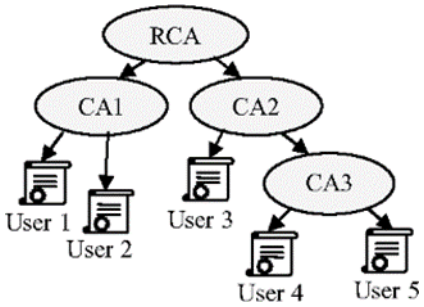
Σχήμα 23 : Single CA Model

Θεωρείται μια εύκολη και απλή διαμόρφωση μια ΥΔΚ, έχοντας όμως μεγάλο ρίσκο σε πιθανές μελλοντικές αλλαγές της Αρχής Πιστοποίησης.

6.2.2 Ιεραρχικό Μοντέλο (Hierarchical Model)

Ίσως το πιο συνηθισμένο μοντέλο εμπιστοσύνης, σε αύτη την περίπτωση του ιεραρχικού μοντέλου, όλοι οι χρήστες εμπιστεύονται την ίδια Ρίζα Αρχής Πιστοποίησης (Root CA). Σε ένα ιεραρχικό μοντέλο ΥΔΚ, οι σχέσεις εμπιστοσύνης είναι μονοκατευθυντικές, δηλαδή οι δευτερεύουσες Αρχές Πιστοποίησης δεν εκδίδουν πιστοποιητικά στις ανώτερες Αρχές Πιστοποίησης τους.

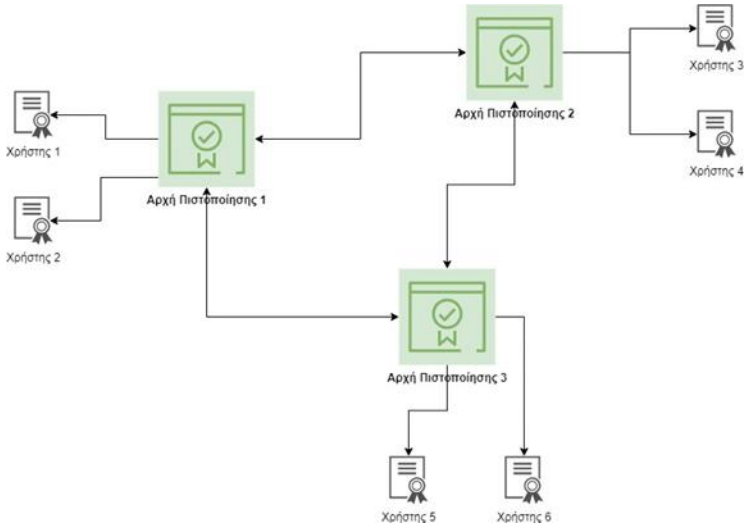
Το ιεραρχικό μοντέλο έχει ένα μόνο σημείο εμπιστοσύνης, οπότε εάν το ιδιωτικό κλειδί της Ρίζας Αρχής Πιστοποιήσης είναι γνωστό από άλλη οντότητα, όλη η ΥΔΚ τίθεται σε κίνδυνο.



Σχήμα 24 : Hierarchical Model

6.2.3 Μοντέλο πλέγματος (Mesh Model)

Είναι επίσης γνωστό ως μοντέλο δια-πιστοποίησης. Σε αυτή την περίπτωση όλες οι Αρχές Πιστοποίησης είναι αυτόνομες, επομένως μια ΑΠ δεν βασίζεται σε μια ανώτερη Ρίζα Αρχής Πιστοποίησης αντίθετα όπως στο Ιεραρχικό Μοντέλο. Εννοείται ότι οι σχέσεις εμπιστοσύνης εντός ενός μοντέλου πλέγματος αν χρειαστεί μπορεί να μην είναι άνευ ορών. Κάθε ΑΠ μπορεί να καθορίσει αυτούς τους περιορισμούς στο προφίλ των πιστοποιητικών, η οποία εκδίδει. Μια αρχιτεκτονική ΥΔΚ βασισμένη στο μοντέλο πλέγματος μπορεί να ενσωματώσει πολύ ευκολά μια νέα αυτόνομη ΑΠ στο σύμπλεγμα της χωρίς το παραμικρό ρίσκο.

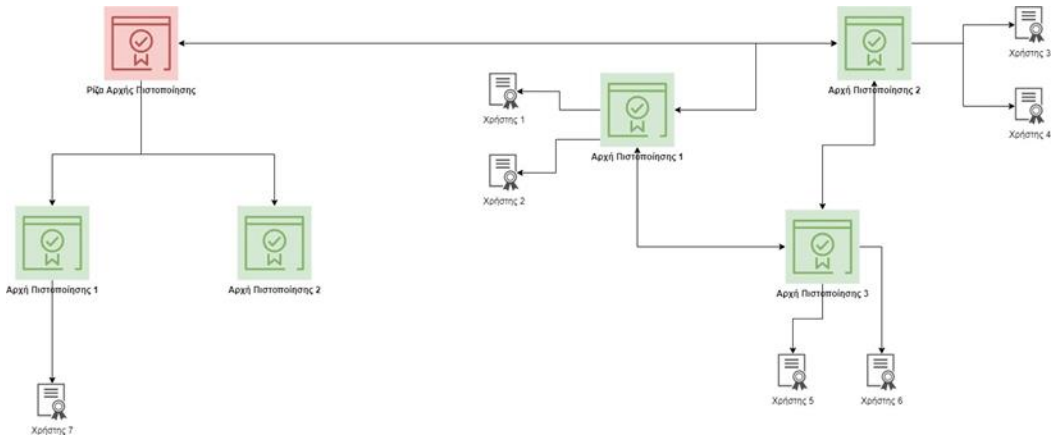


Σχήμα 25 : Mesh Model

Σε αυτό το μοντέλο, ο αριθμός των σχέσεων εμπιστοσύνης είναι ευθέως ανάλογος με τον αριθμό των ΑΠ, έτσι το μέγιστο μήκος διαδρομής σε ένα μοντέλο πλέγματος είναι ο αριθμός των ΑΠ που ανήκουν στην ΥΔΚ.

6.2.4 Υβριδικό Μοντέλο (Hybrid Model)

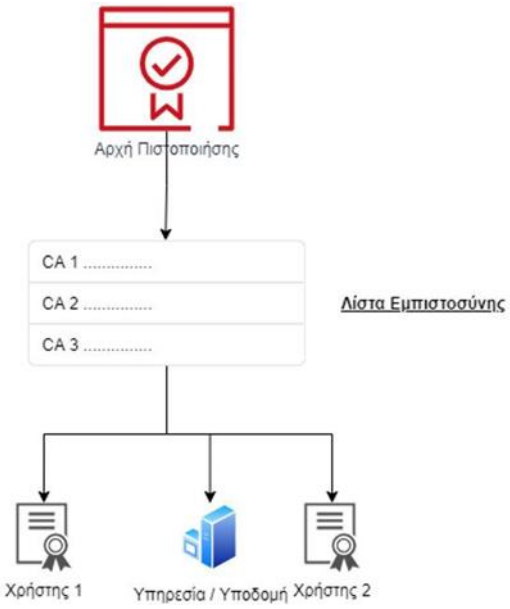
Η τεχνολογική εξέλιξη και οι ανάγκες που προκύπτουν από αυτή, καθιστά επιθυμητό τα μοντέλα εμπιστοσύνης να μην είναι στατικά και στενά περιορισμένα. Όπως υποδηλώνει το όνομά του, το υβριδικό μοντέλο επιτρέπει τη μίξη αρχιτεκτονικών πιστοποίησης, για παράδειγμα, είναι δυνατή η σύνδεση ενός ιεραρχικού PKI με ένα μόνο μοντέλο CA μέσω διασταυρούμενης πιστοποίησης μεταξύ των CA τους.



Σχήμα 26: Hybrid Model

6.2.5 Μοντέλο Λίστας Εμπιστοσύνης

Το μοντέλο λίστας εμπιστοσύνης χρηστών είναι η πιο κοινή αρχιτεκτονική ανάπτυξης εμπιστοσύνης που χρησιμοποιείται σήμερα, που προσφέρεται από λειτουργικά συστήματα και εφαρμογές ιστού. Ένα παράδειγμα είναι η λίστα με περισσότερες από εκατό ΑΠ που περιλαμβάνονται στις διανομές του Microsoft OS.



Σχήμα 27: Μοντέλο Λίστας Εμπιστοσύνης

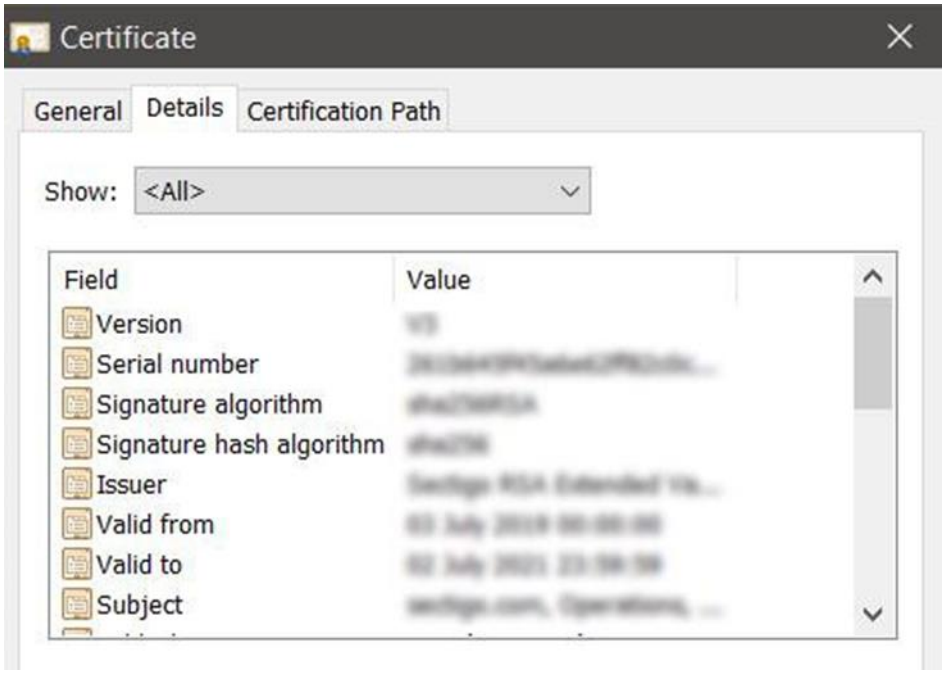
6.3 Πρότυπο x.509

Το X.509 είναι ένα διεθνές πρότυπο που καθορίζει τον τρόπο λειτουργίας των Υποδομών Δημοσίου Κλειδιού (Public Key Infrastructure/PKI). Το 1988 δημοσιεύτηκε η αρχική έκδοση του προτύπου X.509. Προσπαθώντας να επισημοποιήσει τους κανόνες για την έκδοση πιστοποιητικών, το ITU-T ανέπτυξε ένα ιεραρχικό σύστημα για διακεκριμένα ονόματα που ακολουθούσαν τους κανόνες υπηρεσίας ηλεκτρονικού καταλόγου για X.500. Το 1996, η έκδοση 3 του προτύπου παρείχε μια σημαντική ενημέρωση με την προσθήκη πολλαπλών επεκτάσεων που χρησιμοποιούνται ακόμη και σήμερα για να υποστηρίξουν την επέκταση και τις νέες εφαρμογές χρήσης του διαδικτύου. Η ομάδα εργασίας υποδομής δημόσιου κλειδιού Internet Engineering Task Force (IETF), γνωστή ως PKIX, προσάρμοσε το πρότυπο πιστοποιητικού X.509 v3 για την ανάπτυξη του δικού του πιστοποιητικού υποδομής δημόσιου κλειδιού Internet X.509 και Λίστα ανάκλησης πιστοποιητικών (CRL) Πρότυπο προφίλ (RFC 5280)

Μεταξύ άλλων περιλαμβάνει τα παρακάτω:

- **Έκδοση** (Version) η έκδοση X.509 που ισχύει για το πιστοποιητικό
- **Σειριακός αριθμός** (Serial number) το μοναδικό αναγνωριστικό σειριακού αριθμού που παρέχεται από την CA και διακρίνει το πιστοποιητικό από τα άλλα πιστοποιητικά
- **Πληροφορίες αλγορίθμου** (Algorithm information) ο κρυπτογραφικός αλγόριθμος που χρησιμοποιείται από τον εκδότη για την υπογραφή του πιστοποιητικού
- **Διακεκριμένο όνομα εκδότη** (Issuer distinguished name) το όνομα της CA που εκδίδει το πιστοποιητικό

- **Περίοδος ισχύος του πιστοποιητικού** (Validity period of the certificate) η ημερομηνία και η ώρα έναρξης και λήξης της εγκυρότητας του πιστοποιητικού
- **Διακεκριμένο όνομα υποκειμένου** (Subject distinguished name) το όνομα της ταυτότητας στην οποία εκδίδεται το πιστοποιητικό
- **Πληροφορίες δημοσίου κλειδιού** (Subject public key information) το δημόσιο κλειδί που σχετίζεται με την ταυτότητα



Σχήμα 28: X.509

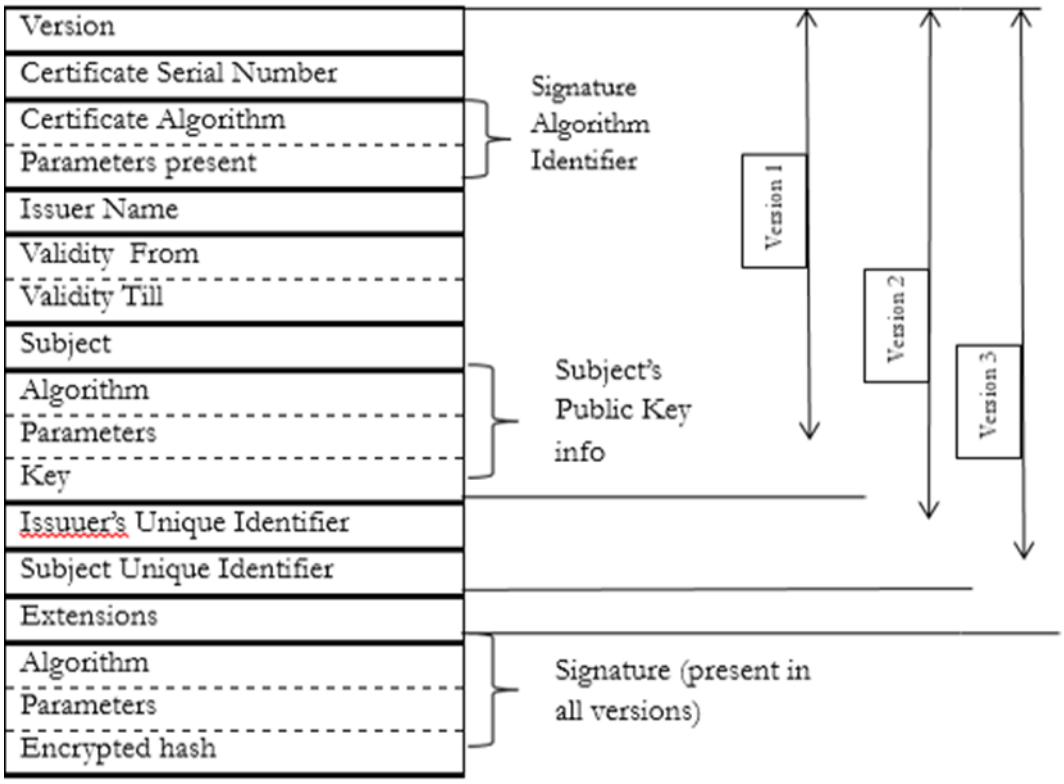
Τα πεδία που προστέθηκαν στην 2η έκδοση είναι τα εξής:

- **Μοναδικό αναγνωριστικό εκδότη** (Issuer unique identifier): Περιέχει μια μοναδική τιμή με πληροφορίες για τον εκδότη του πιστοποιητικού σύμφωνα με το πρότυπο X.500.
- **Μοναδικό αναγνωριστικό υποκειμένου** (Subject unique identifier): Περιέχει μια μοναδική τιμή με πληροφορίες για τον ιδιοκτήτη του πιστοποιητικού σύμφωνα με το πρότυπο X.500.

Οι επεκτάσεις πιστοποιητικών που εισήχθησαν στην 3η έκδοση του προτύπου X.509 για τα πιστοποιητικά, επιτρέπουν την προσαρμογή των πιστοποιητικών σε εφαρμογές. Επίσης παρέχουν τη δυνατότητα συσχέτισης πρόσθετων χαρακτηριστικών με χρήστες ή δημόσια κλειδιά. Κάθε επέκταση, η οποία αναγνωρίζεται από το OID (Object Identifier), χαρακτηρίζεται ως "κρίσιμη" ή "μη κρίσιμη" και περιλαμβάνει τα ειδικά δεδομένα της επέκτασης. Στο πεδίο επεκτάσεων της 3ης έκδοση προστέθηκαν τα εξής :

- **Όνομα επέκτασης** (extension name)

- **Κρισιμότητα επέκτασης** (criticality indicator)
- **Τιμή επέκτασης** (extension value), δηλαδή την πληροφορία που περιέχει.



Σχήμα 29: X.509 All Versions

6.4 Πολιτικές και Υποδομή Δημοσίου Κλειδιού

6.4.1 Πολιτική Πιστοποίησης (CP)

Η Πολιτική Πιστοποίησης χρησιμοποιείται σε ένα PKI για να καθορίσει απαιτήσεις που δηλώνουν τι πρέπει να κάνουν οι συμμετέχοντες σε αυτό. Μια μεμονωμένη ΑΠ ή οργανισμός μπορεί να χρησιμοποιήσει ένα CPS για να αποκαλύψει πώς πληροί τις απαιτήσεις ενός CP ή πώς εφαρμόζει τις πρακτικές και τους ελέγχους του.

Ένα CP διευκολύνει τη δια λειτουργικότητα μέσω διασταυρούμενης πιστοποίησης, μονομερούς πιστοποίησης ή άλλων μέσων. Ως εκ τούτου, προορίζεται να καλύψει πολλαπλές ΑΠ. Αντίθετα, ένα CPS είναι μια δήλωση μιας μεμονωμένης ΑΠ ή οργανισμού. Σκοπός του δεν είναι η διευκόλυνση της διαλειτουργικότητας (καθώς αυτό είναι η λειτουργία ενός CP).

6.4.2 Δήλωσης Πρακτικών Πιστοποίησης (CPS)

Η Δήλωση Πρακτικών Πιστοποίησης (CPS) ορίζεται στο Πλαίσιο PKIX ως δήλωση των πρακτικών που εφαρμόζει η Αρχή Πιστοποίησης στην έκδοση πιστοποιητικών. Η Δήλωση Πρακτικών Πιστοποίησης καθορίζει όλες τις διαδικασίες που είναι απαραίτητες για την αποδοτική και ασφαλή έκδοση και διαχείριση των πιστοποιητικών που εκδίδονται από μια Αρχή Πιστοποίησης ώστε να πληροί τις απαιτήσεις της Πολιτικής Πιστοποίησης. Οι πρακτικές που ορίζονται στη Δήλωση Πρακτικών Πιστοποίησης πρέπει να αναπτυχθούν σύμφωνα με τις άλλες πολιτικές και πρότυπα ασφάλειας ενός οργανισμού (για παράδειγμα, πρακτικές στους τομείς του προσωπικού, της φυσικής και περιβαλλοντικής ασφάλειας).

Ο Αμερικανικός Δικηγορικός Σύλλογος (ABA) έχει αναπτύξει μια σειρά οδηγιών για την ανάπτυξη μιας δήλωσης πρακτικών πιστοποίησης που καθορίζει τις πολιτικές και τις πρακτικές ενός οργανισμού για τη λειτουργία μιας Αρχής Πιστοποίησης. Καθώς οι ολοένα και πιο πολύτιμες επιχειρηματικές συναλλαγές εκτελούνται με χρήση ψηφιακών πιστοποιητικών, η Δήλωση Πρακτικών Πιστοποίησης γίνεται ένα σημαντικό νομικό και λειτουργικό έγγραφο που παρέχει τα μέσα τόσο για τον καθορισμό της εφαρμογής των ψηφιακών πιστοποιητικών εντός μιας επιχειρηματικής κοινότητας όσο και για την παροχή νομικής προστασίας σε περίπτωση διαφωνιών.

6.5 Ασφαλή χρονοσήμανση

Στον ψηφιακό κόσμο, είναι σημαντικό να μπορούμε να εμπιστευόμαστε ότι οι υπογραφές και τα έγγραφα είναι αυθεντικά. Η χρονοσήμανση ή αλλιώς χρονοσφραγίδα είναι ένας τρόπος για να αποδειχθεί ότι τα περιεχόμενα ενός εγγράφου υπάρχουν σε μια συγκεκριμένη χρονική στιγμή και δεν έχουν αλλάξει από τότε.

Όταν ένα έγγραφο έχει χρονική σήμανση, δημιουργείται ένας κρυπτογραφικός κατακερματισμός με βάση τα περιεχόμενα του εγγράφου. Αυτός ο κατακερματισμός στη συνέχεια υπογράφεται με ένα ιδιωτικό κλειδί, δημιουργώντας μια ψηφιακή υπογραφή. Ο υπογεγραμμένος κατακερματισμός, μαζί με το δημόσιο κλειδί και άλλα μεταδεδομένα, τίθεται στη συνέχεια με χρονική σήμανση από ένα αξιόπιστο τρίτο μέρος.

Η χρονοσφραγίδα αποδεικνύει ότι το περιεχόμενο του εγγράφου υπήρχαν τη στιγμή που υπογράφηκε και η ψηφιακή υπογραφή αποδεικνύει ότι το έγγραφο δεν έχει αλλάξει από τότε. Ως εκ τούτου , οι χρονοσφραγίδες αποτελούν σημαντικό τρόπο διασφάλισης της αυθεντικότητας των ψηφιακών υπογραφών και εγγράφων.

Η χρονική σήμανση μπορεί να χρησιμοποιηθεί για να αποδείξει ανεξάρτητα και αδιαμφισβήτητα την ώρα μιας συναλλαγής, τη στιγμή που υπογράφηκε ένα έγγραφο και πότε αρχειοθετήθηκε. Τα RFC 3161 και RFC 5816 είναι πρότυπα για την ασφαλή κρυπτογραφική χρονοσήμανση και τα προϊόντα και τους οργανισμούς που πρέπει να περιλαμβάνουν στις χρονικές σφραγίδες.

Αυτό περιλαμβάνει την παροχή μιας αξιόπιστης πηγής χρόνου, μιας αξιόπιστης χρονικής αξίας και ενός μοναδικού αναγνωριστικού για κάθε χρονική σήμανση που έχει εκδοθεί. Το TSA δεσμεύει κρυπτογραφικά το μοναδικό κατακερματισμό / σύνοψη μηνυμάτων / δακτυλικό αποτύπωμα των δεδομένων με την τρέχουσα ημερομηνία και ώρα που συγχρονίζονται με μια αξιόπιστη πηγή ώρας.

Αυτό γίνεται με μια ειδική ψηφιακή υπογραφή, χρησιμοποιώντας ένα ιδιωτικό κλειδί υπογραφής υπό τον αποκλειστικό έλεγχο του TSA που θα πρέπει να δημιουργηθεί και να αποθηκευτεί σε μια μονάδα ασφαλείας υλικού υψηλής εμπιστοσύνης (HSM).

7

Τεχνική υλοποίηση

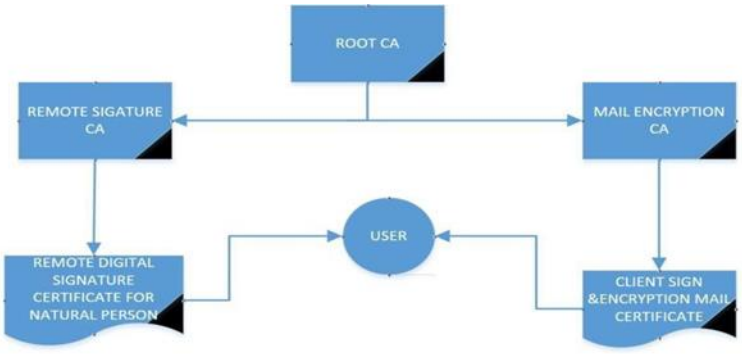
Στην ενότητα αυτή θα παρουσιαστεί η υλοποίηση δύο υποδομών δημοσίου κλειδιού για εκπαιδευτικούς σκοπούς. Σκοπός είναι η κατανόηση των εφαρμογών της κρυπτογραφίας δημόσιου κλειδιού όπως και της διαχείρισης του κύκλου ζωής των ψηφιακών πιστοποιητικών.

Στόχος της υλοποίησης είναι δημιουργηθεί ένα υβριδικό μοντέλο το οποίο θα αποτελείται από μία κοινή Ρίζα Αρχής Πιστοποίησης (Root CA) (με αλγόριθμο κρυπτογράφησης RSA) και δύο Ενδιάμεσων Αρχών Πιστοποίησης (Intermediate CA – Certificate Authority) (με αλγόριθμο ελλειπτικών καμπυλών NIST P) από διαφορετικές πλατφόρμες υποδομής δημοσίου κλειδιού. Σαν αποτέλεσμα θα δημιουργήσουμε δύο διαφορετικά πιστοποιητικά του ιδίου τελικού χρήστη για δύο διαφορετικές λειτουργίες, όπου η πρώτη λειτουργία αφορά απομακρυσμένη ψηφιακή υπογραφή ενός εγγράφου ενώ η δεύτερη αφορά την υπογραφή ενός ηλεκτρονικού μηνύματος με την χρήση ηλεκτρονικού ταχυδρομείου (Microsoft Outlook).

Πιο συγκεκριμένα χρησιμοποιήθηκε ένα εικονικό εργαστηριακό περιβάλλον υποδομής ORACLE VM VirtualBox και λειτουργικού συστήματος Windows Server 2019.

Επίσης για τις απαιτήσεις της εργασίας εγκαταστάθηκαν τα λογισμικά ADSS Ascertia PKI & MS-PKI σε μία αρχιτεκτονική διάταξη που θα παρέχει τη δυνατότητα διεξαγωγής ολοκληρωμένης εικόνας σχεδίασης και ανάπτυξης μίας Υποδομής Δημόσιου Κλειδιού.

Παρακάτω αναπτύσσονται τα δύο τεχνικά σενάρια:



Σχήμα 30: Δομή πιστοποιητικών Σεναρίων

7.1 Σενάριο Εργασίας Α

Δημιουργία μίας Ρίζα Αρχής Πιστοποίησης (Root CA) και Ενδιάμεση Αρχή Πιστοποίησης (Intermediate CA – Certificate Authority), στην τεχνική πλατφόρμα ADSS Acertia. Στο συγκεκριμένο σενάριο θα παράξουμε ένα προφίλ ψηφιακής υπογραφής με ελλειπτικές καμπύλες και θα καταλήγει σε μια εφαρμογή κινητού ενός χρήστη όπου θα του δίνει την δυνατότητα να παράγει μια υπογραφή και να υπογράφει ένα έγγραφο απομακρυσμένα.

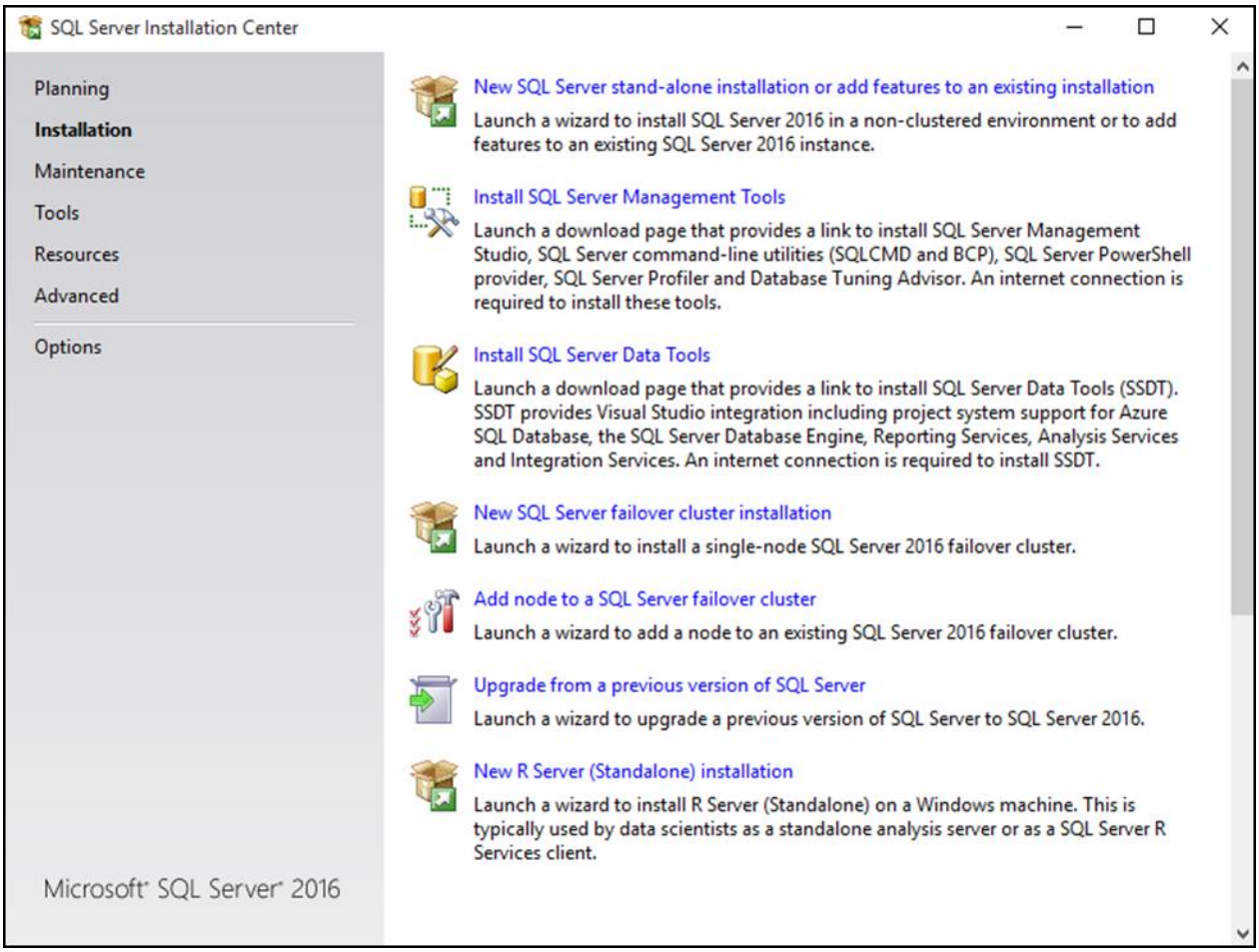
Πριν από εγκατάσταση του ADSS server πρέπει να εγκατασταθεί η MICROSOFT SQL SERVER και για την σωστή λειτουργία του συστήματος θα πρέπει να πληρούνται οι παρακάτω ελάχιστες απαιτήσεις:

• .NET Framework 4.6. SQL Server 2016 setup automatically installs .NET Framework. • Microsoft Windows Installer 4.5 or a later version (SQL Server will install this if necessary) • Windows PowerShell 2.0 • Internet Explorer 7 or a later version is required for Microsoft Management Console (MMC), SQL Server Data Tools (SSDT), the Report Designer component of Reporting Services, and HTML Help. • TCP/IP networking	
RAM	Minimum: 512 MB Recommended: 4 GB or higher
Hard Disk space	10 GB free space
Processor (x64)	AMD Opteron, AMD Athlon 64, Intel Xeon with Intel EM64T support, Intel Pentium IV with EM64T support Minimum: 1.4 GHz Recommended: 2.0 GHz or faster
Operating System	Windows 7 Windows 7 Service Pack 1 Windows 8 Windows 8.1 Windows 10 Windows Server 2008 R2 Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019

Εγκατάσταση Enterprise Edition

Τα πρωταρχικά βήματα που πρέπει να ακολουθηθούν για την εγκατάσταση είναι τα εξής :

1. Να εκτελεστεί το **Setup.exe** αρχείο για την δημιουργία του SQL Server.
2. Να εκτελέσουμε το **SQL Server 2016 Installation Center** και να επιλέξουμε την πρώτη επιλογή **"New SQL Server stand-alone installation"** και στην συνέχεια να πατήσουμε OK

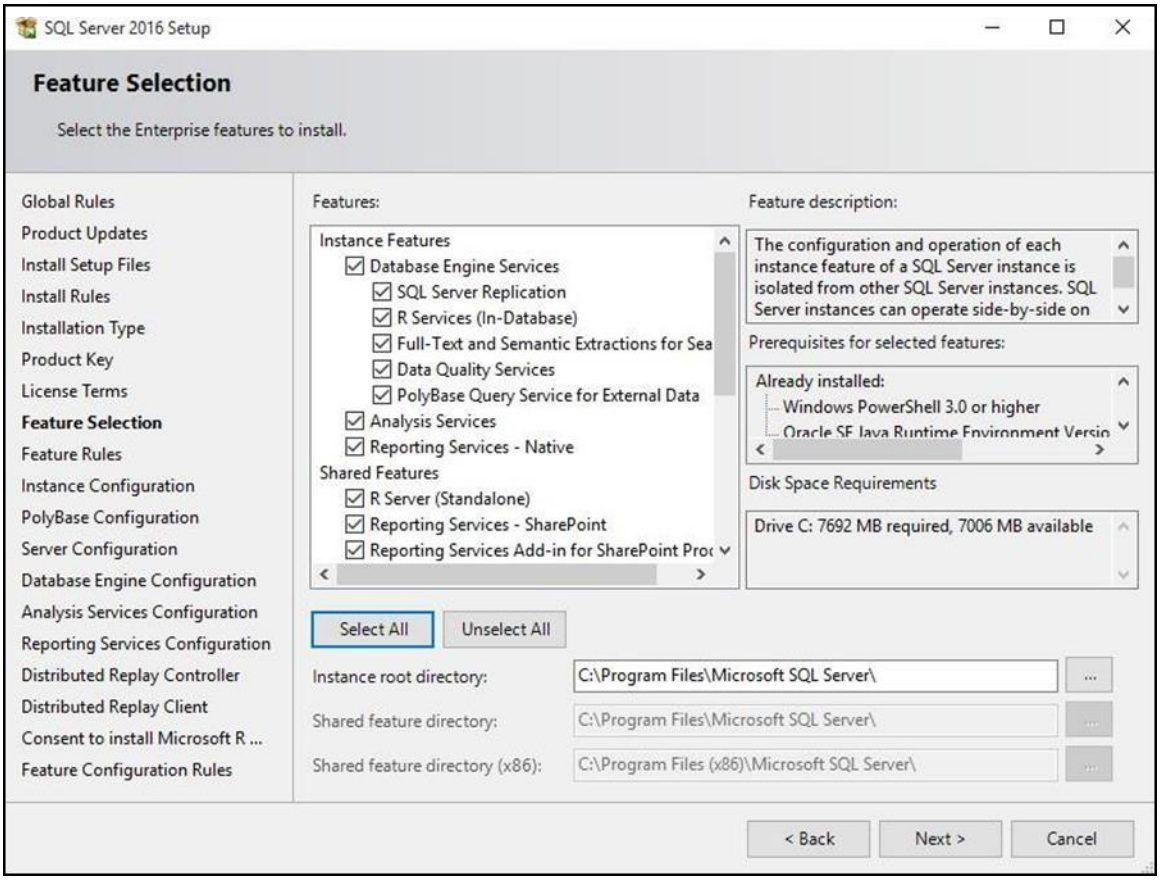


3. Το επόμενο βήμα είναι να προμηθεύουμε το license key του λογισμικού και στη συνέχεια να κάνουμε κλικ στο κουμπί Επόμενο.

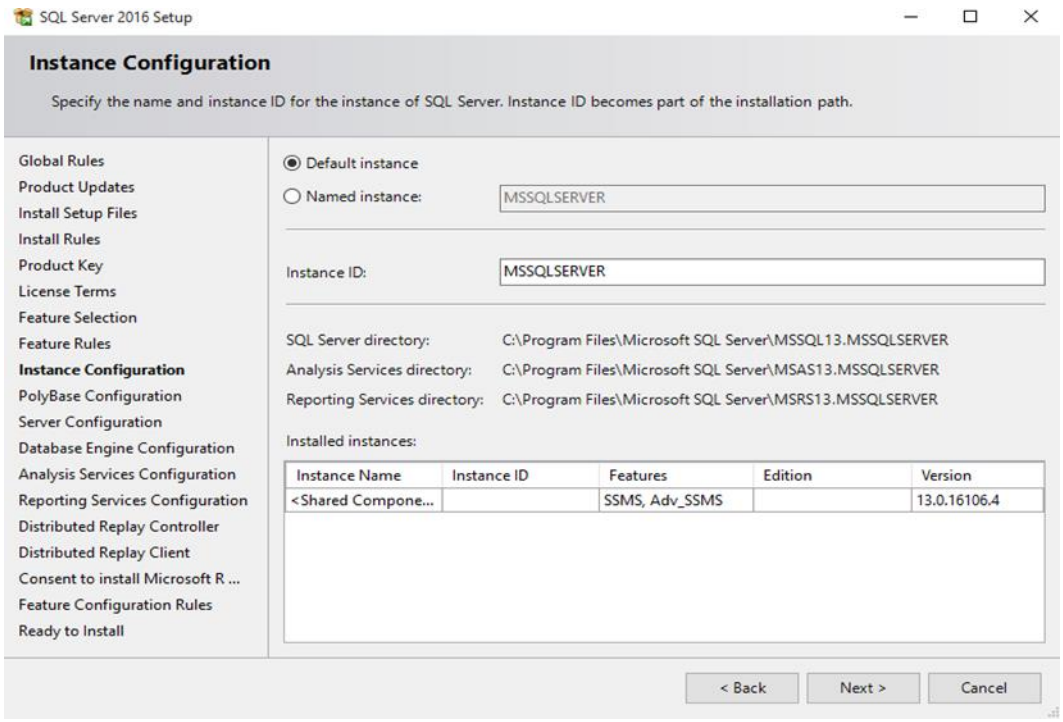
4. Αποδεχόμαστε του ορούς άδειας και χρήσης του λογισμικού , κάνουμε κλικ στο κουμπί Επόμενο και στη συνέχεια πατάμε το κουμπί Εγκατάσταση.

5. Το επόμενο βήμα είναι να επιλέξουμε ποιες δυνατότητες του SQL Server θα εγκατασταθούν. Επιλέγουμε τη δυνατότητα “SQL Server feature installation" και κάνουμε κλικ στο κουμπί Επόμενο.

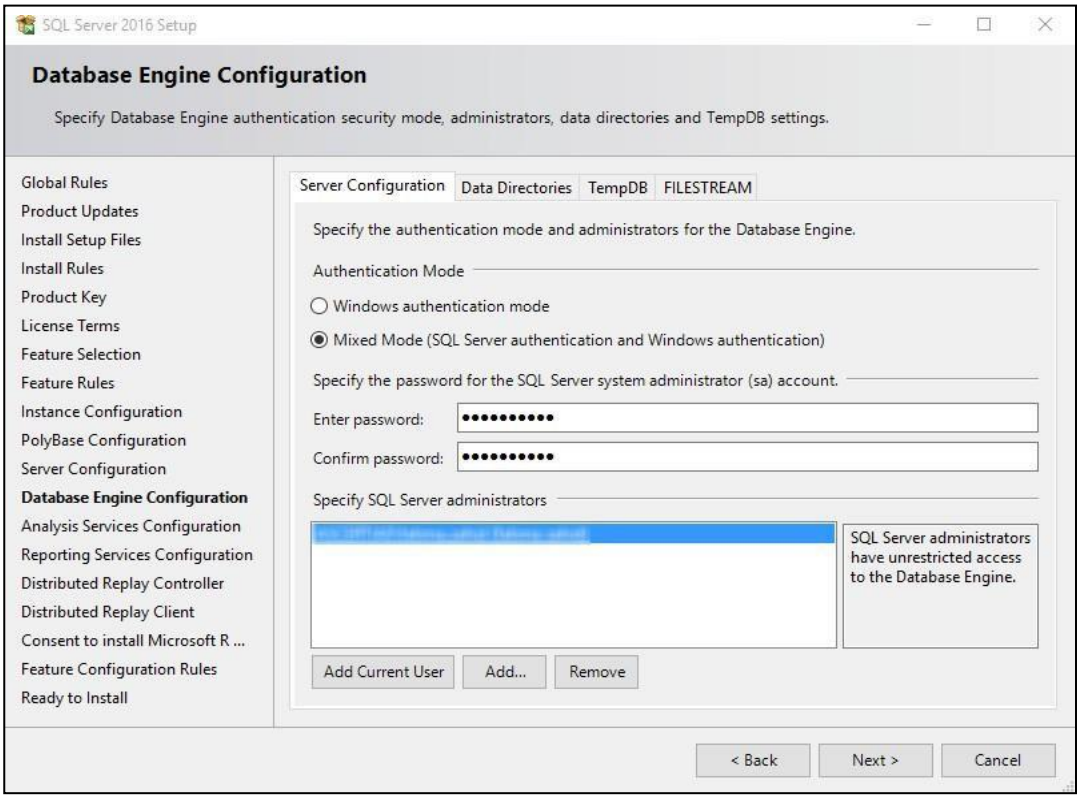
6. Στη συνέχεια θα εμφανιστεί η οθόνη επιλογής δυνατοτήτων. Κάνουμε κλικ στα πλαίσια ελέγχου για να εγκαταστήσουμε μερικές ή όλες τις δυνατότητες που μας ενδιαφέρουν. Για να εγκαταστήσουμε το SQL Server 2016 Management Studio, επιλέγουμε " Management Tools – Basic " και στη συνέχεια κάνουμε κλικ στο κουμπί Επόμενο.



7. Στον Πίνακα Διαμόρφωσης, προσδιορίζουμε συγκεκριμένα το MSSQLSERVER και τα δυο πεδία “Named instance” και"Instance".



8.Επόμενο βήμα είναι η PolyBase Διαμόρφωση. Αφήνουμε την προκαθορισμένη επιλογή και κάνουμε κλικ στο Επόμενο .

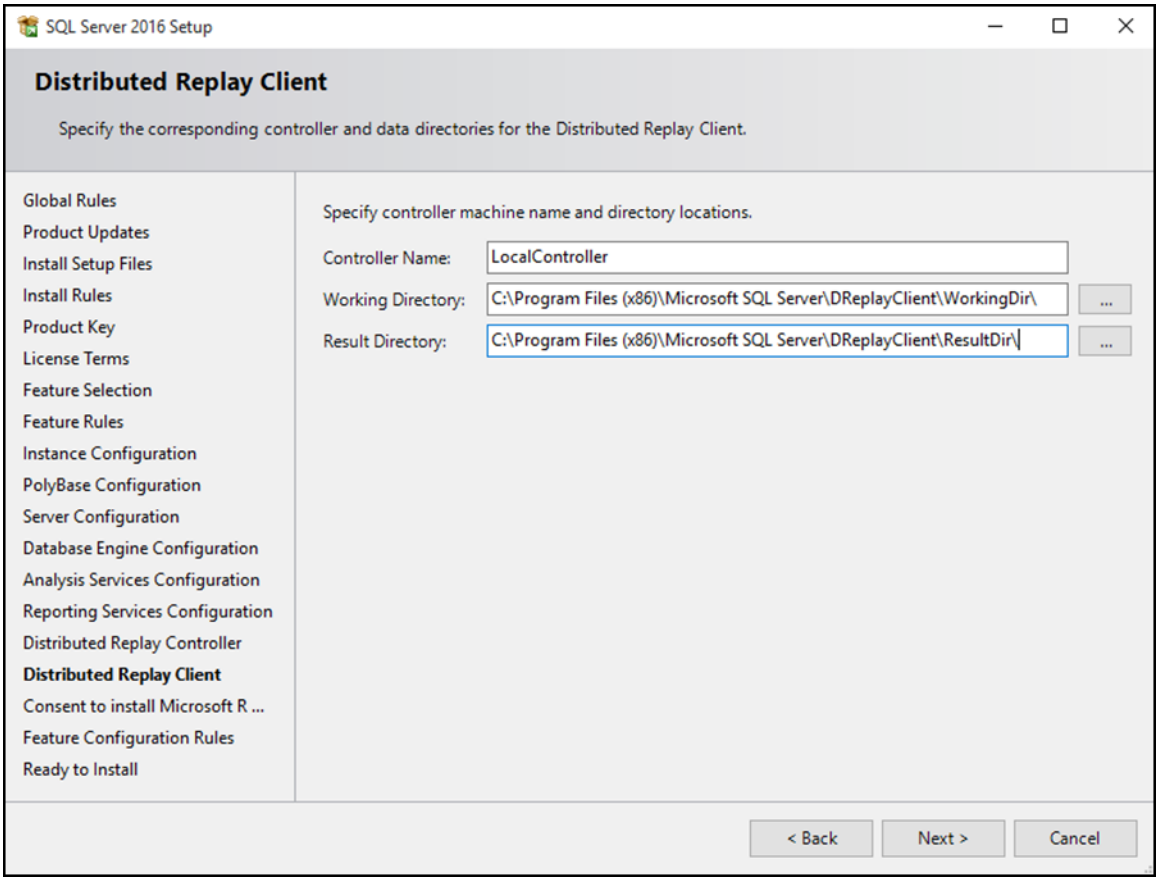


9. Το επόμενο βήμα είναι η Διαμορφώση διακομιστή, κάνουμε κλικ στο Επόμενο για να δώσουμε λεπτομέρειες για τη βάση δεδομένων.

10. Στη συνέχεια επιλέγουμε το SQL Server Analysis Services που θα συμπεριληφθεί στην εγκατάσταση, και κατ' επέκταση θα μας οδηγήσει για να γίνει η ενεργοποίηση του Analysis Services Server Mode. Για να μπορούμε να χρησιμοποιήσουμε κανονικά σχήματα SQL (σχεσιακά) για υπηρεσίες ανάλυσης θα πρέπει να προσδιορίσουμε τη λειτουργία των πινάκων . Επίσης για να χρησιμοποιήσουμε τις πολυδιάστατες δομές δεδομένων (Multidimensional data structures) , επιλέγουμε το Multidimensional and Data Mining Mode.

11. Η επόμενη οθόνη μας δίνει την επιλογή για το εάν θα παρέχονται ή όχι αναφορές σφαλμάτων στη Microsoft . Ορίζουμε μια επιλογή και κάνουμε κλικ στο κουμπί Επόμενο για να συνεχίσει η εγκατάσταση.

12. Εάν επιλεχθεί το Distributed Replay Services για την εγκατάσταση, στη επόμενη οθόνη θα ζητηθεί από τον χρήστη να δοθούν δικαιώματα προς χρήση. Στην συνέχεια πατάμε κλικ στο κουμπί Επόμενο για να συνεχίσει η εγκατάσταση.



13. Εάν επιλέξουμε να εγκαταστήσουμε την δυνατότητα Distributed Replay Client, στην επόμενη οθόνη θα εμφανιστούν τα Controller Name, Working Directory και Results Directory. Τα προεπιλεγμένα ονόματα θα πρέπει να είναι επαρκή για την εγκατάσταση. Κάνουμε κλικ στο κουμπί Επόμενο για να συνεχίσουμε την εγκατάσταση.

14. Στο επόμενο βήμα εγκαθιστούμε το Microsoft R Open, κάνουμε κλικ στο κουμπί
Αποδοχή και έπειτα στο Επόμενο .

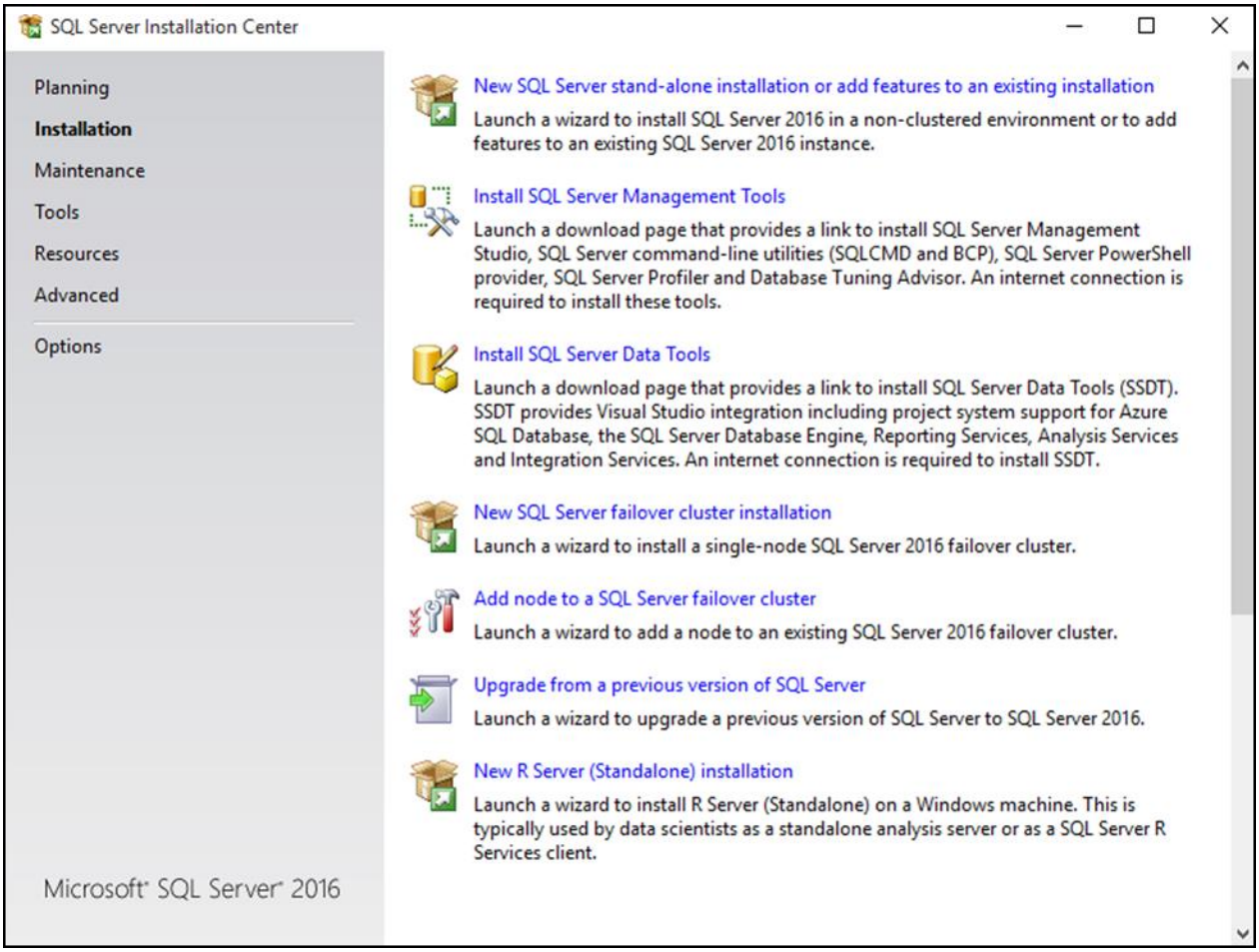
15. Κάνουμε κλικ στο κουμπί Εγκατάσταση

16. Όταν ολοκληρωθεί η εγκατάσταση του SQL Server πατάμε το κουμπί Κλείσιμο .

Εγκατάσταση SQL Server Management Studio

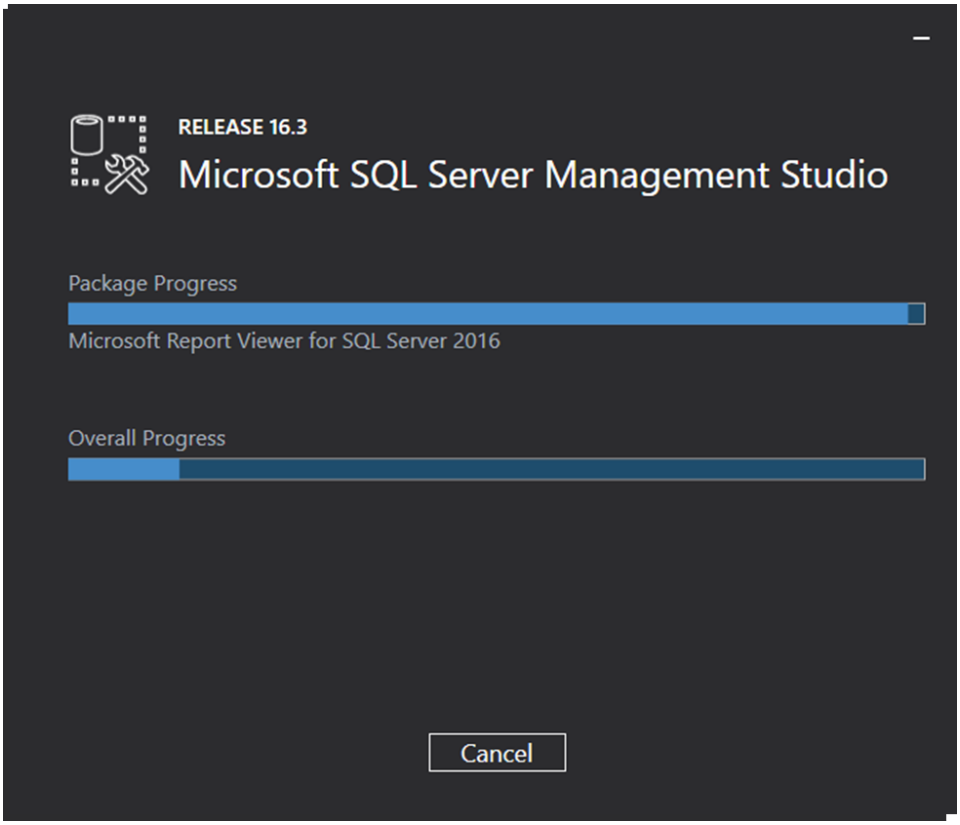
Για να ολοκληρωθεί το πακέτο εγκατάστασης της υποδομής της βάσης δεδομένων απαιτείται και η εγκατάσταση του διαχειριστικού εργαλείου SQL Server 2016 Management Studio όπου τα βήματα είναι τα εξής :

1. Εκτελούμε το Setup.exe αρχείο του SQL Server installer
2. Αφού εκτελεστεί το SQL Server installation center επιλέγουμε την δεύτερη επιλογή ¨install SQL Server Management Tool ¨ και στην συνέχεια πατάμε οκ



3. Ο οδηγός εγκατάστασης θα μας μεταφέρει σε μια ιστοσελίδα για τη λήψη του SQL Server Management Studio.

4.Μόλις γίνει η λήψη του εν λόγω αρχείου (SSMS) πατάμε το κουμπί εγκατάστασης για να ξεκινήσει η διαδικασία.



5. Αφήνουμε να ολοκληρωθεί η διαδικασία και έπειτα αφού η οθόνη, μας υποδειξεί επιτυχής εγκατάσταση, κάνουμε κλικ στο κουμπί closed και το SSMS εχεί εγκατασταθεί.

- **Εγκατάσταση ADSS Server**

Απαιτήσεις Συστήματος

Πριν από εγκατάσταση και για την σωστή λειτουργία του συστήματος θα πρέπει να πληρούνται οι παρακάτω απαιτήσεις:

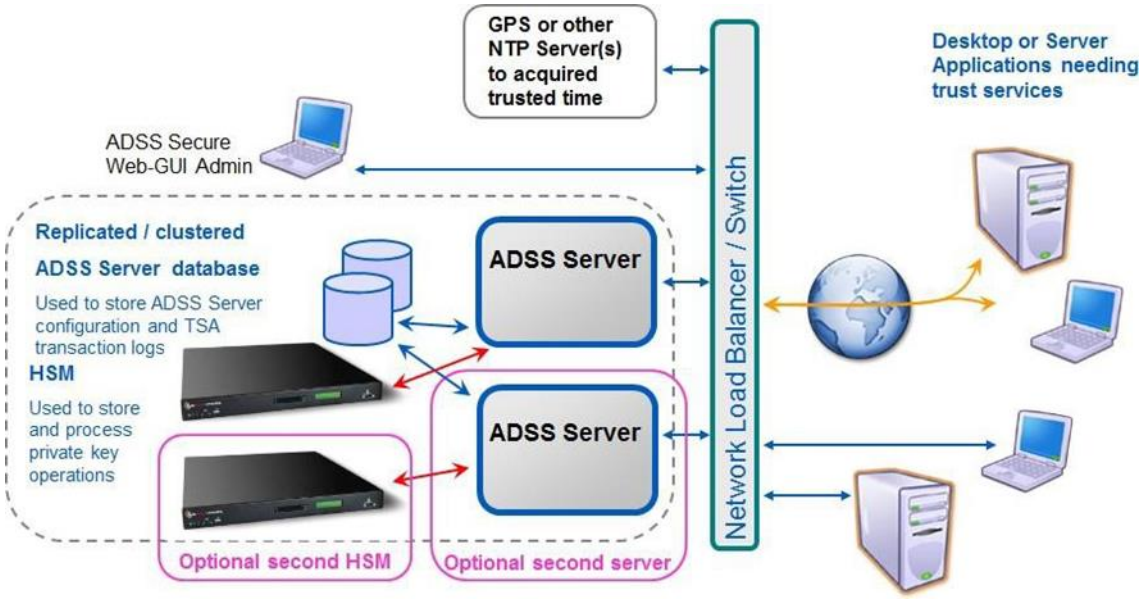
Components	Requirements
ADSS Server	ADSS Server is a Java EE 11 application, supported on these platforms: **Operating System** The following 64-bit operating systems are supported: • Windows Server 2019, 2016, 2012 R2, 2012 • Linux (RedHat v7.x, v8.x, CentOS v7.x, v8.x, SUSE) **Hardware** A modern multi-core CPU such as the Xeon E3-xxxx or E5-xxxx or E55xx or E56-xx or similar are recommended, with 16 GB RAM (min 8GB RAM) and 200 GB disk space. Additional RAM may be required to power signing or LTANS archive services. Roughly 0.5 GB to 1 GB of disk space is required to keep the trace logs per 100,000 service transactions. **Database** ADSS Server saves its configuration and transactional data in a database. The following databases are supported: • Microsoft SQL Server 2019, 2017, 2016, 2014, 2012 (Express, Standard, Web or Enterprise Edition) • Azure SQL Database (Database-as-a-service) • Oracle 19c, 12c • PostgreSQL v13.x, v12.x, v11.x, v10.x, v9.6.x • MySQL v8.x, Percona-XtraDB-Cluster v5.7.x and v8.0 About 1GB of database space is required to store the service logs of 100,000 transactions for each service, unless these are regularly auto archived or customised.
Optional Database Server	The database can be run on a separate server if preferred. This is recommended for high performance environments to allow all server resources to be directed to ADSS Server services. **Hardware:** A modern multi-core CPU such as the Xeon E3-xxxx or Xeon E5-xxxx or E55xx or E56-xx or similar range are recommended, with 16 GB RAM, typically 5-10 GB or more of disk space will be required depending on usage and transactional data / log retention requirements.

Client systems (systems sending service requests to ADSS Server)	Any reasonable system. ADSS Client SDK for Java API requires JRE v1.7 or above. ADSS Client SDK for .NET requires Microsoft .NET Framework 4.5 or above.
Operator Browsers	The following browsers are supported for ADSS Server Operators: • Google Chrome 70.x or above • Mozilla Firefox 60.x or above • Microsoft Edge 35.x or above • Microsoft Internet Explorer (IE) 11.x

Components	Requirements
Mobile Devices OS	For authorised remote signing, the mobile apps (iOS and Android) of Go>Sign Mobile will require the following OS versions: • iOS 9.0 or above • Android 6 (Marshmallow) or above
Optional HSMs	If required, the following Hardware Security Modules are supported: • Thales SafeNet Luna and ProtectServer HSMs • nCipher nShield Solo or Connect HSMs • Utimaco HSMs • Microsoft Azure Key Vault HSM • Amazon AWS Cloud HSM (Supported when ADSS Server deployed on Linux)
Optional DMZ proxy machine	A DMZ proxy server can be configured if required. The following DMZ proxy machines are supported: • Windows Server - Microsoft IIS 8.0 or above, Apache or IBM HTTP Server • Linux - Apache or IBM HTTP Server Use a reasonable CPU, 2GB RAM,100 MB disk space

Τυπικό Σενάριο Ανάπτυξης

Ένα τυπικό σενάριο ανάπτυξης εγκατάστασης σε ένα ADSS Server σχηματικά εμφανίζεται σαν το παρακάτω



Ο διακομιστής ADSS και η βάση δεδομένων που χρησιμοποιεί , μπορούν να εγκατασταθούν στον ίδιο υπολογιστή. Για υψηλή απόδοση των συστημάτων , συνιστάται η εγκατάσταση τους σε χωριστά λειτουργικά συστήματα.

Οι λεπτομέρειες που εμφανίζονται στο παραπάνω σενάριο είναι οι ελάχιστες απαιτήσεις συστήματος, αυτές μπορεί να χρειαστεί να αναθεωρηθούν για να δημιουργηθούν συγκεκριμένες απαιτήσεις χρήσης.

Εγκατάσταση Διακομιστή ADSS

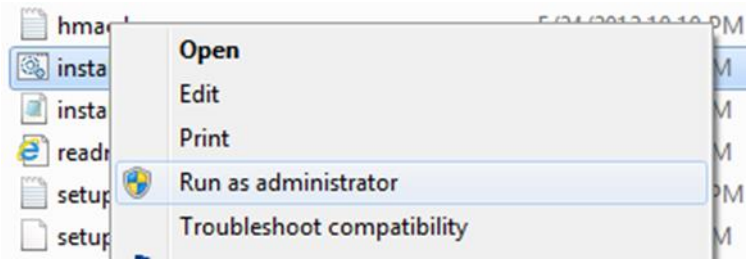
Ο ADSS Server είναι μια εφαρμογή Java EE με πλούσια λειτουργικότητα. Το αρχείο άδειας χρήσης του ADSS Server περιέχει έναν κατάλογο των υπηρεσιών/μοντέλων που έχουν αδειοδοτηθεί. Ο ADSS Server παραδίδεται με μια προσαρμοσμένη διανομή του Apache Tomcat και της Java ενώ η Ascertia συνεχίζει να τα αναβαθμίζει περιοδικά στις τελευταίες διαθέσιμες εκδόσεις.

Διαδικασία εγκατάστασης

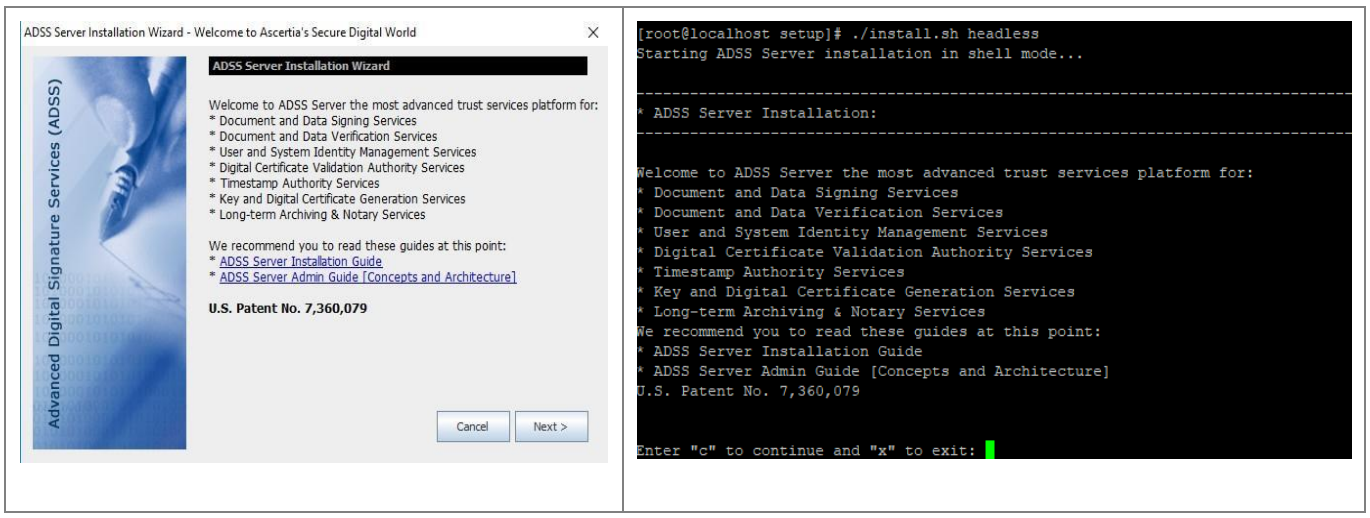
Το πρόγραμμα εγκατάστασης του ADSS Server πρέπει να αποσυμπιεστεί σε έναν κατάλληλο κατάλογο (που αργότερα θα αναφέρεται ως ADSS-Server-Home). Η διαδρομή του καταλόγου εγκατάστασης του ADSS Server δεν πρέπει να περιέχει χαρακτήρες κενού, διαφορετικά η διαδικασία εγκαταστάσης δεν θα ξεκινήσει.

Για να ξεκινήσουμε την εγκατάσταση, μεταβαίνουμε στον κατάλογο ADSS-Server- Home/setup.

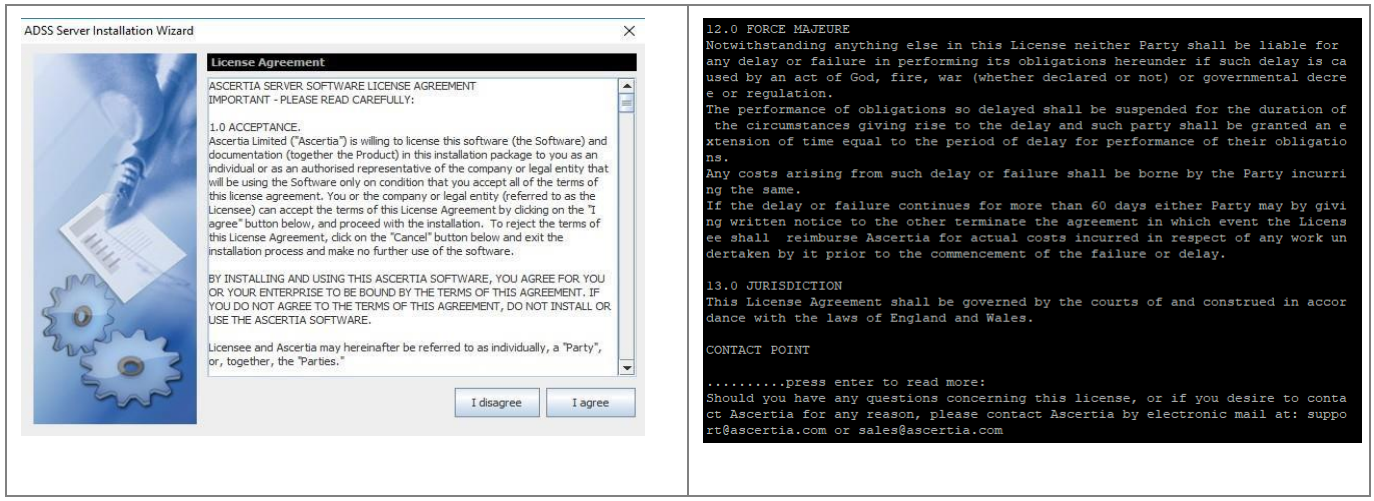
Επιλέγουμε να κάνουμε την εγκατάσταση σε περιβάλλον Windows , εγκαθιστούμε το αρχείο install. bat με δικαιώματα διαχειριστή, όπως φαίνεται παρακάτω (διαφορετικά οι υπηρεσίες του ADSS Server δεν θα καταχωρηθούν στον Πίνακα υπηρεσιών των Windows) για να ξεκινήσει το πρόγραμμα εγκατάστασης



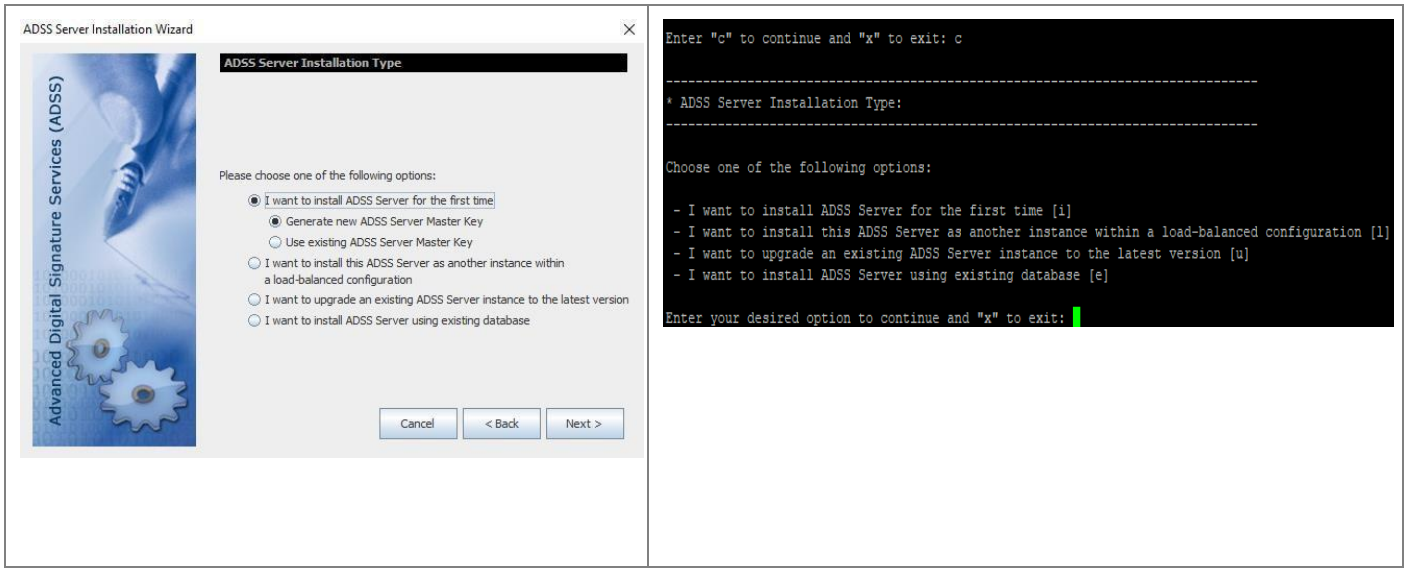
Εγκατάσταση του αρχείου **install.bat :**



Κάνουμε κλικ στο Επόμενο όπως δείχνει παρακάτω η οθόνη :



Στην επόμενη οθόνη πρέπει να αποδεχτούμε τους όρους και τις προϋποθέσεις κάνοντας κλικ στο “I agree” για να συνεχίσει η διαδικασία εγκατάστασης :



Υπάρχουν διάφορες διαθέσιμες επιλογές εγκατάστασης στον ADSS Server. Αυτές είναι:

I want to install ADSS Server for the first time – Χρησιμοποιούμε αυτή την επιλογή εάν θέλουμε να εγκαταστήσουμε τον τελευταίο ADSS Server χρησιμοποιώντας μια νέα/άδεια βάση δεδομένων. Για αυτόν τον τύπο εγκατάστασης είναι διαθέσιμες οι ακόλουθες επιλογές.

Generate new ADSS Server Master Key - Αυτή η επιλογή συνιστάται όταν εγκαθιστούμε τον ADSS Server για πρώτη φορά, είτε για δοκιμαστική είτε για παραγωγική χρήση. Αυτή η επιλογή προϋποθέτει ότι έχει ήδη δημιουργηθεί μια νέα βάση δεδομένων και ότι έχουν εκχωρηθεί τα κατάλληλα δικαιώματα πρόσβασης στη βάση δεδομένων στον χρήστη της βάσης δεδομένων.

Use Existing ADSS Server Master Key- Αυτή η επιλογή συνιστάται όταν το ήδη εγκατεστημένο κύριο κλειδί διακομιστή ADSS και οι ρυθμίσεις παραμέτρων πρέπει να χρησιμοποιηθούν για μια νέα αντιγραφόμενη περίπτωση διακομιστή ADSS. Αυτή η επιλογή προϋποθέτει ότι έχει ήδη δημιουργηθεί μια νέα βάση δεδομένων, ότι έχουν εκχωρηθεί τα κατάλληλα δικαιώματα πρόσβασης στη βάση δεδομένων στον χρήστη της βάσης δεδομένων και ότι έχουν ήδη εξαχθεί όλες οι ρυθμίσεις του υπάρχοντος διακομιστή ADSS.

I want to install this ADSS Server as another instance within a load-balanced configuration

Χρησιμοποιούμε αυτήν την επιλογή για να προσθέσουμε μια άλλη παρουσία ADSS Server σε μια υπάρχουσα εγκατάσταση ADSS Server. Μπορούμε να εγκαταστήσουμε όλα τα στοιχεία του ADSS Server (πυρήνας, κονσόλα ή/και υπηρεσία) σε πολλούς υπολογιστές για την καλύτερη εξυπηρέτηση των εισερχόμενων αιτήσεων. Η συγκεκριμένη επιλογή χρησιμοποιείται επίσης για την επίτευξη υψηλής διαθεσιμότητας (μηχανισμός εφεδρείας) εάν η κύρια παρουσία σταματήσει να ανταποκρίνεται. Η υψηλή διαθεσιμότητα υποστηρίζεται μόνο για τις περιπτώσεις ADSS Server Core και Console. Η περίπτωση υπηρεσίας ADSS Server μπορεί πάντα να εγκατασταθεί σε λειτουργία εξισορρόπησης φορτίου, όπου ένας εξισορροπιστής φορτίου (βασισμένος σε λογισμικό ή υλικό) διαχειρίζεται τις εισερχόμενες αιτήσεις και εάν κάποια από τις περιπτώσεις αποτύχει, ο εξισορροπιστής φορτίου μεταφέρει έξυπνα το φορτίο στις άλλες περιπτώσεις υπηρεσιών

I want to upgrade an existing ADSS Server instance to the latest version

Χρησιμοποιούμε αυτήν την επιλογή εάν έχουμε ήδη εγκαταστήσει μια παλαιότερη έκδοση του ADSS Server και θέλουμε να την αναβαθμίσουμε στην τελευταία έκδοση. Ο ADSS Server παρέχει έναν αυτοματοποιημένο τρόπο αναβάθμισης τόσο της βάσης δεδομένων όσο και της της εφαρμογής από τις προηγούμενες εκδόσεις (v3. 0 και άνω) στην τελευταία έκδοση, χωρίς να απαιτείται η εκτέλεση χειροκίνητων ενεργειών από τους διαχειριστές.

I want to install ADSS Server using existing database

Χρησιμοποιούμε αυτή την επιλογή εάν θέλουμε να εγκαταστήσουμε τον ADSS Server χρησιμοποιώντας μια υπάρχουσα βάση δεδομένων.

Εγκατάσταση του ADSS Server για πρώτη φορά

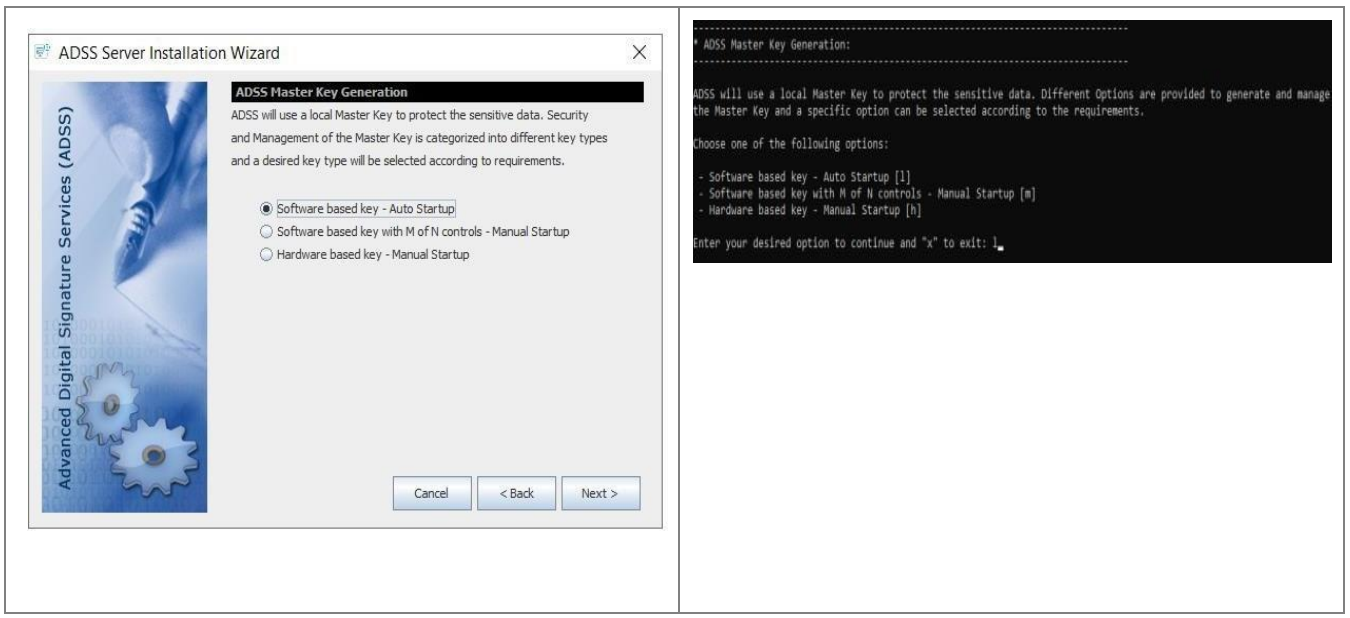
Μόλις επιλεγεί η απαιτούμενη επιλογή εγκατάστασης, θα οδηγηθούμε στην οθόνη για να επιλέξουμε έναν συγκεκριμένο τύπο κύριου κλειδιού. Ο διακομιστής ADSS χρησιμοποιεί δυναμικό κύριο κλειδί για να διασφαλίσει την προστασία και την ασφάλεια των δεδομένων. Για τη δημιουργία ενός δυναμικού κύριου κλειδιού, ο ADSS Server παρέχει στους χρήστες του πολλαπλούς μηχανισμούς που κατηγοριοποιούνται σε διαφορετικούς τύπους κλειδιών. Αυτά περιλαμβάνουν:

- Software based key – Auto Startup
- Software based key with M of N controls – Manual Startup
- Hardware based key – Manual Startup

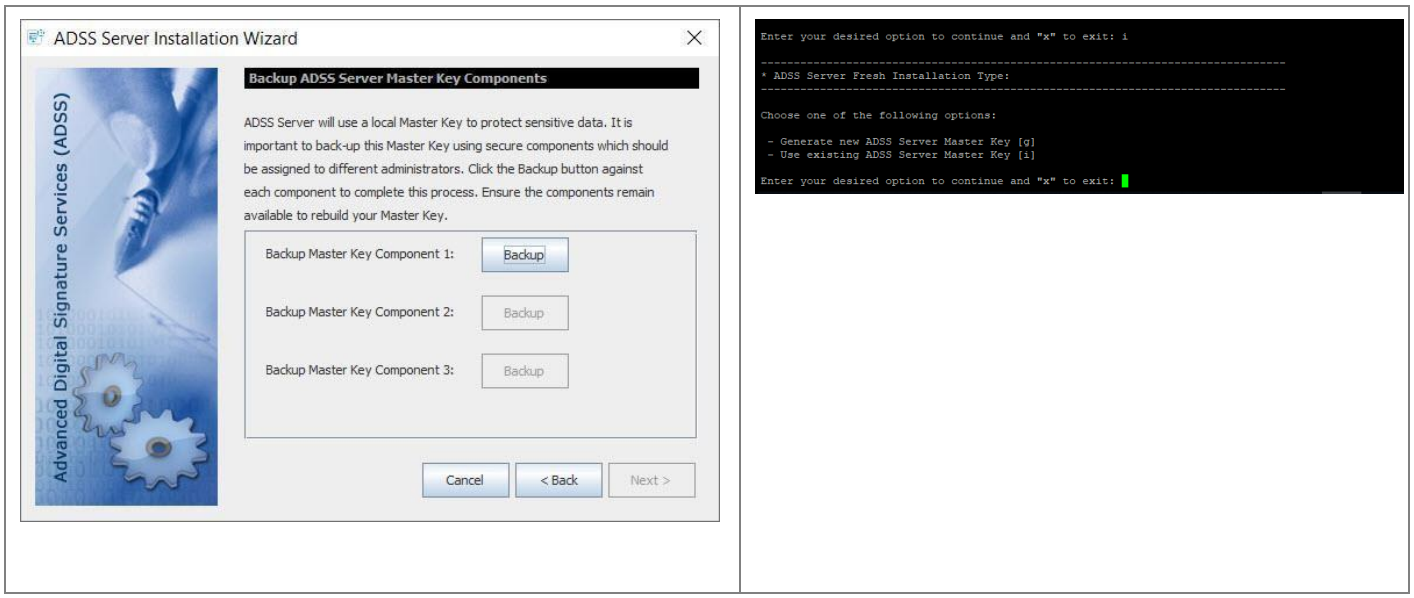
Ο επιθυμητός τύπος κλειδιών θα επιλεγεί ανάλογα με την απαίτηση. Οι λεπτομέρειες για κάθε τύπο κλειδιού εξηγούνται παρακάτω:

- **Software Based Key – Auto Startup**

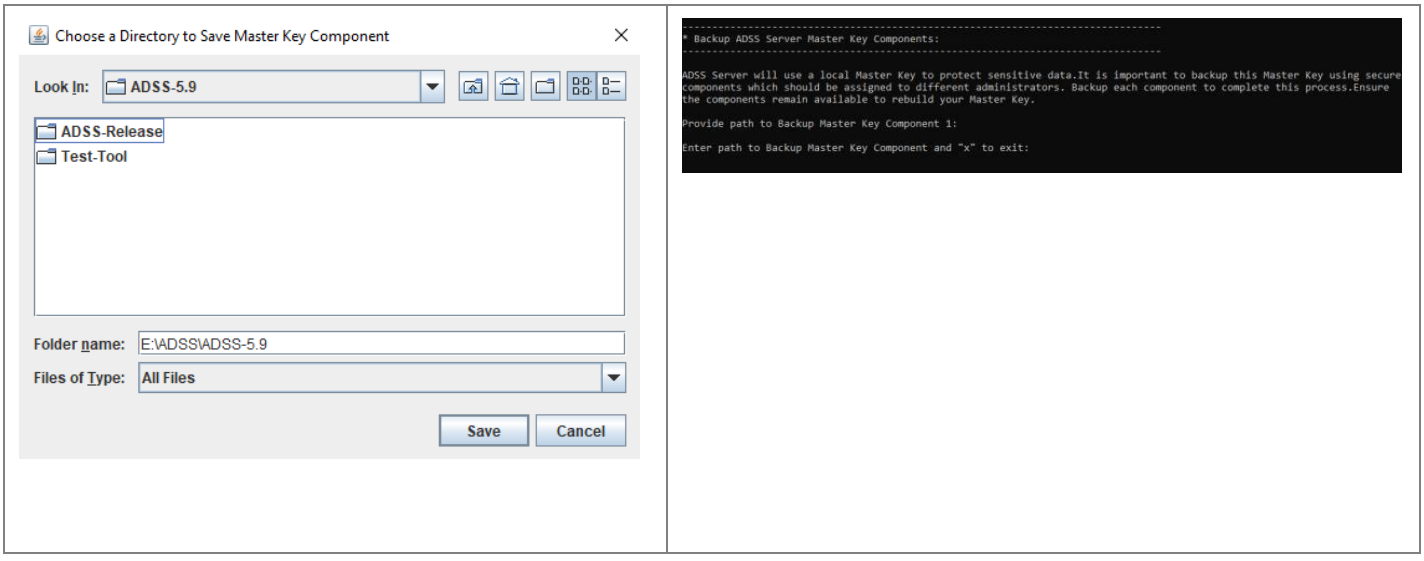
Σε αυτό το σύστημα, το κύριο κλειδί παράγεται χρησιμοποιώντας μια πηγή κρυπτογράφησης λογισμικού και προστατεύεται από τον διακομιστή ADSS. Το κύριο κλειδί μπορεί να ανανεώνεται σε τακτικά για να διασφαλίζεται η ασφάλεια. Εδώ, το κύριο κλειδί θα προστατεύεται από τον ίδιο τον διακομιστή ADSS, επομένως το ADSS θα ξεκινά χωρίς καμία παρέμβαση του χειριστή. Κατά τη διαδικασία εγκατάστασης θα εμφανιστεί η παρακάτω οθόνη:

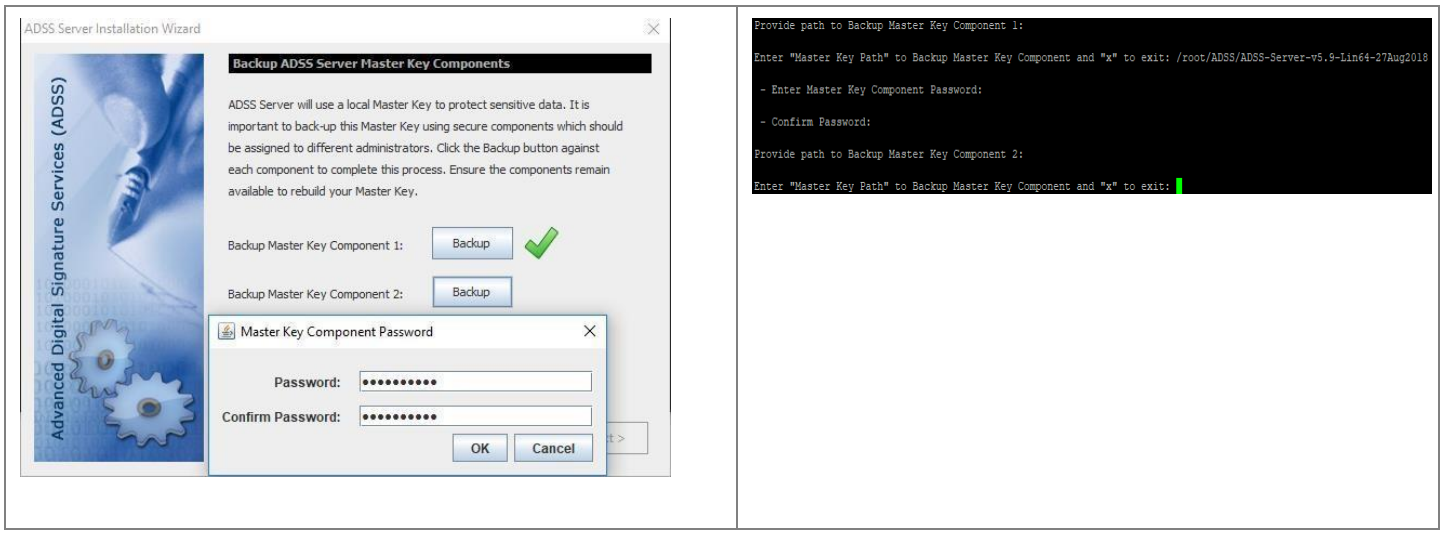


Κατά την εγκατάσταση θα δημιουργηθεί ένα Master key το οποίο θα μας ζητηθεί από το πρόγραμμα να κρατήσουμε ένα αντίγραφο ασφάλειας αυτού του κλειδιού με την μορφή των παρακάτω τριών στοιχείων :

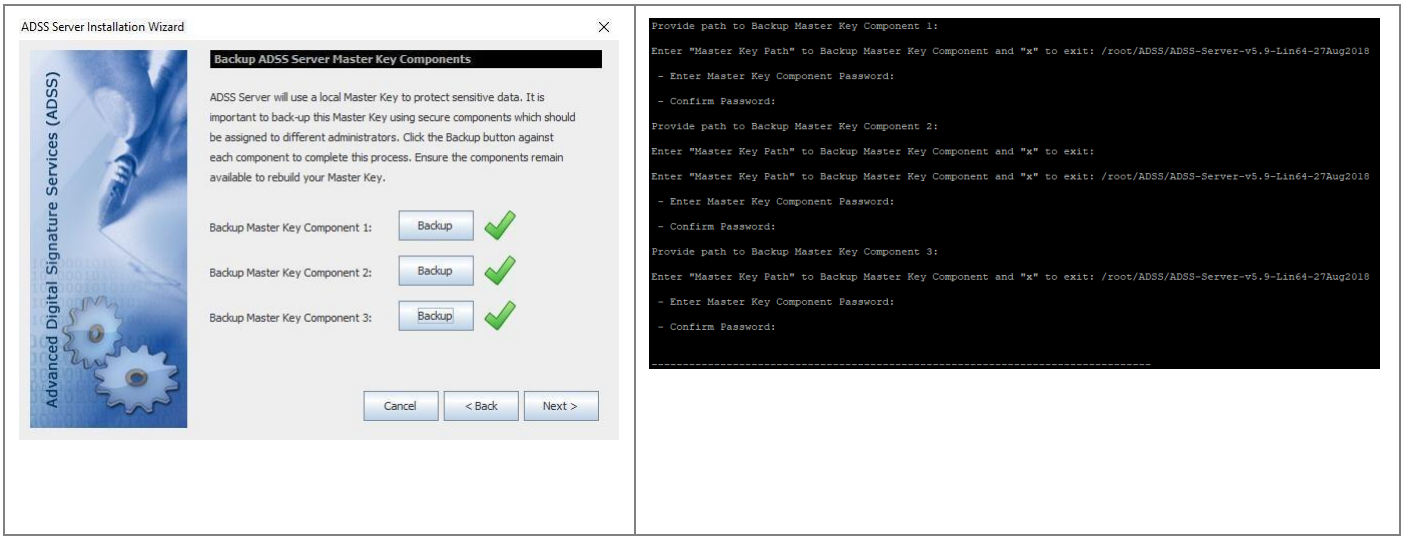


Σε κάθε κουμπί ¨Back up¨ το λογισμικό μας ζητάει να δώσουμε έναν κωδικό ασφάλειας για να εξασφαλίσει και να κρυπτογραφήσει τα αντίγραφα των κλειδιών ασφάλειας.

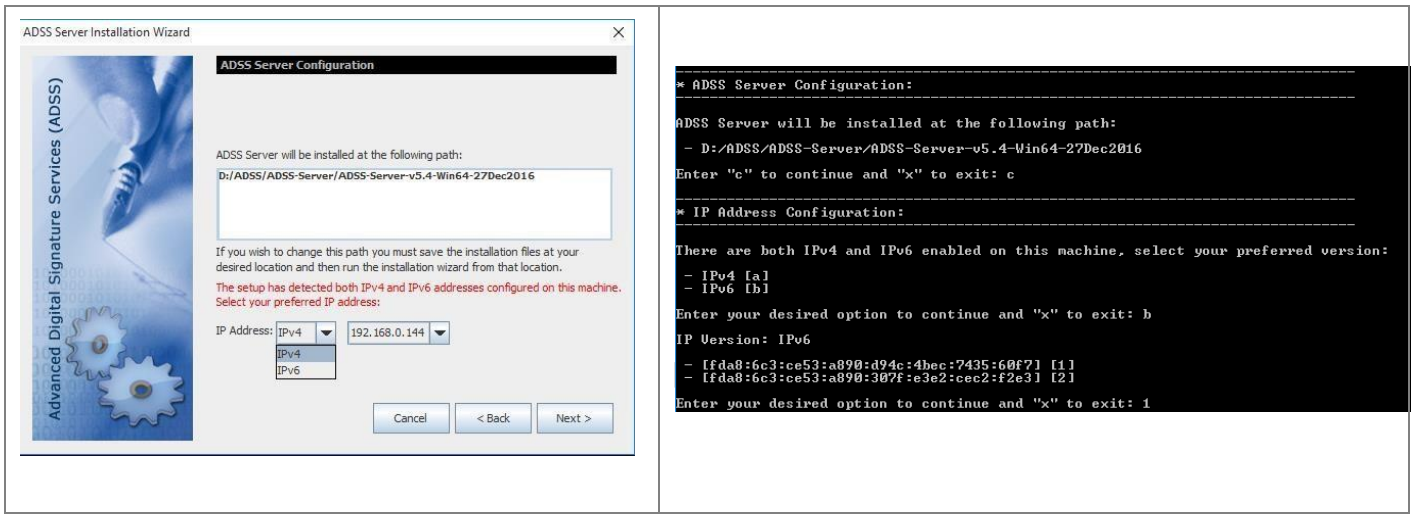




Συνιστάται η χρήση διαφορετικού κωδικού πρόσβασης για κάθε στοιχείο του κύριου κλειδιού. Μετά την ολοκλήρωση της δημιουργίας αντιγράφων ασφαλείας εμφανίζεται η ακόλουθη οθόνη:

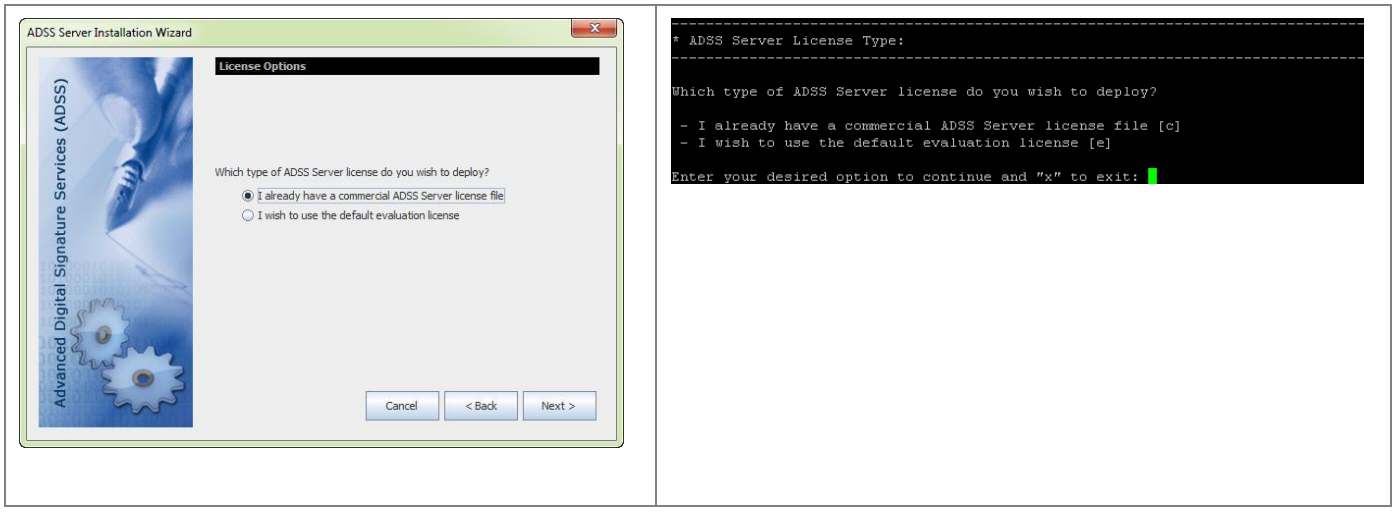


Μόλις κάνουμε κλικ στο κουμπί Επόμενο η οθόνη δείχνει τη διαδρομή στην οποία θα εγκατασταθεί το λογισμικό ADSS Server και επιτρέπει την επιλογή του σχήματος IP για την εγκατάσταση του ADSS Server

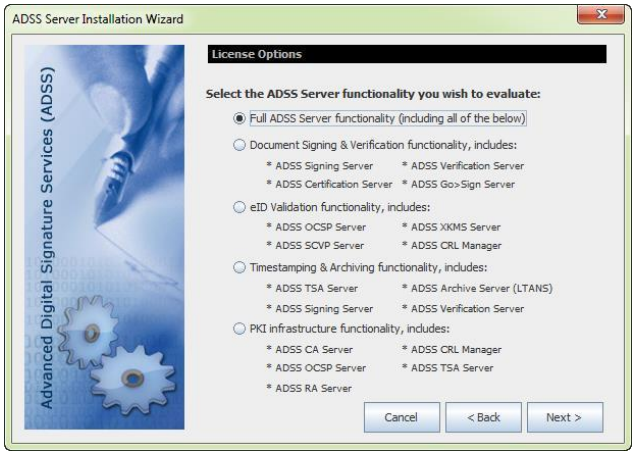


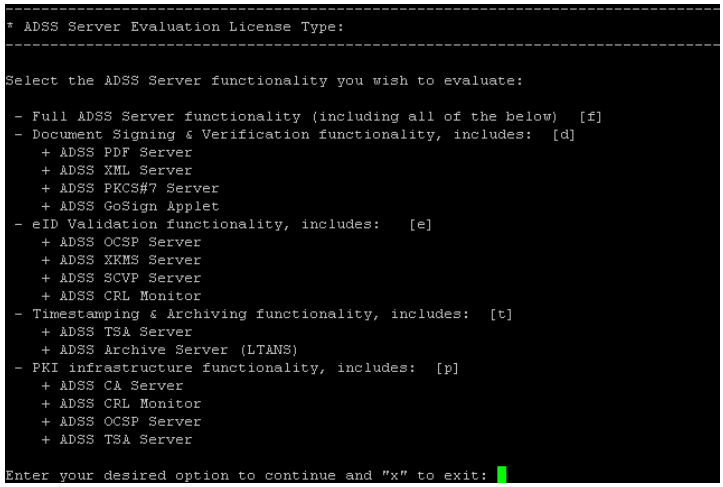
Κάνοντας κλικ στο "Επόμενο" εμφανίζεται η οθόνη Επιλογές άδειας χρήσης:

Επιλέγουμε το “I wish to use the default evaluation license”. Όπου το όριο της άδειας αξιολόγησης είναι ένας μήνας από την ημερομηνία της πρώτης εγκατάστασης.



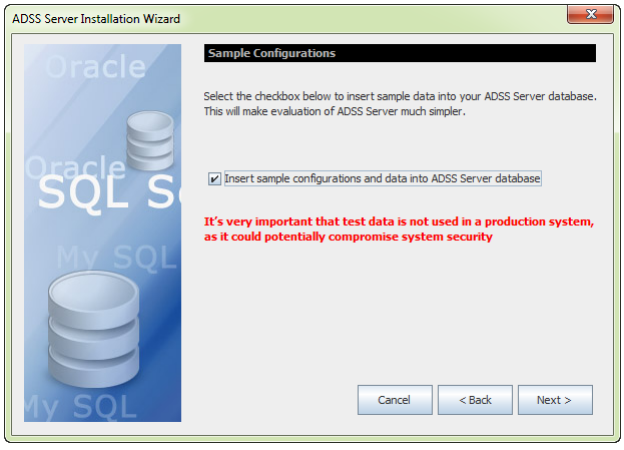
Στην επόμενη οθόνη εμφανίζονται όλες οι επιλογές των πακέτων εγκατάστασης αναλόγως το σενάριο που θέλει να εκτελέσει ένας χρήστης ή μία εταιρεία να χρησιμοποιήσει το λογισμικό επιλέγει και το αντίστοιχο πακέτο. Για τα δικά μας σενάρια επιλέξαμε την πακέτο που εμπεριέχει όλες τις υπηρεσίες του λογισμικού.

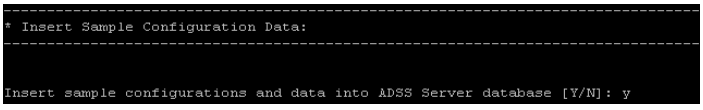




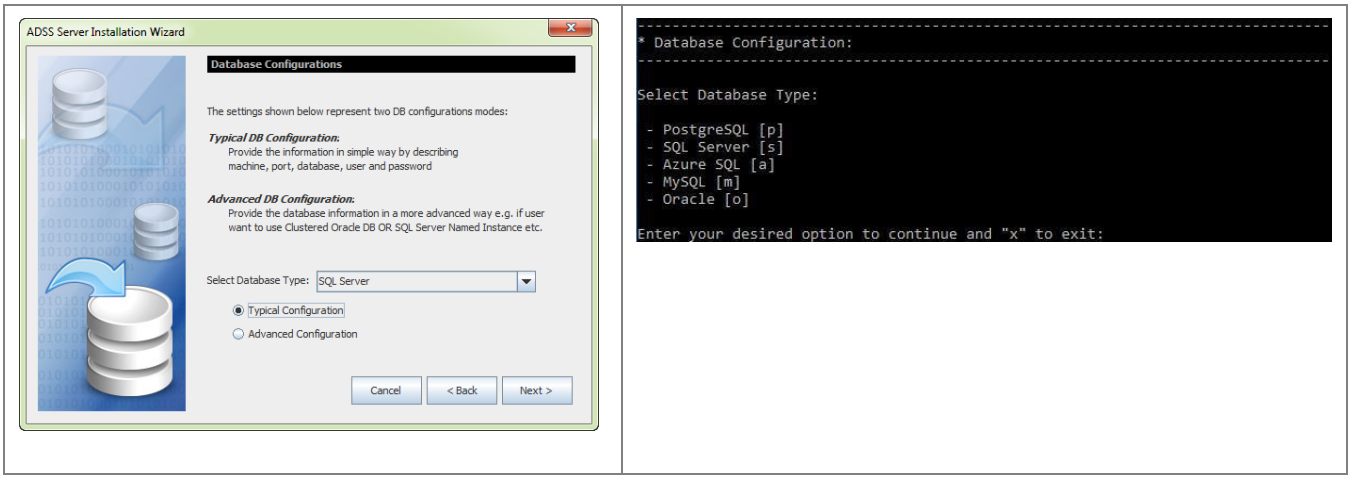
Κάνουμε κλικ στο επόμενο για να προχωρήσουμε την εγκατάσταση

Η επιλογή αυτή θα εισάγει τα δεδομένα του δείγματος στα δεδομένα για να επιτρέψει την άμεση δοκιμή/αξιολόγηση του ADSS Server.





Διαμόρφωση της βάσης δεδομένων

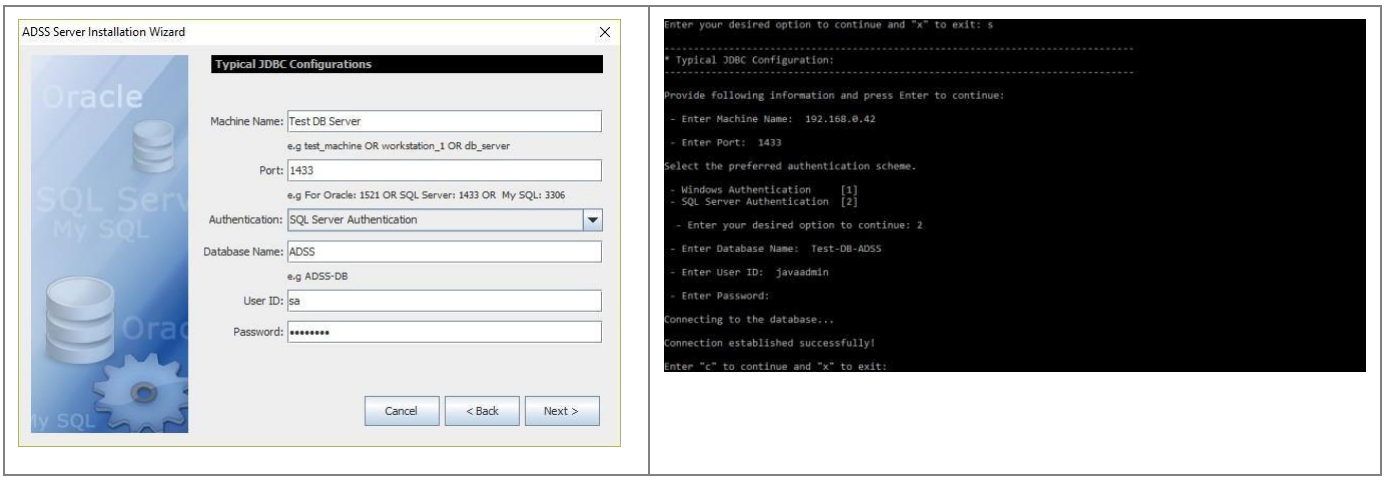


Στην οθόνη αυτή επιλέγουμε τον τύπο της βάσης δεδομένων (π. χ. SQL Server) και τον τύπο διαμόρφωσης (Τυπική/Προηγμένη)

Οι τυπικές ρυθμίσεις μάς επιτρέπουν να καθορίσουμε το όνομα του διακομιστή βάσης δεδομένων, το όνομα της βάσης δεδομένων, τη θύρα. Η Ρύθμιση για προχωρημένους επιτρέπει επίσης τη διαμόρφωση της διεύθυνσης URL του προγράμματος οδήγησης βάσης δεδομένων χαμηλού επιπέδου, των JARs κλπ. Αν δεν υπάρχει εμπειρία σε αυτόν τον τομέα, συνιστάται η τυπική διαμόρφωση.

Παράμετροι σύνδεσης με τη βάση δεδομένων

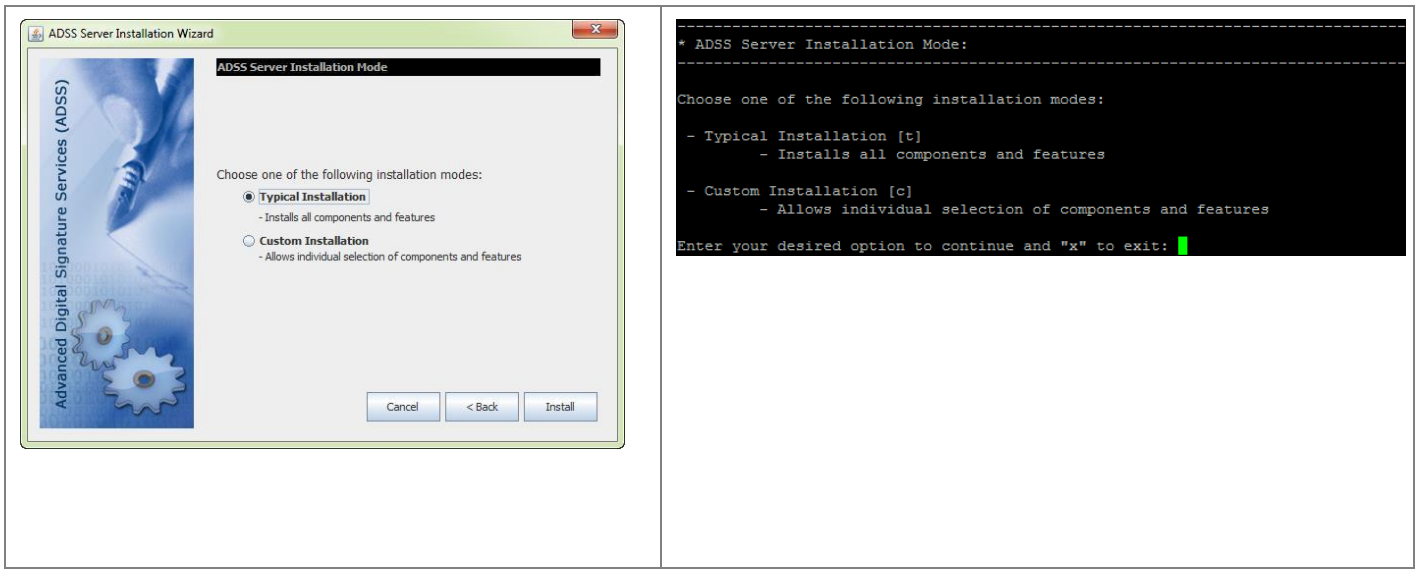
Επιστρέφοντας στην εγκατάσταση του ADSS Server, επιλέγοντας "Typical Configurations" στην οθόνη Database Configurations και πατώντας Next εμφανίζεται η ακόλουθη οθόνη:



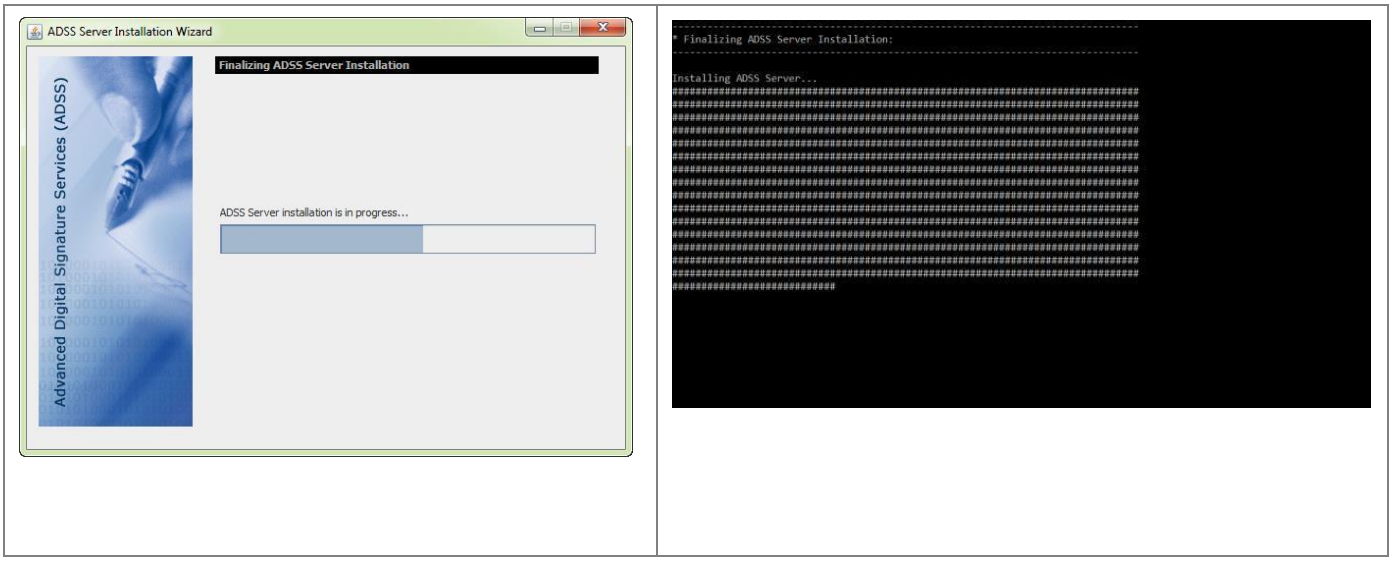
Τα στοιχεία διαμόρφωσης έχουν ως εξής:

Item	Description
Machine Name	The system name or IP address of the machine where the database server is running, e.g. asc_db_server. If you are installing ADSS Server on the same machine as the database, please enter "localhost" as the Machine Name.
Port	The port number to be used to connect to the database e.g. 1433 for SQL Server.
Authentication Scheme	In case of ADSS Server installation with SQL Server as Database, user can be authenticated by two ways i.e.: • SQL Server Authentication • Windows Authentication For SQL Server Authentication, user needs to enter the User Name and Password of SQL Server. Whereas in Windows Authentication, these fields will be disabled, and user will be authenticated by the logged-in user Windows/Domain credentials.
	Note: Under typical JDBC configurations only Kerberos authentication is supported. For NTLM based authentication use the advanced JDBC configurations.
Database Name	The name of database for ADSS Server. This can be a newly created empty database or an existing database. Make sure the database exists before clicking the Next button.
User ID	The user ID used by ADSS Server to connect to the database. Ensure that this user exists and has the appropriate privileges to create and access tables.
Password	The corresponding password for the User ID.

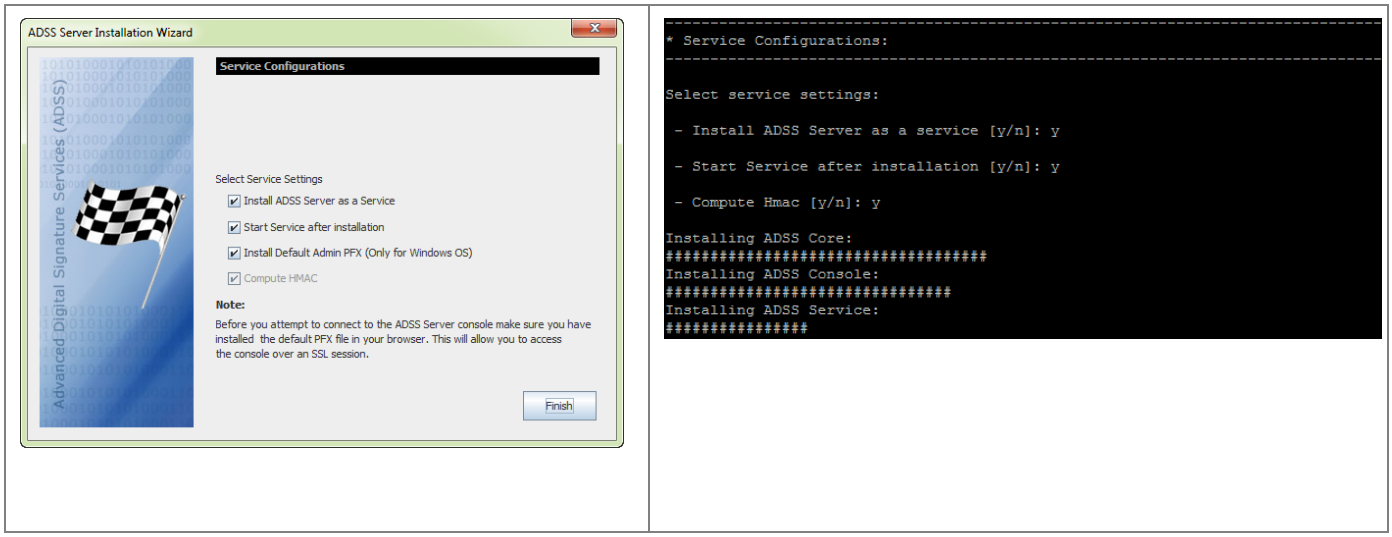
Στο επόμενο βήμα διαλέγουμε την τυπική εγκατάσταση – Η επιλογή αυτή θα εγκαταστήσει όλα τα στοιχεία του ADSS Server με προεπιλεγμένες παραμέτρους μνήμης, δηλαδή Core (1024 MB), Console (1024 MB) και Service (2048 MB) στο τρέχον σύστημα.



Μετά την παροχή του μέγιστου ορίου μνήμης, κάνουμε κλικ στο κουμπί Install και ξεκινά η διαδικασία εγκατάστασης, συμπεριλαμβανομένων και την εκτέλεση των σεναρίων βάσης δεδομένων και την ενημέρωση της διαμόρφωσης αρχείων.



Μόλις ολοκληρωθεί η εγκατάσταση, εμφανίζεται η ακόλουθη οθόνη:



Install ADSS Server as a service - (η προεπιλεγμένη συνιστώμενη επιλογή) Σε περιβάλλον Windows, τα επιλεγμένα στοιχεία του ADSS Server θα καταχωρηθούν στον πίνακα υπηρεσιών των Windows με τα ακόλουθα ονόματα:

- Ascertia-ADSS-Console
- Ascertia-ADSS-Core
- Ascertia-ADSS-Service

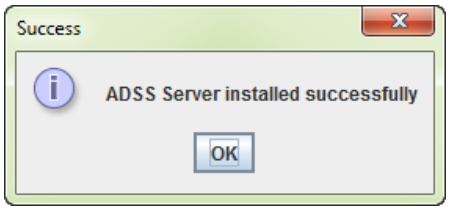
Start Service after installation Αυτή η επιλογή είναι διαθέσιμη μόνο εάν έχει επιλεγεί η προηγούμενη επιλογή. Εάν επιλεγεί, οι εγγεγραμμένες υπηρεσίες θα εκκινούνται αυτόματα μετά την εγκατάσταση, εάν το κύριο κλειδί δημιουργηθεί με την επιλογή "Software based key - Auto Startup". Εάν το κύριο κλειδί δημιουργήθηκε με τις άλλες δύο επιλογές όπου απαιτείται χειροκίνητη εκκίνηση, τότε οι υπηρεσίες δεν θα ξεκινήσουν αυτόματα μετά την εγκατάσταση.

Install Default Admin PFX (Only for Windows OS) Επιλέγοντας αυτή την επιλογή θα εγκαταστήσουμε το προεπιλεγμένο πιστοποιητικό ελέγχου ταυτότητας πελάτη στο keystore του MS CAPI, το οποίο σας επιτρέπει να συνδεθείτε στην κονσόλα του ADSS Server χρησιμοποιώντας τον χρήστη Admin (αυτό απαιτείται μόνο όταν ο ADSS Server εγκαθίσταται για πρώτη φορά).

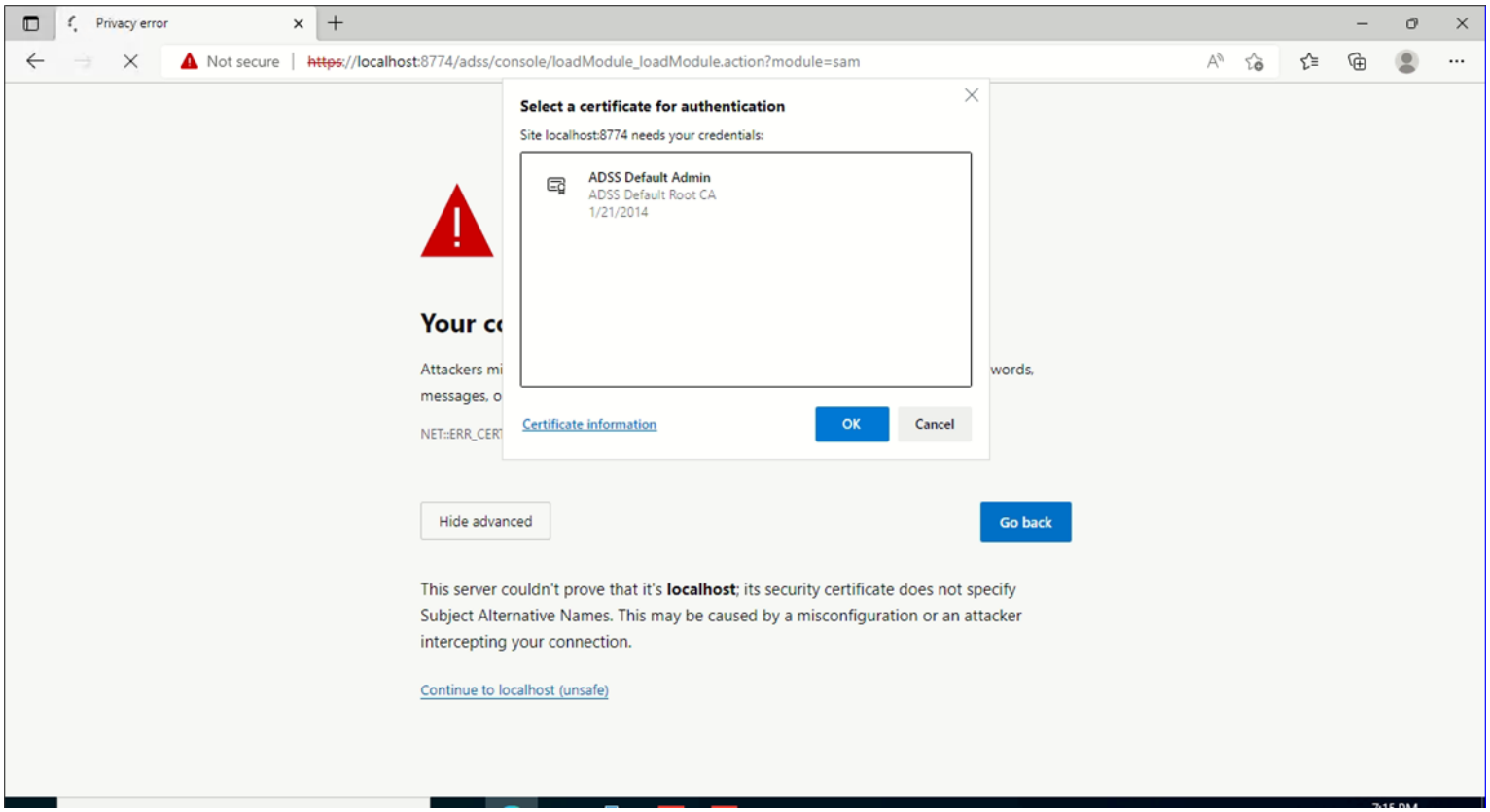
Αυτή η επιλογή είναι απενεργοποιημένη στο UNIX και το αρχείο adss_default_admin. pfx πρέπει να εισαχθεί στο Firefox ή σε άλλο πρόγραμμα περιήγησης στο διαδίκτυο, χειροκίνητα από τον κατάλογο ADSS-Server-Home/setup/certs/ προκειμένου να συνδεθούμε στην ADSS Server Κονσόλα.

Compute HMAC – Το HMAC είναι ένα κρυπτογραφικό άθροισμα ελέγχου που υπολογίζεται από τον ADSS Server σε κάθε εγγραφή στη βάση δεδομένων του ADSS Server για τον εντοπισμό μη

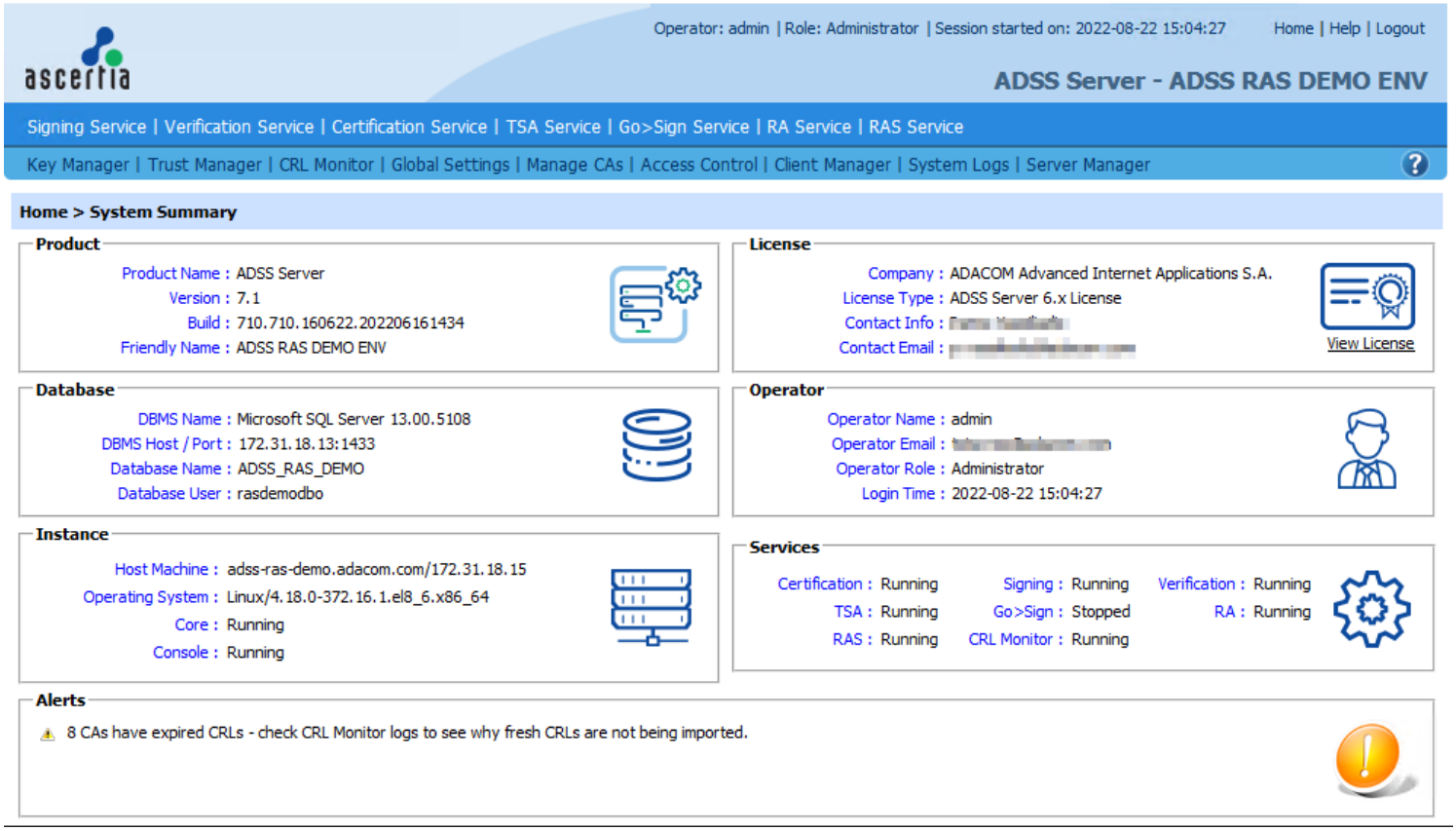
εξουσιοδοτημένων αλλαγών στη βάση δεδομένων. Ο υπολογισμός του HMAC είναι υποχρεωτικός για μια νέα εγκατάσταση, οπότε η επιλογή είναι επιλεγμένη και γκριζαρισμένη. Κάνοντας κλικ στο κουμπί Finish, ολοκληρώνεται ο οδηγός εγκατάστασης του ADSS Server και εμφανίζεται ένα μήνυμα επιτυχημένης εγκατάστασης :



Αφού ολοκληρωθεί η βασική εγκατάσταση επιλέγουμε έναν browser και συνδεόμαστε στο localhost:8774/adss, Όπου θα μας ζητήσει το πιστοποιητικό του διαχειριστή που δημιουργήσαμε για να πάρουμε πρόσβαση.

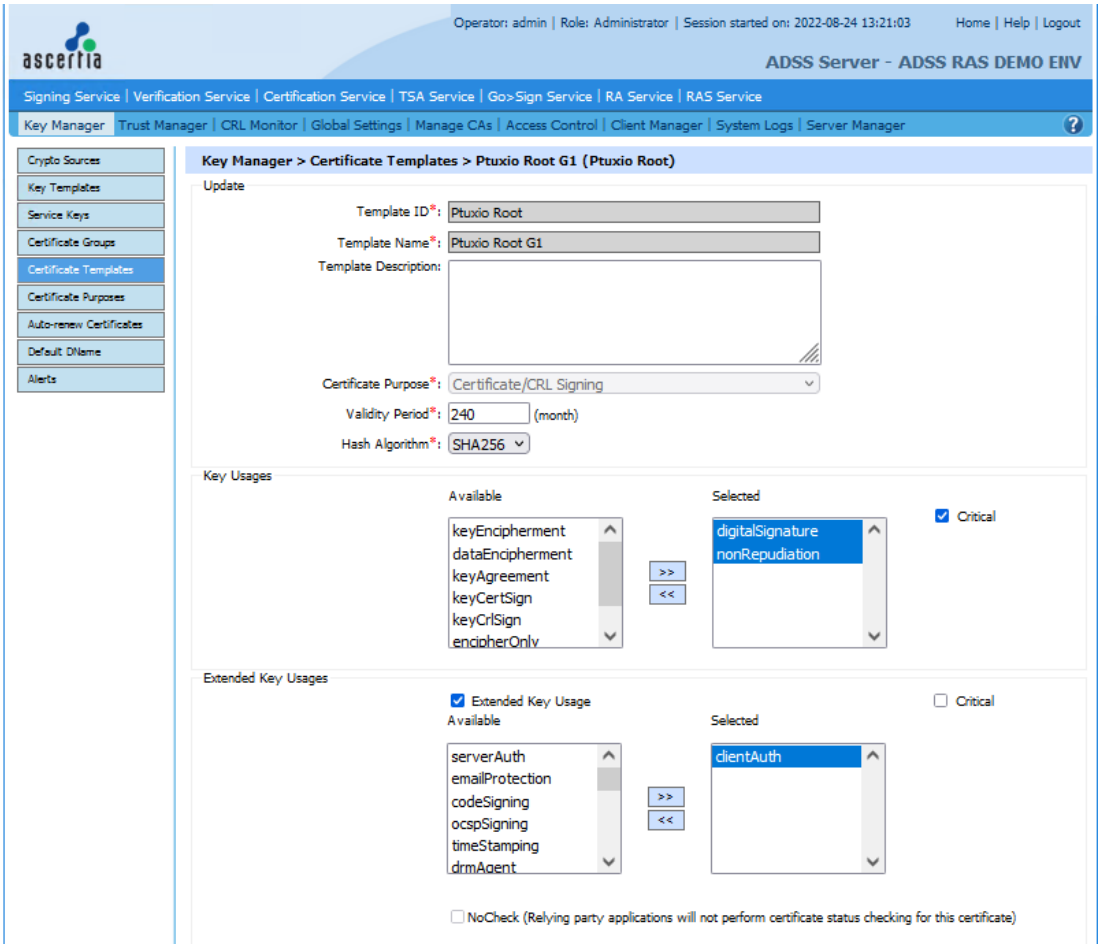


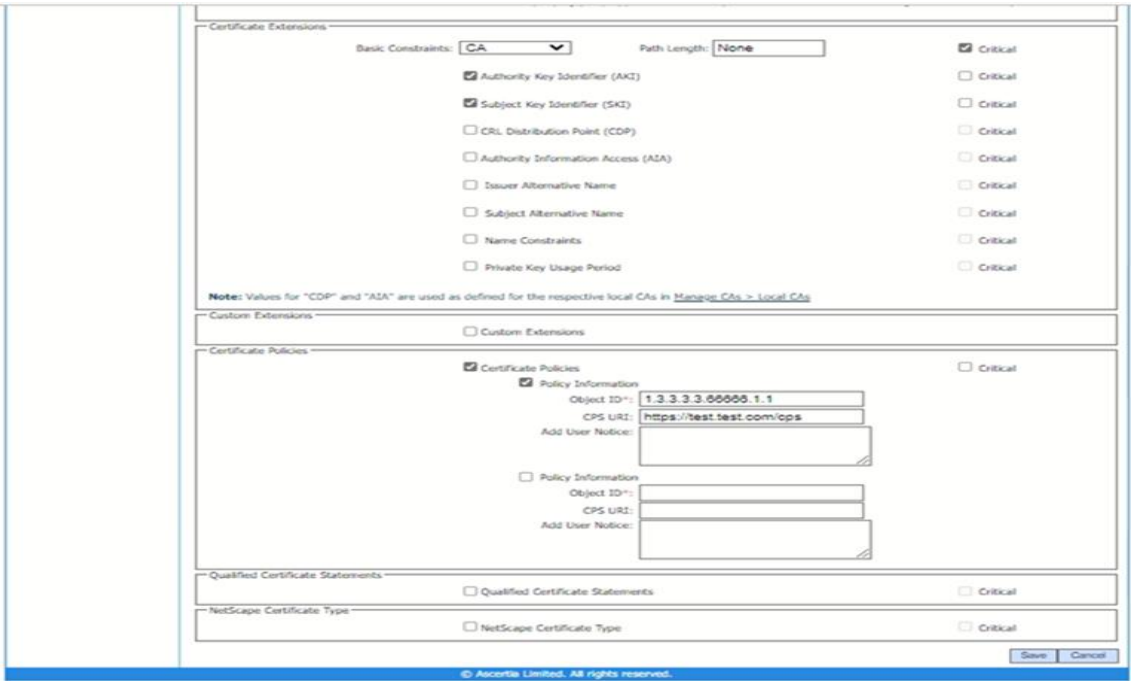
Εφόσον γίνει η πιστοποίηση παίρνουμε πρόσβαση στην κεντρική κονσόλα του ADSS server.



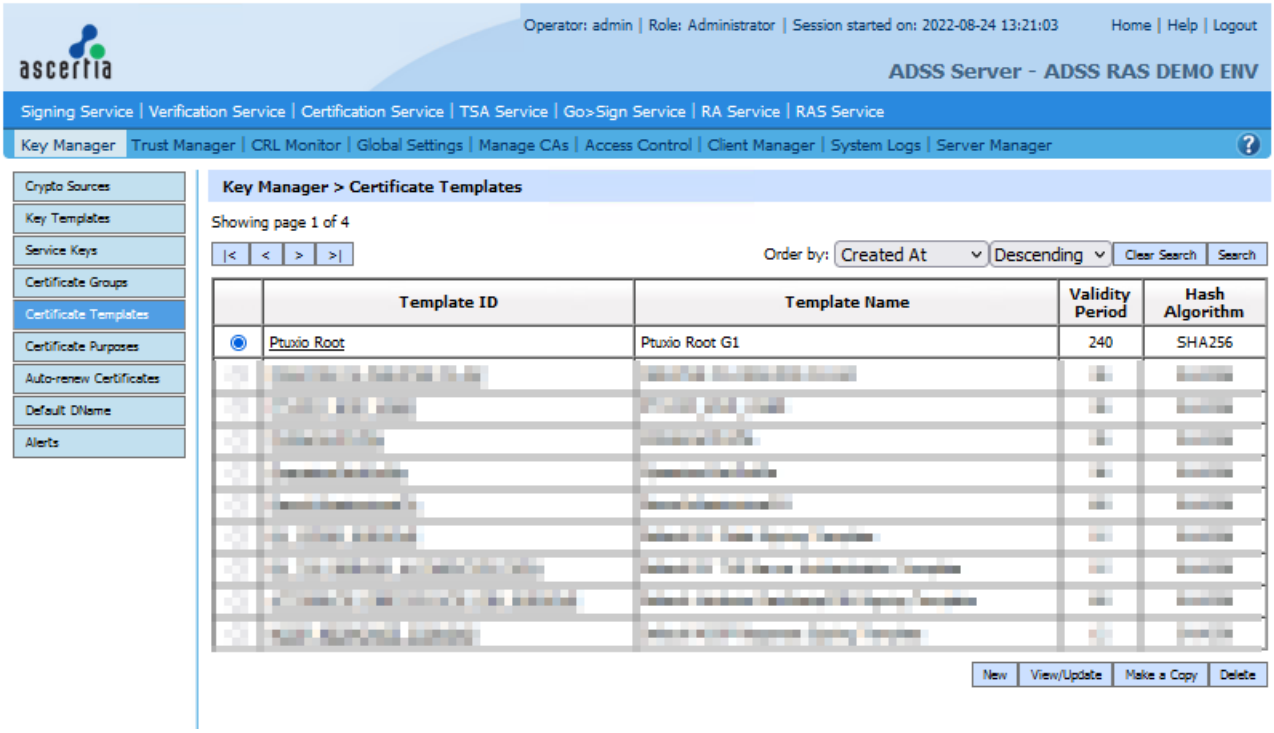
Στην συνέχεια μεταβαίνουμε στην καρτέλα Key Manager → Certificates Templates ώστε να δημιουργήσουμε το προφίλ το πιστοποιητικού της Αρχής Πιστοποίησης (Root CA)

Το προφίλ περιέχει στοιχεία όπως διάρκεια ζωής του πιστοποιητικού , Key Usages, Extended Key Usages και Certificates Polices

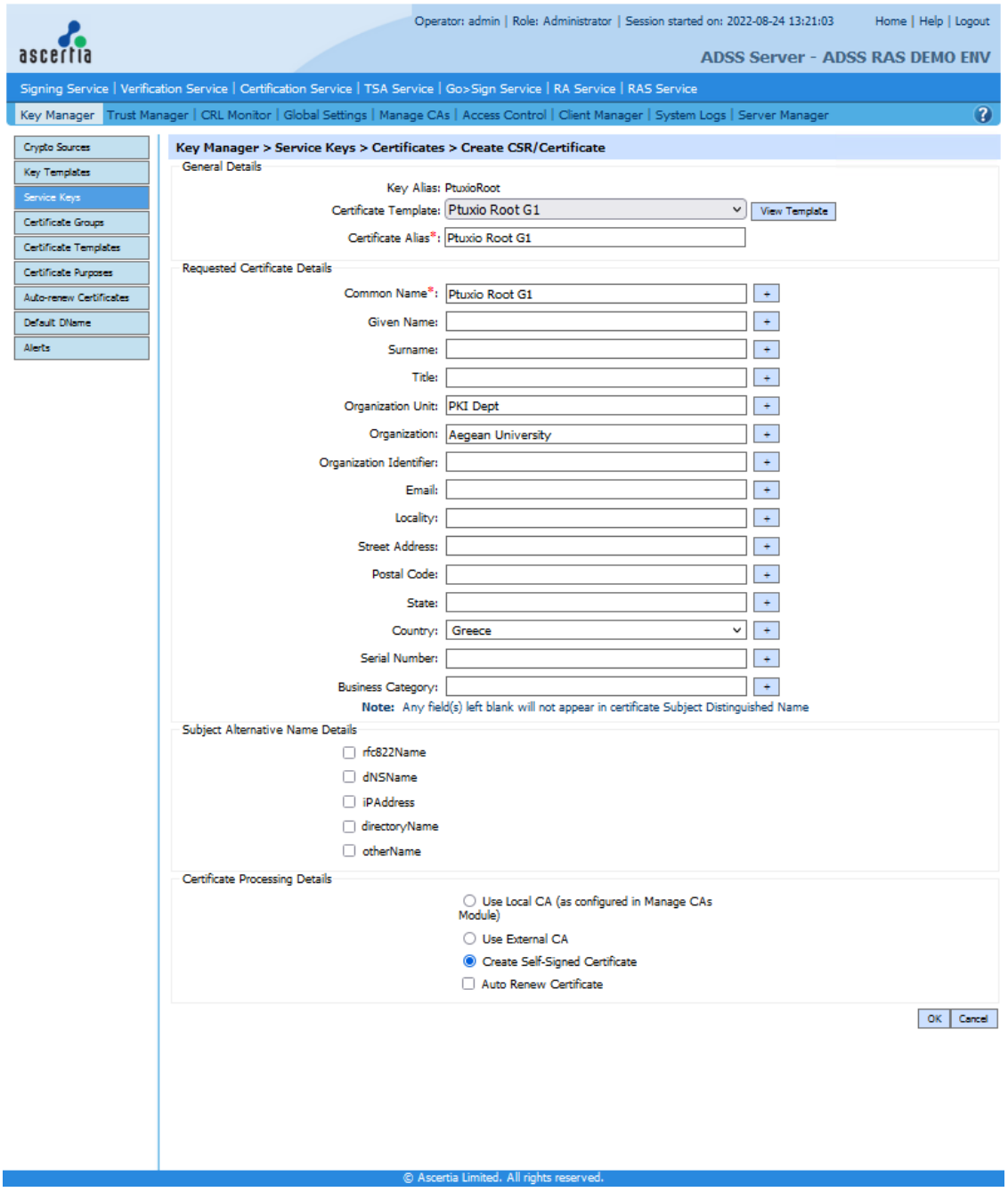




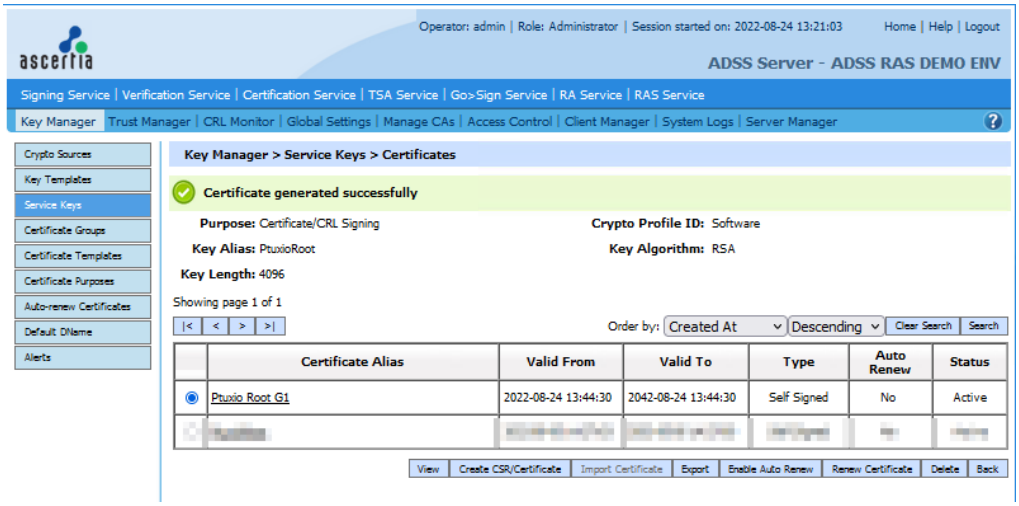
Πατώντας save το προφίλ δημιουργείται με επιτυχία όπως διαπιστώνουμε παρακάτω



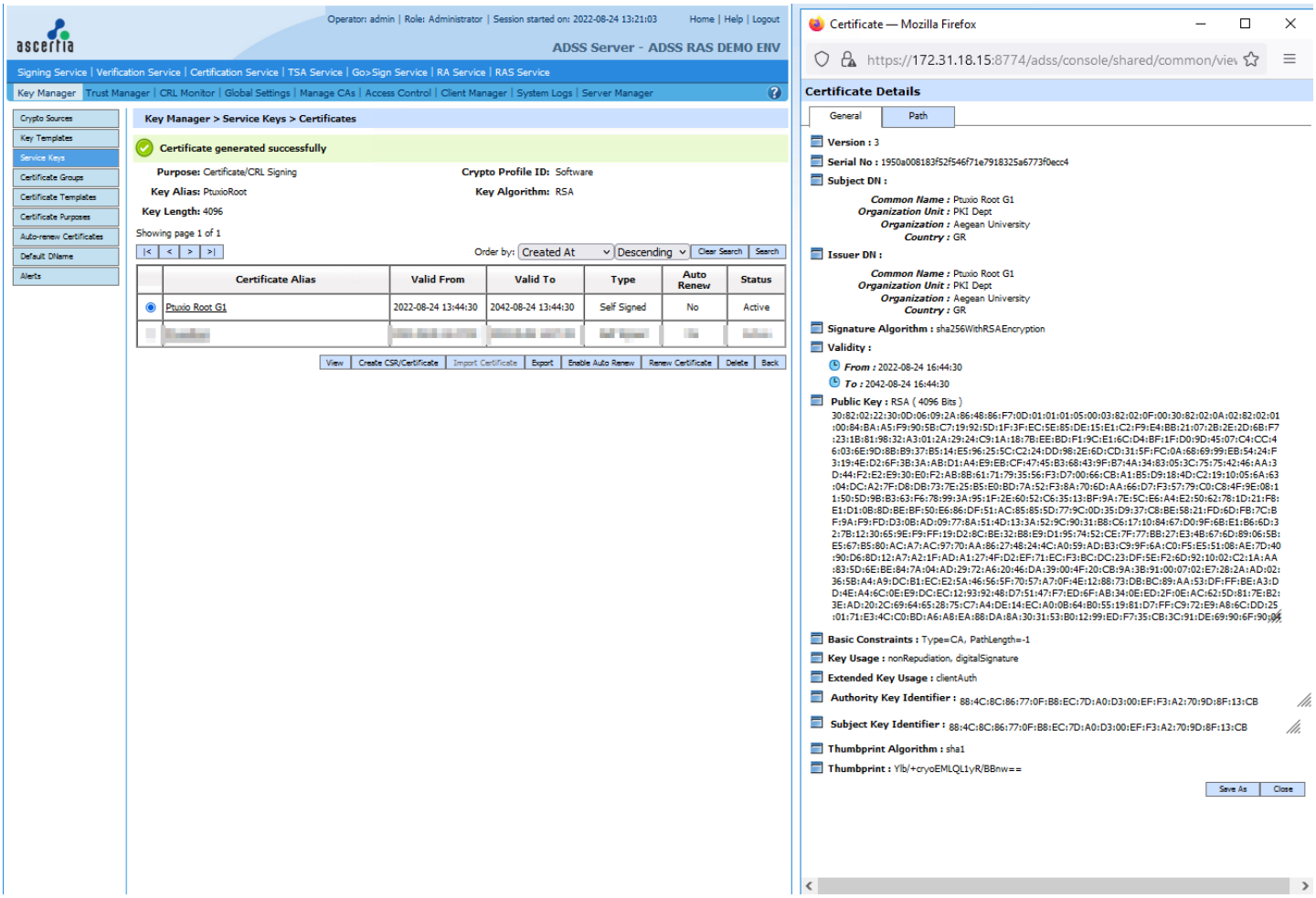
Έχοντας ολοκληρώσει το προφίλ του πιστοποιητικού μεταβαίνουμε στην κατηγορία Service Key όπου θα δημιουργήσουμε τα κλειδιά και θα συντάξουμε τις πληροφορίες που θα περιέχει. Το πιστοποιητικό όντας Αρχής Πιστοποίησης (Root CA) θα την υπογράψει ο εαυτός της.



Πατώντας ΟΚ το πιστοποιητικό δημιουργείτε με επιτυχία σύμφωνα με τα στοιχεία που του ορίστηκαν .

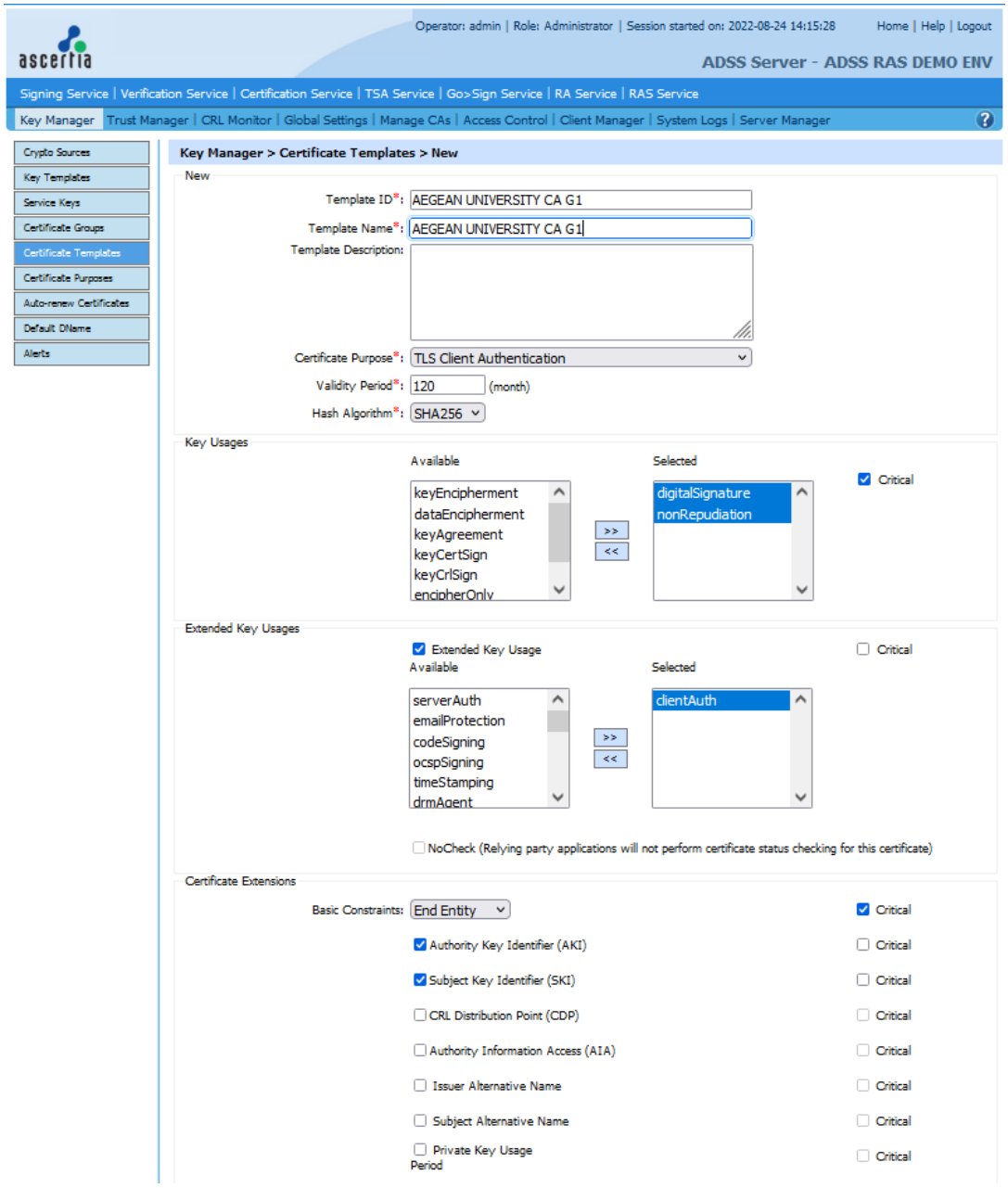


Στην παρακάτω εικόνα παρουσιάζεται το πιστοποιητικό Αρχής Πιστοποίησης (Root CA) και τα στοιχεία που συμπεριλάβαμε.

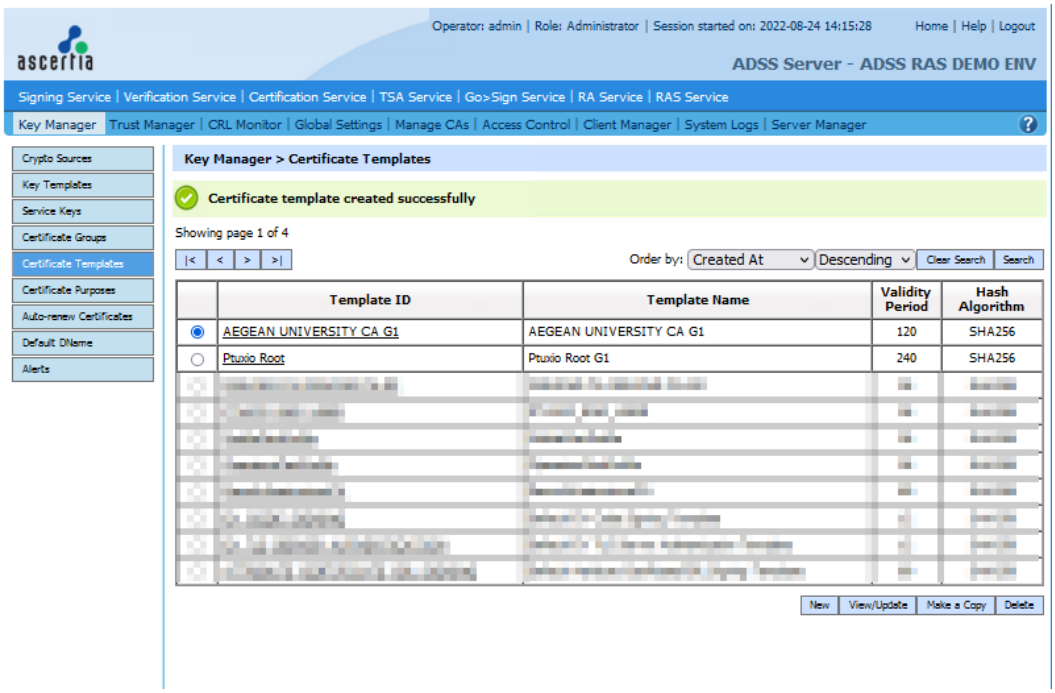


Στην συνέχεια μεταβαίνουμε εκ νέου στην καρτέλα Key Manager → Certificates Templates ώστε να δημιουργήσουμε αυτή την φόρα το προφίλ του πιστοποιητικού της Ενδιάμεσης Αρχή Πιστοποίησης (Intermediate CA – Certificate Authority)

Το προφίλ επίσης περιέχει στοιχεία όπως διάρκεια ζωής του πιστοποιητικού , Key Usages, Extended Key Usages και Certificates Polices.

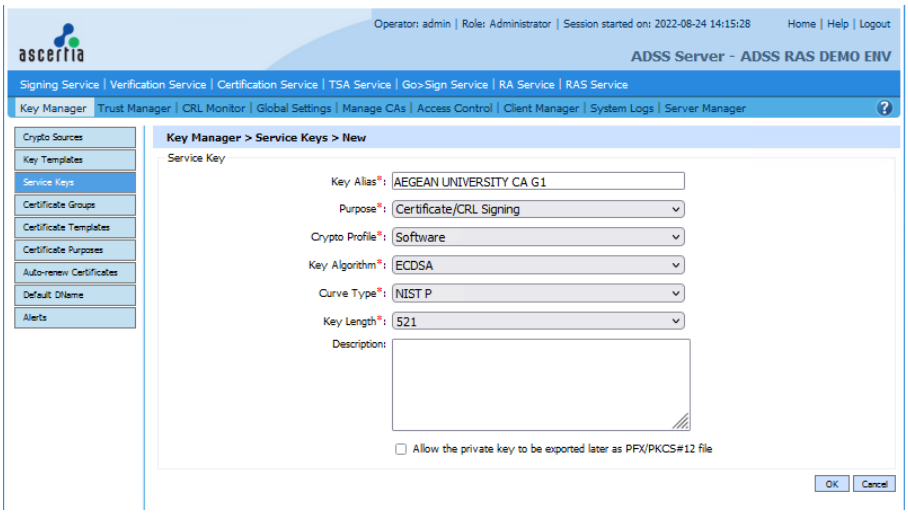


Πατώντας save το προφίλ δημιουργείται με επιτυχία όπως διαπιστώνουμε παρακάτω

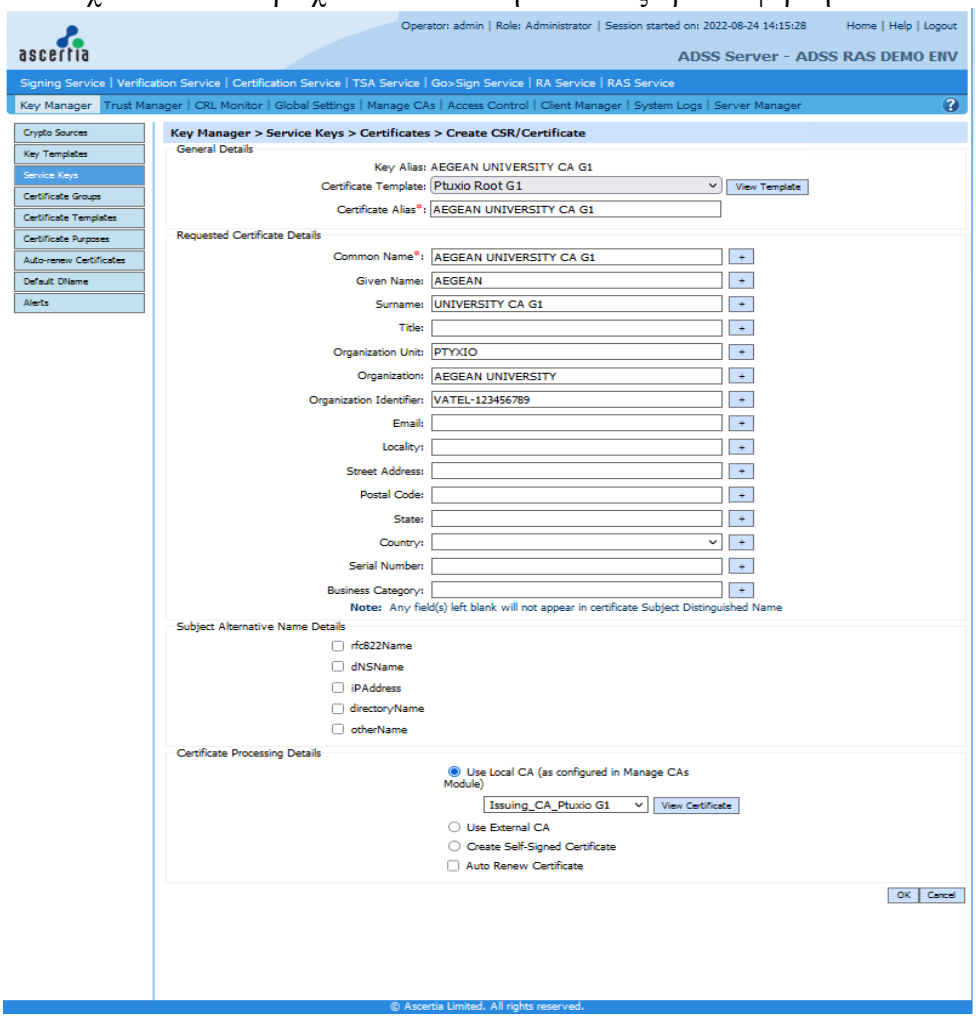


Έχοντας ολοκληρώσει το προφίλ του πιστοποιητικού μεταβαίνουμε στην κατηγορία Service Key για να δημιουργήσουμε τα κλειδία και να συντάξουμε τις πληροφορίες που θα περιέχει το πιστοποιητικού της Ενδιάμεσης Αρχής Πιστοποίησης (Intermediate CA – Certificate Authority) όπου στην συνέχεια θα την υπογράψει η Αρχή Πιστοποίησης (Root CA) που δημιουργήσαμε και με αυτόν τον τρόπο θα δημιουργηθεί η αλυσίδα εμπιστοσύνης ανάμεσα στα δυο πιστοποιητικά.

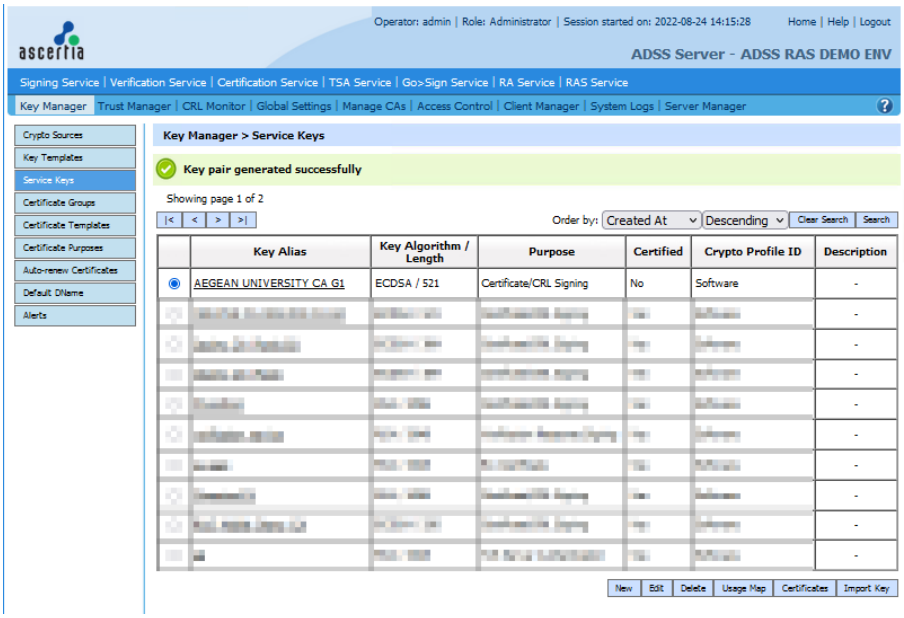
Η Intermediate CA θα δημιουργηθεί με αλγόριθμο ελλειπτικών καμπυλών ECDSA , τύπο καμπύλης NIST P και με μέγεθος κλειδιού 521 Bits.



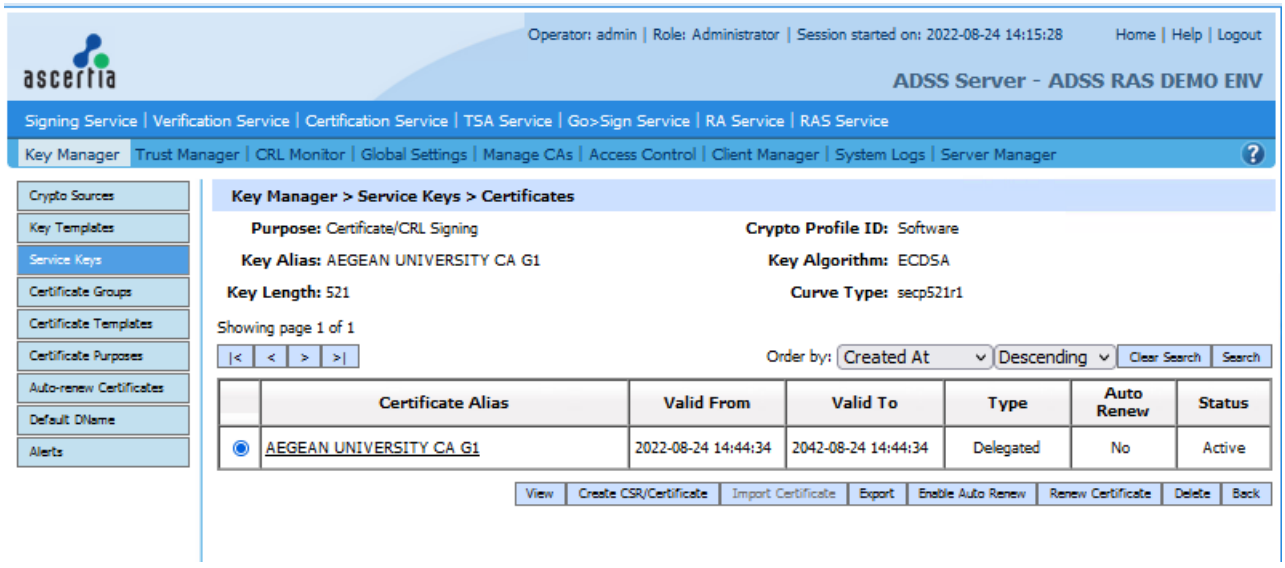
Συντάσσουμε τα στοιχεία που θα περιέχει το πιστοποιητικό όπως προαναφέρθηκε

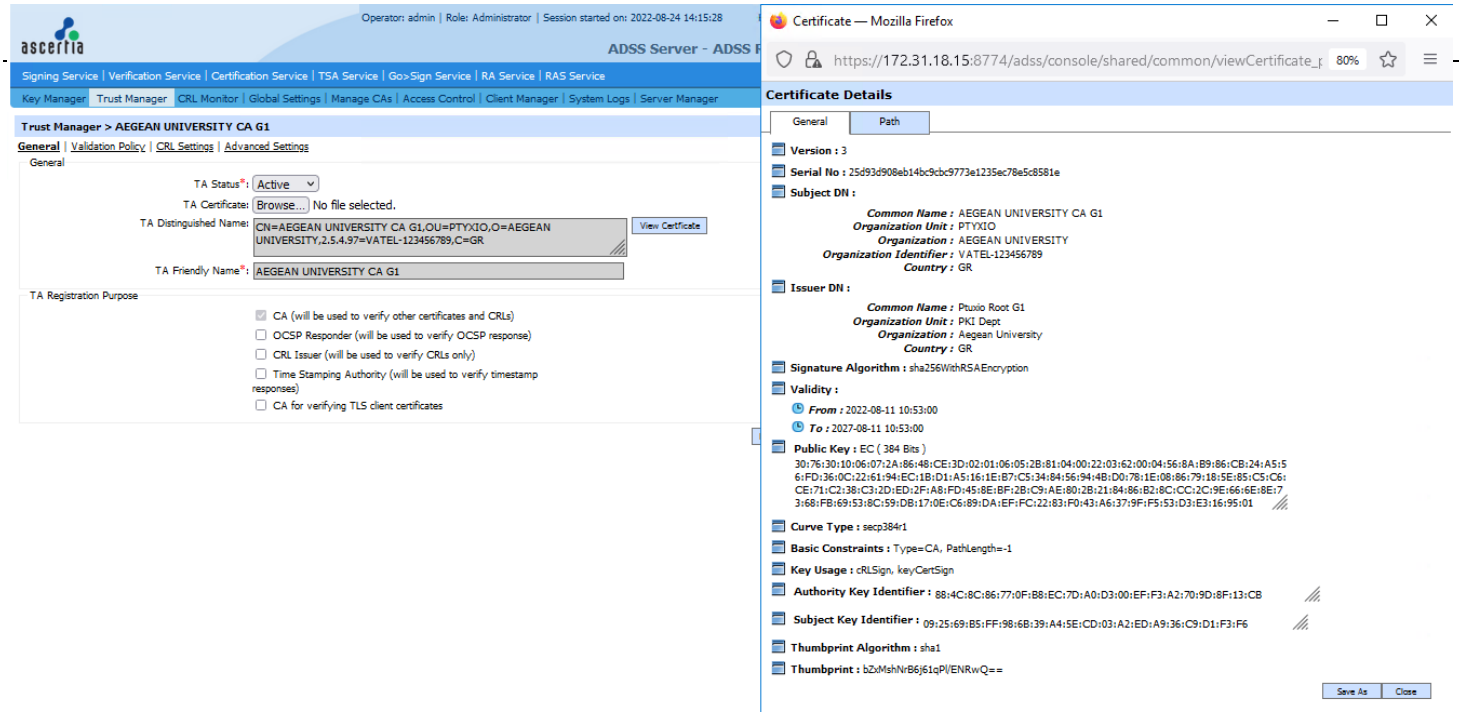


Στην παρακάτω εικόνα βλέπουμε την επιτυχημένη δημιουργία των κλειδιών.

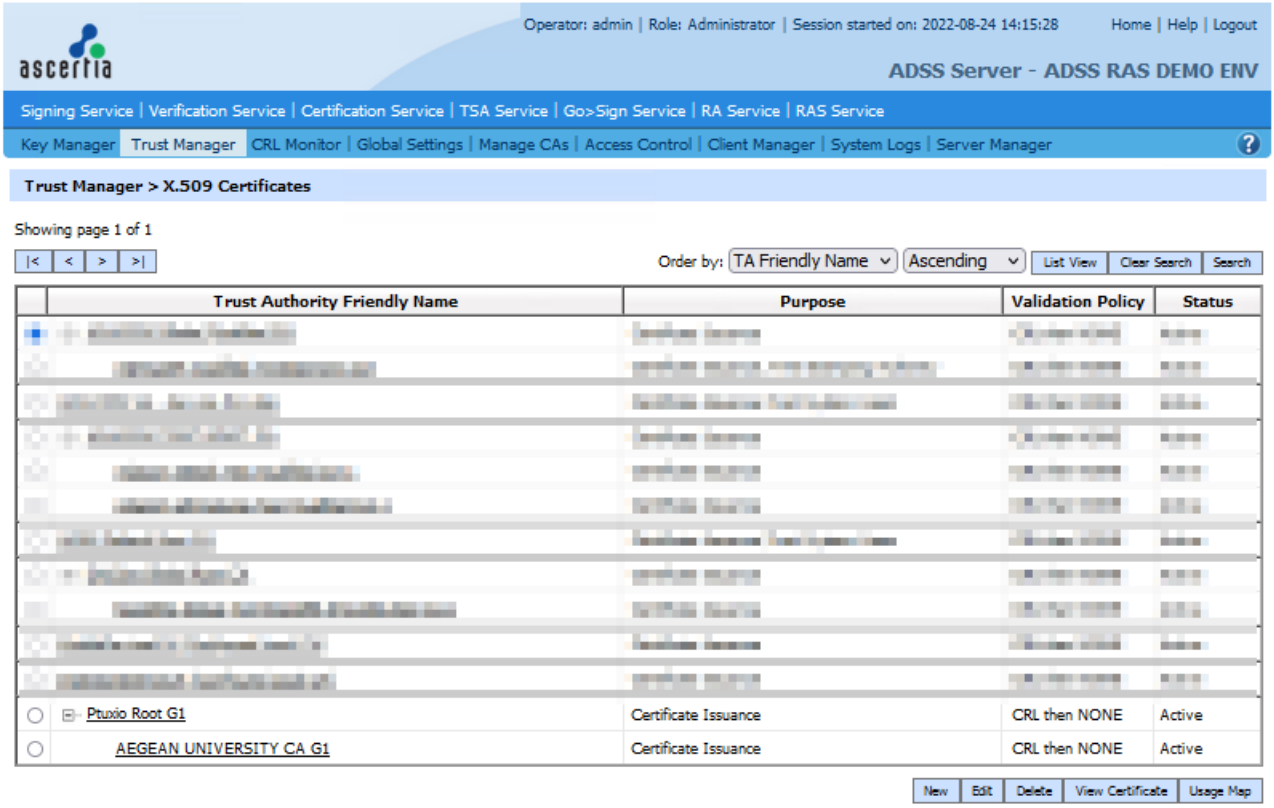


Το πιστοποιητικό δημιουργήθηκε με επιτυχία





Και η αλυσίδα εμπιστοσύνης δημιουργήθηκε με επιτυχία



Αφού ολοκληρώθηκε με επιτυχία η δημιουργία των πιστοποιητικών , στην συνέχεια θα διαμορφωθούν όλες οι υπηρεσίες του PKI server που απαιτούνται ώστε να γίνει η σωστή διασύνδεση του με την εφαρμογή απομακρυσμένης υπογραφής εγγράφων της Ascertia που ονομάζετε Signing Hub.

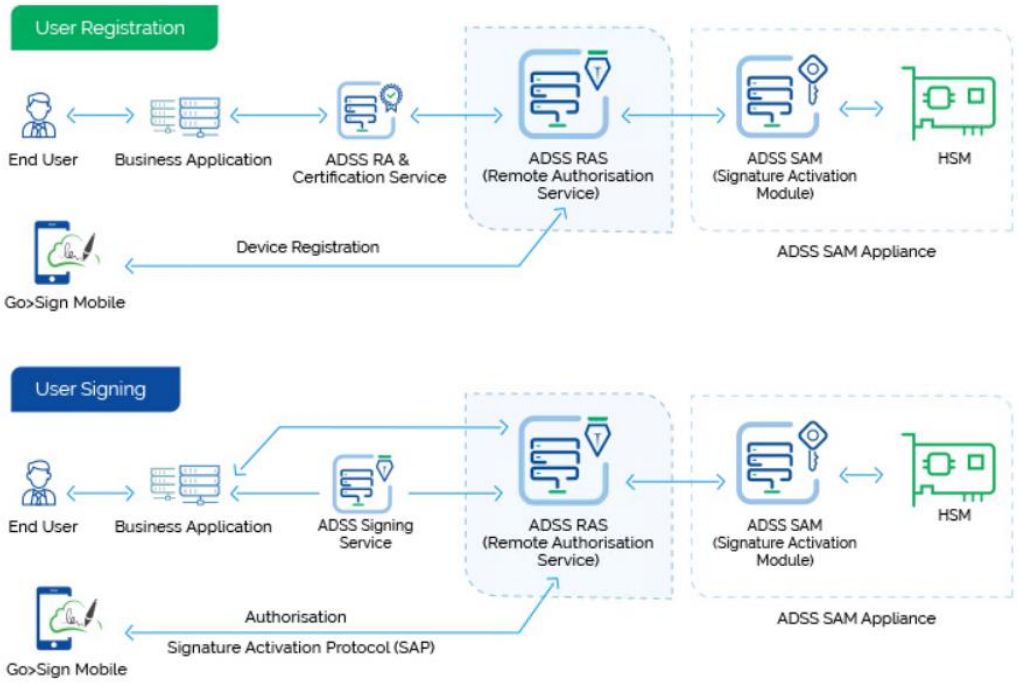
Στην παρακάτω εικόνα φαίνονται όλες οι υπηρεσίες που πρέπει να διαμορφωθούν, διασυνδεθούν για να παραχθεί το τελικό αποτέλεσμα.

Αρχικά ένας τελικός χρήστης εγγράφετε σε ένα Business Application οπού καταχωρεί τα στοιχεία του για να αυθεντικοποιηθεί από την CA και κατ' επέκταση να δημιουργηθεί το πιστοποιητικό του , το όποιο αποθηκεύεται στο HSM.

Ταυτόχρονα με την δημιουργία του λογαριασμού του και την αυθεντικοποίηση του στο Business Application, δημιουργείται και ένας λογαριασμός στο Signing Hub application (εφαρμογή απομακρυσμένης υπογραφής).

Στην συνέχεια ο χρήστης συνδέεται στο Signing Hub ανεβάζει το έγγραφο που επιθυμεί και την ώρα που αιτείτε την εφαρμογή της υπογραφής του σε αυτό , η εφαρμογή ζητάει τα διαπιστευτήρια και τα βιομετρικά στοιχεία (μέσω κινητού τηλεφώνου) του χρήστη .

Αφού δοθούν τα σωστά διαπιστευτήρια , το Signing Hub ζητάει από τον ADSS server το πιστοποιητικό του χρήστη για να υπογράψει το έγγραφο.



Υπηρεσίες διασύνδεσης ADSS

Remote Authorization Signing (RAS)

Η υπηρεσία Remote Authorization Signing (RAS) παρέχει τη δυνατότητα να προστατεύει το SAM από τον εξωτερικό κόσμο και να λειτουργεί ως γέφυρα μεταξύ της Business/Go>Sign Mobile Application και της Υπηρεσίας SAM. Παρέχει την απαιτούμενη διεπαφή API για επιχειρηματικές εφαρμογές για την εγγραφή χρηστών, την αποστολή αιτημάτων υπογραφής κατακερματισμού, τον έλεγχο της κατάστασης των εκκρεμών αιτημάτων υπογραφής και τη λήψη του υπογεγραμμένου κατακερματισμού (δηλαδή υπογραφή PKCS#1). Παρέχει επίσης τις απαιτούμενες διεπαφές API για την εφαρμογή Go>Sign Mobile για να επιτρέπει στους χρήστες να συνδέονται στην εφαρμογή αφού επιλέξουν τους διαφορετικούς ελέγχους ταυτότητας που είναι κωδικός QR, μέσω SMS και EMAIL OTP και χωρίς έλεγχο ταυτότητας. Επιτρέπει στην εφαρμογή Go>Sign Mobile να καταχωρεί κινητή συσκευή με δημόσιο κλειδί εξουσιοδότησης, να στέλνει ειδοποιήσεις push, να λαμβάνει το αίτημα εξουσιοδότησης και να στέλνει το υπογεγραμμένο αίτημα εξουσιοδότησης (δηλαδή Δεδομένα ενεργοποίησης υπογραφής - SAD).

ADSS RA

Η Υπηρεσία ADSS RA χειρίζεται όλα τα αιτήματα διαχείρισης πιστοποιητικών για λογαριασμό τελικών οντοτήτων που μπορεί να περιλαμβάνουν ανθρώπινους χρήστες, διακομιστές και συσκευές δικτύου. Αυτά τα αιτήματα διαχείρισης πιστοποιητικών μπορεί να αφορούν την έκδοση ή την ανάκληση πιστοποιητικού. Η Υπηρεσία ADSS RA μπορεί να λάβει αίτημα διαχείρισης πιστοποιητικού από συσκευές που χρησιμοποιούν το πρωτόκολλο SCEP, επιχειρηματικές εφαρμογές μέσω μιας διεπαφής υπηρεσίας web ή από το ADSS Go>Sign Desktop όπου απαιτείται αλληλεπίδραση με τον χρήστη. Τα αιτήματα που διεκπεραιώνονται με επιτυχία από τις Υπηρεσίες ADSS RA διαβιβάζονται στην αρμόδια Αρχή Πιστοποιητικών (CA) για δράση.

ADSS Go>Sign

Η υπηρεσία ADSS Go>Sign χρησιμοποιείται για τη διαχείριση και τον αυστηρό έλεγχο της χρήσης του Go>Sign Client σε ένα περιβάλλον εφαρμογής web. Οι εφαρμογές Ιστού καλούν την υπηρεσία Go>Sign για να ξεφορτώσουν την πολυπλοκότητα του καθορισμού των πολλών επιλογών που προσφέρει το Go>Sign Client για προβολή, κατακερματισμό, υπογραφή και χειρισμό πεδίων φορμών, έλεγχο πεδίων υπογραφής, εμφανίσεις υπογραφών, ρύθμιση φίλτρων πιστοποιητικών, προγραμμάτων οδήγησης και άλλες λεπτομέρειες .

ADSS (ADSS Certification Service)

Η Υπηρεσία Πιστοποίησης ADSS (ADSS Certification Service) παρέχει μια ΑΠ υπηρεσιών ιστού XML/SOAP που επιτρέπει στις επιχειρηματικές εφαρμογές να ζητούν δημιουργία και/ή πιστοποίηση κλειδιών καθώς και αιτήματα πιστοποίησης βάσει χειριστή από τη λειτουργική μονάδα Key Manager. Τα αιτήματα πιστοποίησης μπορούν επίσης να γίνουν χρησιμοποιώντας μια διεπαφή CMC μέσω HTTP/S. Μπορούν να οριστούν και να διαχειρίζονται πολλαπλές CA

ADSS (ADSS Verification Service)

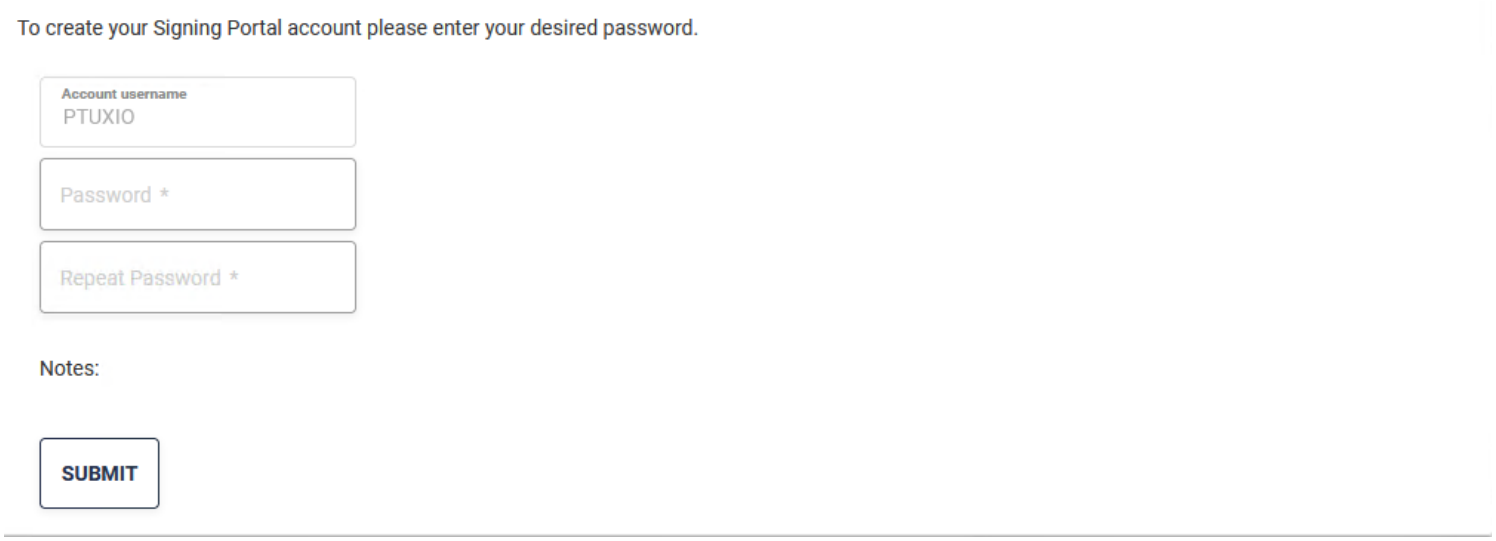
Η Υπηρεσία Επαλήθευσης ADSS (ADSS Verification Service) παρέχει εκτεταμένες λειτουργίες για την επαλήθευση υπογεγραμμένων αντικειμένων δεδομένων και την επικύρωση των συσχετισμένων αλυσίδων πιστοποιητικών. Όλες οι κοινές μορφές υπογραφής μπορούν να επαληθευτούν, συμπεριλαμβανομένων των υπογραφών S/MIME, DSig, PDF, CMS, XAdES, CAdES, ETSI PAdES, PKCS#7 και XML. Η διεπαφή με την υπηρεσία επαλήθευσης ADSS είναι συμβατή με το OASIS DSS και το DSS-X και είναι επίσης διαθέσιμη μια επιλογή HTTP/S υψηλής ταχύτητας. Τα πιστοποιητικά μπορούν επίσης να σταλούν σε αυτήν την υπηρεσία για επικύρωση. Υποστηρίζονται απλές και σύνθετες μέθοδοι δημιουργίας διαδρομής και επικύρωσης διαδρομής.

ADSS (ADSS Signing Service)

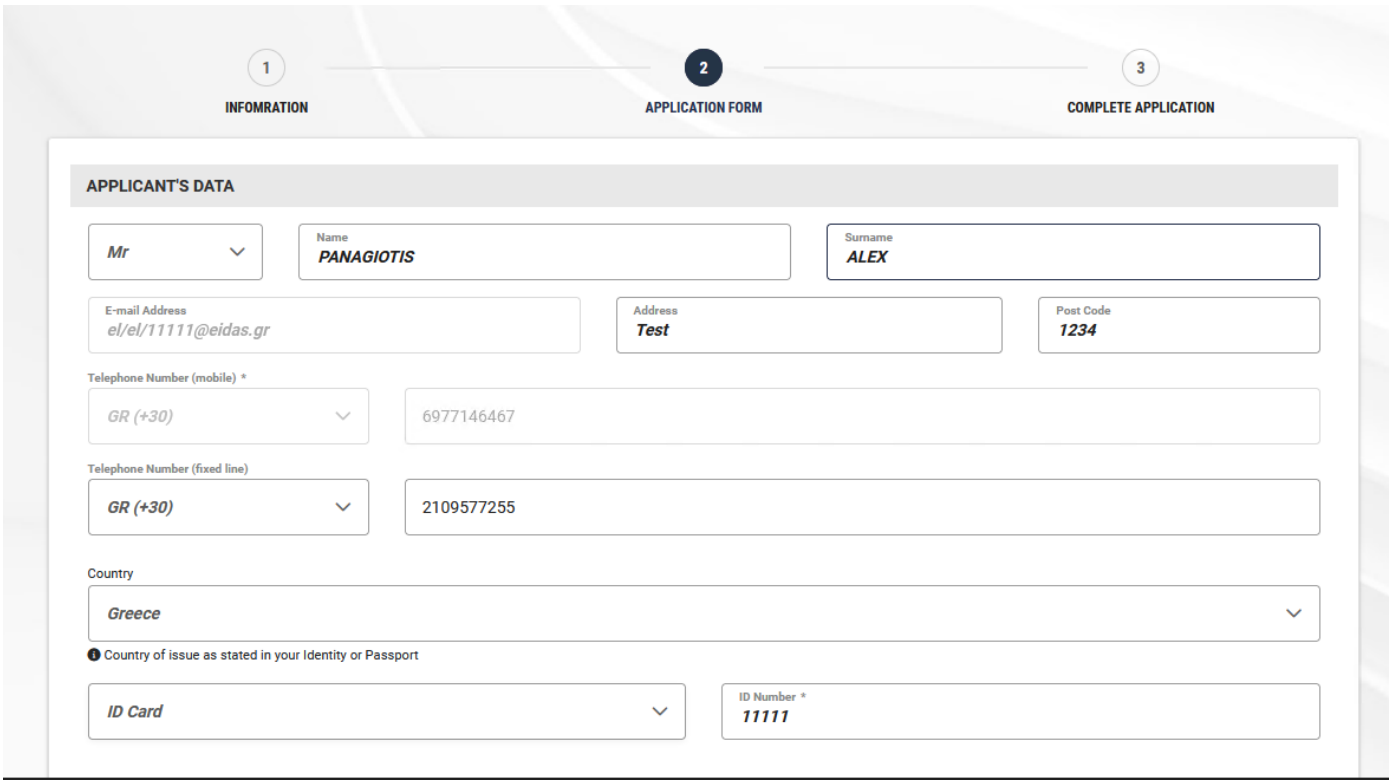
Η υπηρεσία υπογραφής ADSS (ADSS Signing Service) παρέχει τη δυνατότητα ψηφιακής υπογραφής εγγράφων και δεδομένων διαφόρων μορφών χρησιμοποιώντας υπογραφές S/MIME, DSig, PDF, CMS, XAdES, CAdES, ETSI PAdES, PKCS#7 και XML. Η διεπαφή με την υπηρεσία υπογραφής ADSS είναι συμβατή με το OASIS DSS και είναι επίσης διαθέσιμη μια επιλογή HTTP/S υψηλής ταχύτητας. Στα έγγραφα PDF μπορούν επίσης να προστεθούν κενά πεδία υπογραφής, να κατακερματιστούν και να περάσουν υπογραφές για τελική συναρμολόγηση.

Αναλυτικότερα η διαδικασία είναι η εξής :

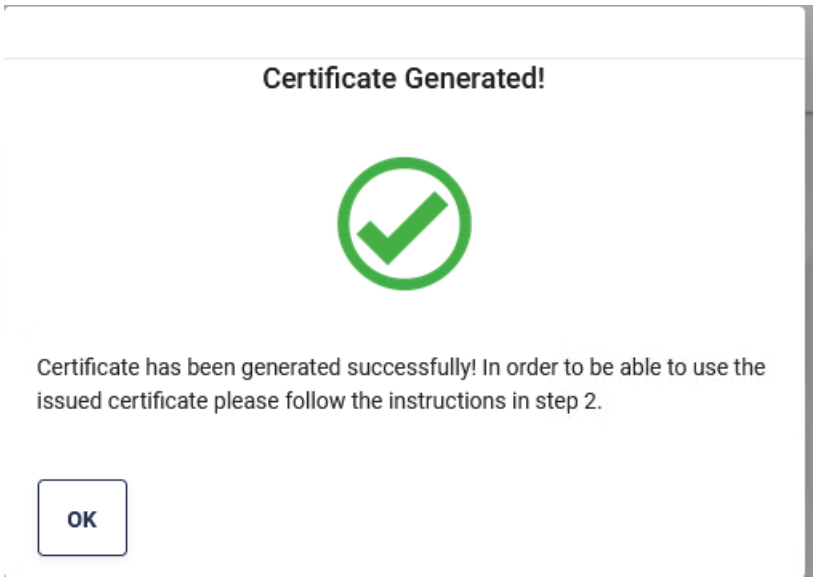
Κάνουμε την εγγραφή μας στο Business Application και καταχωρούμε τα στοιχεία μας για να αυθεντικοποιηθούμε από την CA.

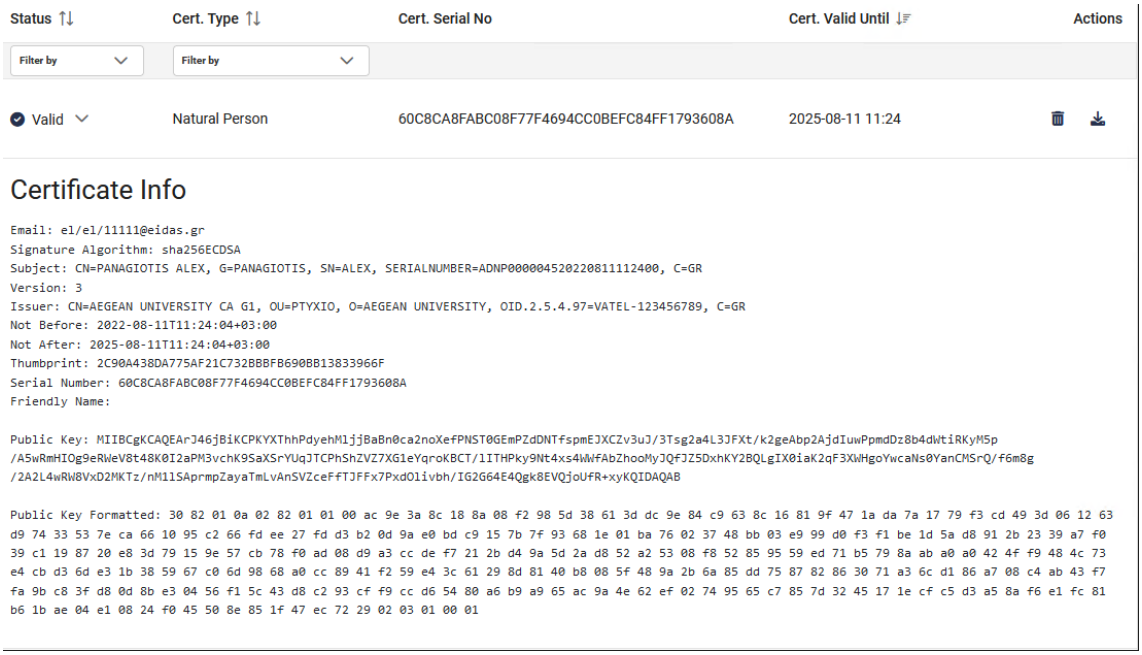


Καταχώριση στοιχείων πιστοποιητικού.

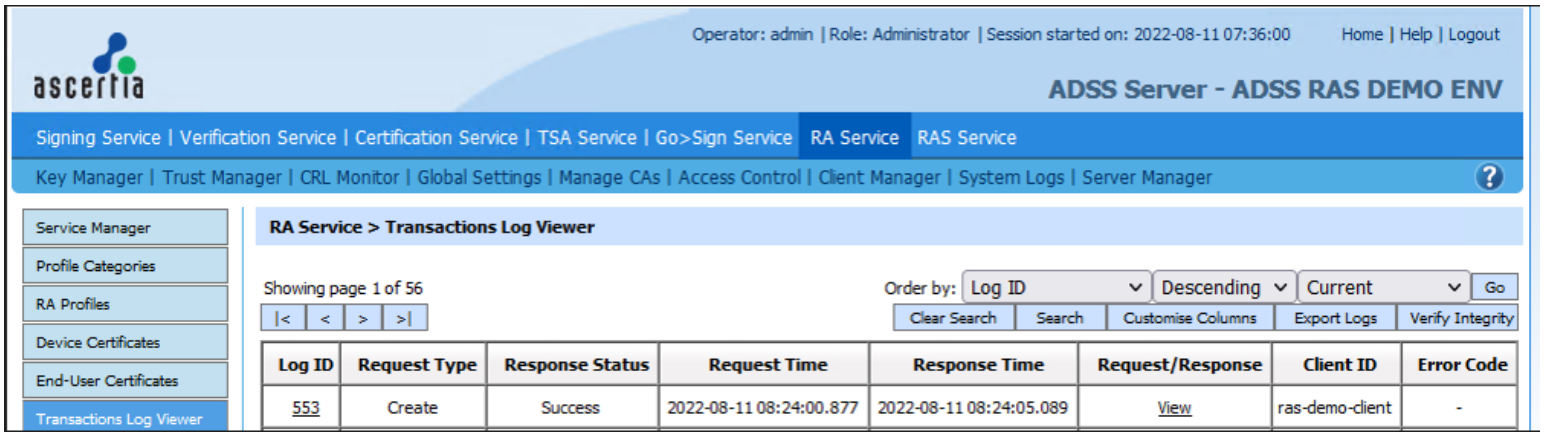


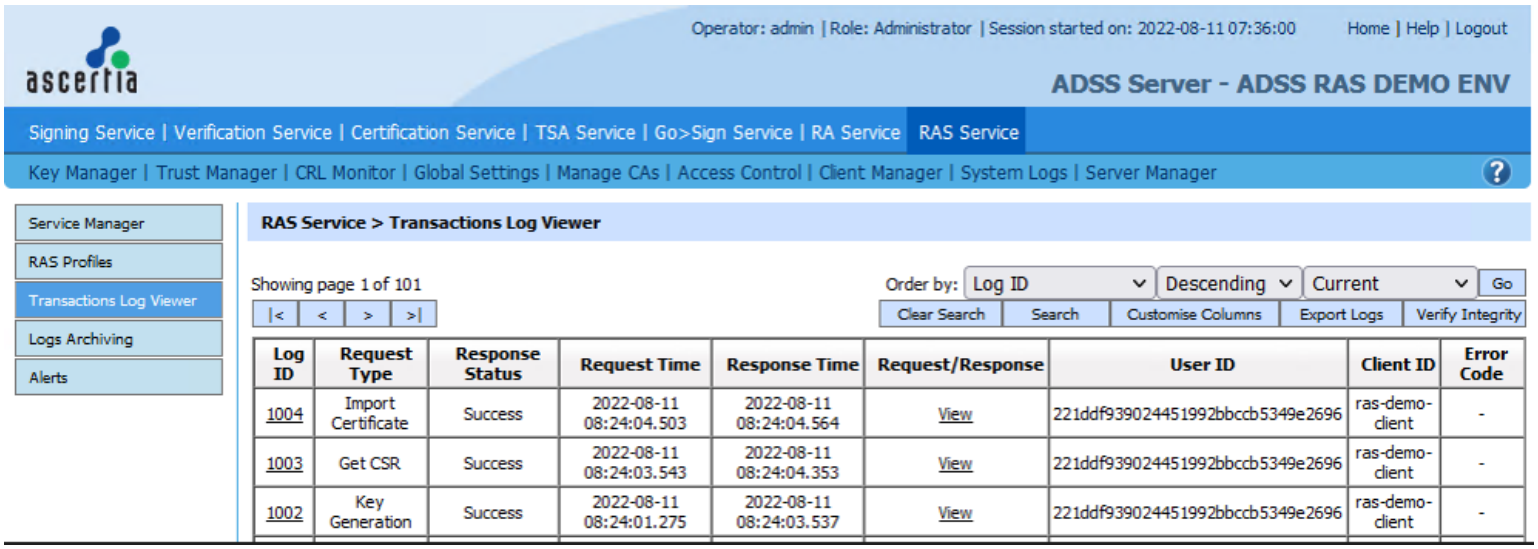
Επιτυχής δημιουργία του πιστοποιητικού

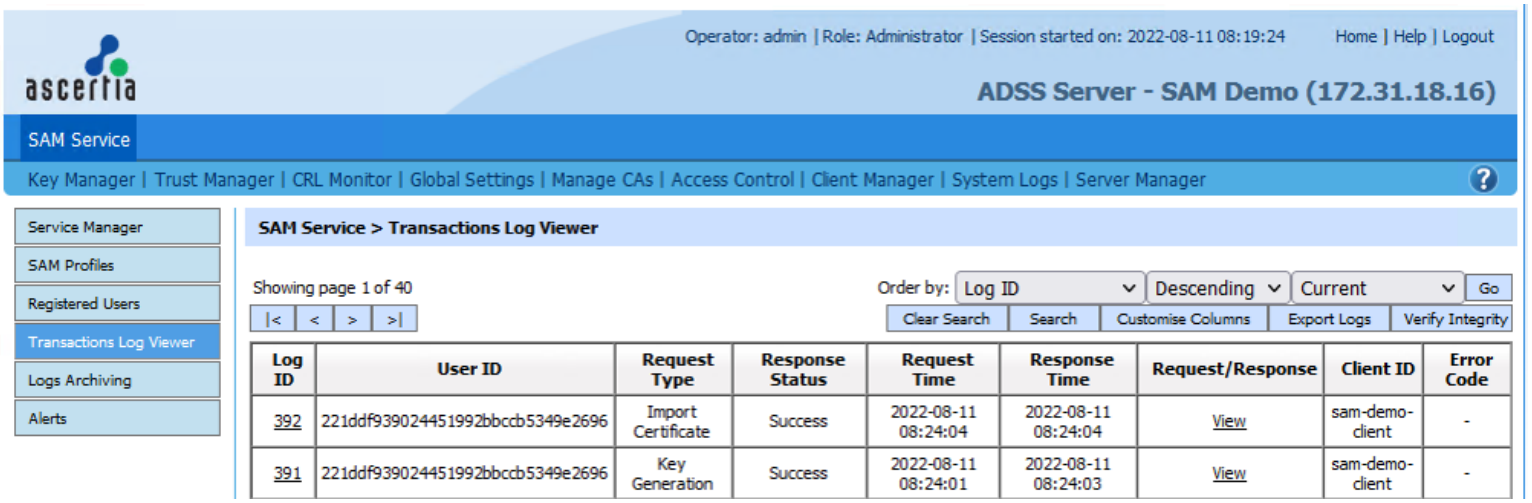




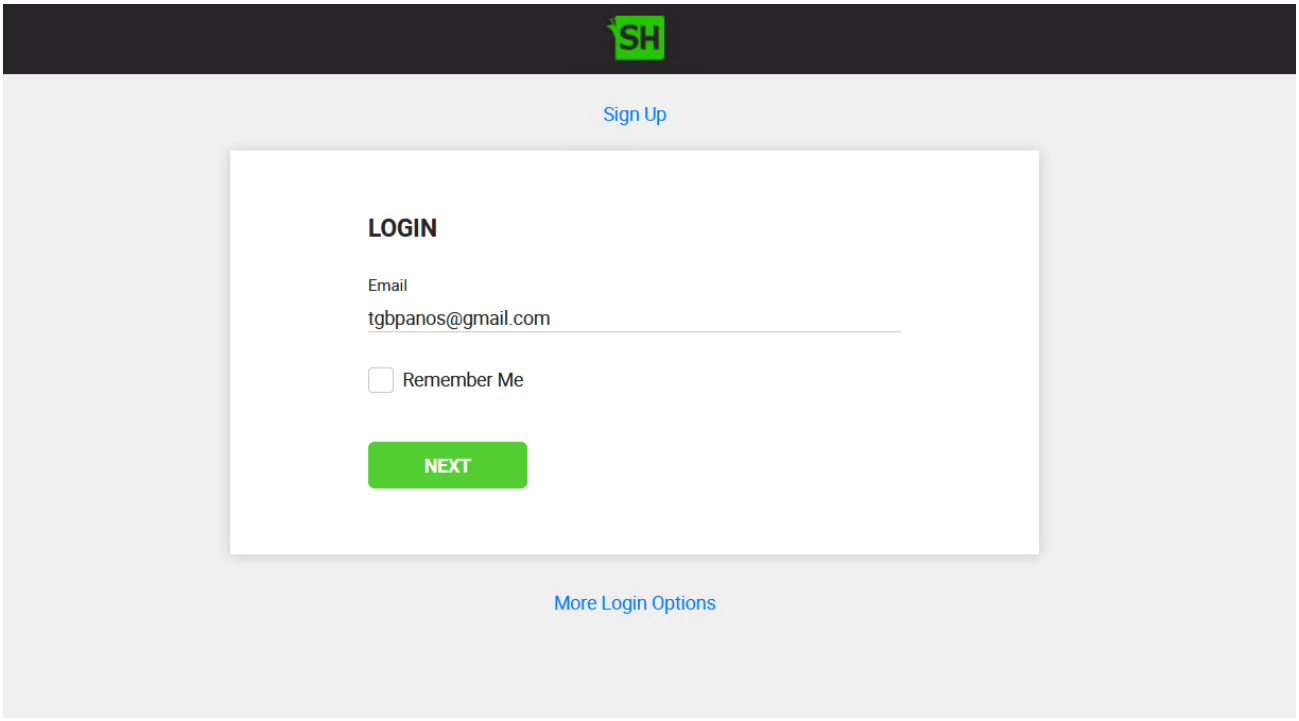
Ταυτόχρονα βλέπουμε και την επιτυχημένη δημιουργία, καταχώριση του πιστοποιητικού στον server.



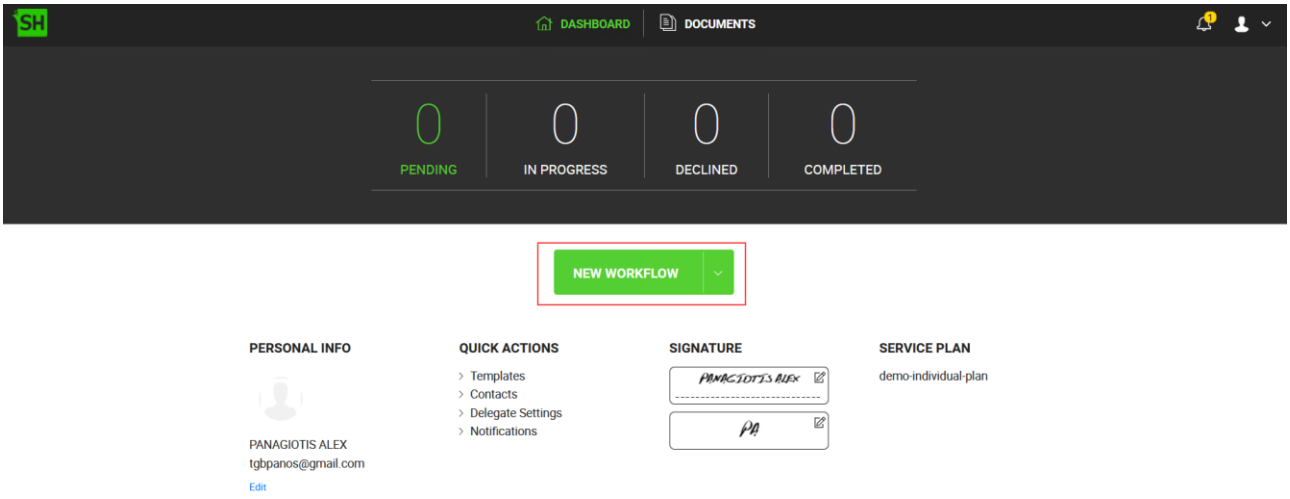




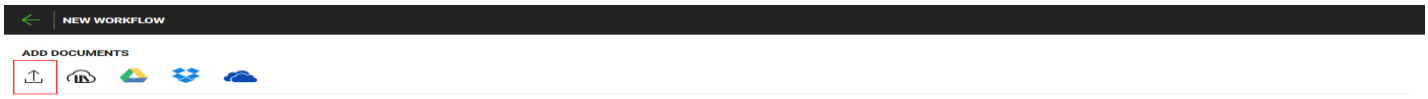
Στην συνέχεια κάνουμε είσοδο στην εφαρμογή απομακρυσμένης υπογραφής Signing Hub application



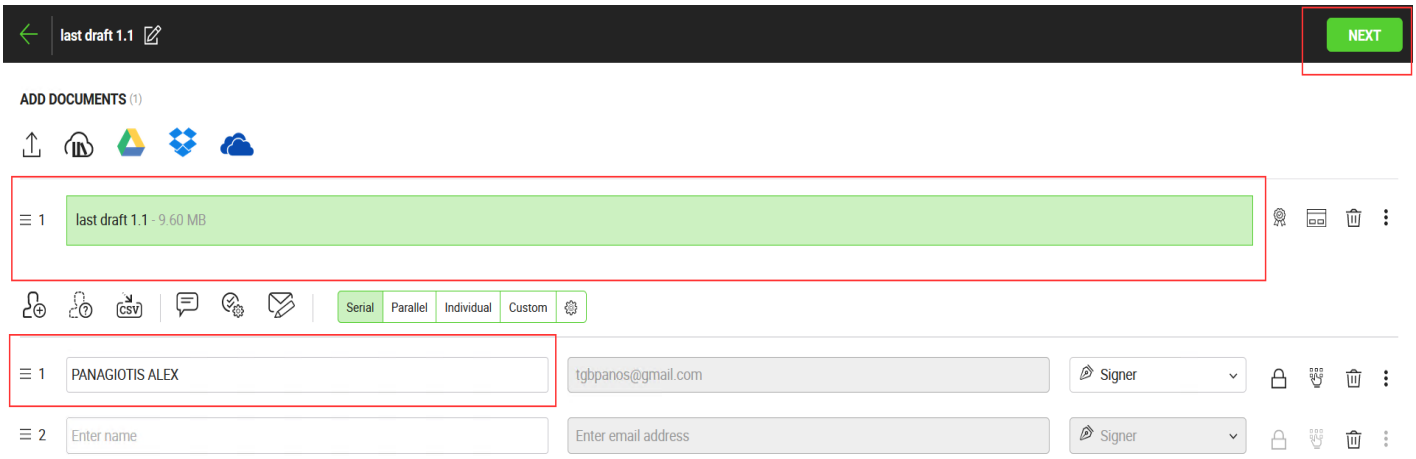
Από την κεντρική κονσόλα της εφαρμογής επιλέγουμε την ροή που θέλουμε να έχει το έγγραφο μας.



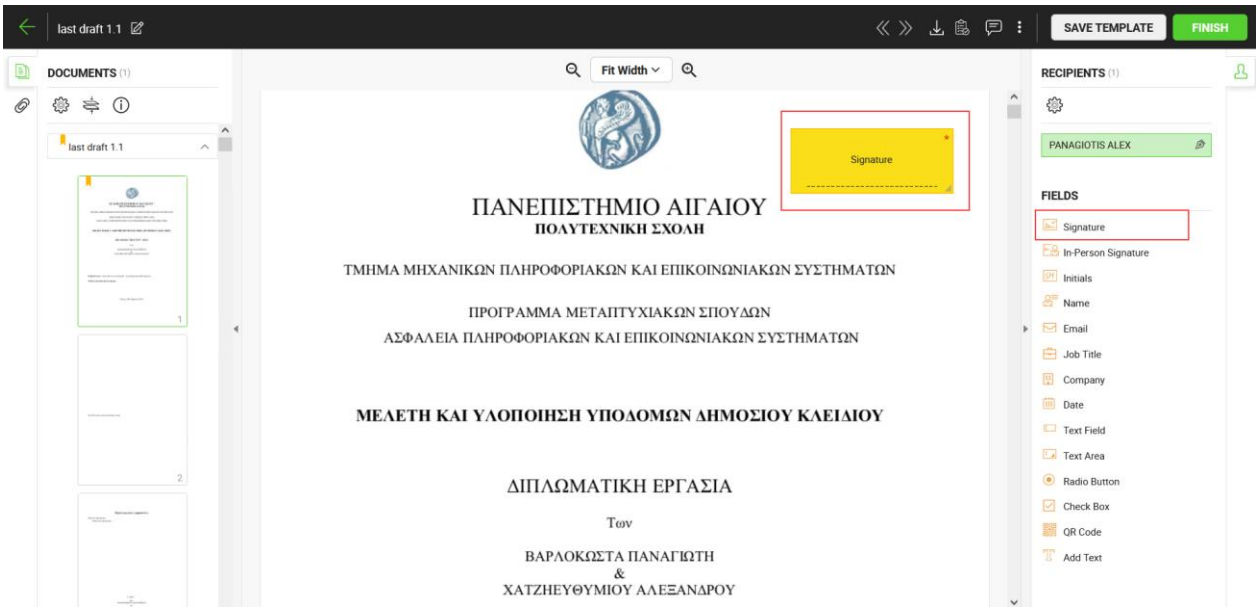
Αφού γίνει η επιλογή στο επόμενο βήμα διαλέγουμε και ανεβάζουμε το έγγραφο που επιθυμούμε.



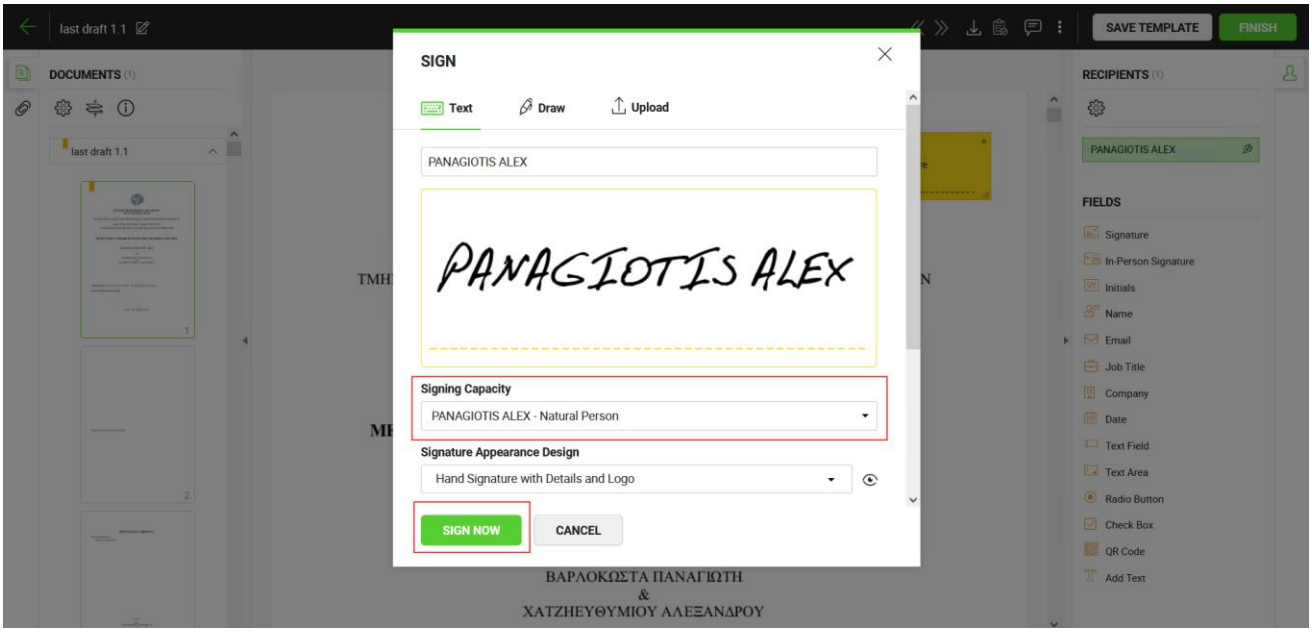
Ταυτόχρονα επιλέγουμε και τον χρήστη που θέλουμε θα υπογράψει το έγγραφο , όπου στην προκειμένη περίπτωση είναι ο δικός μας



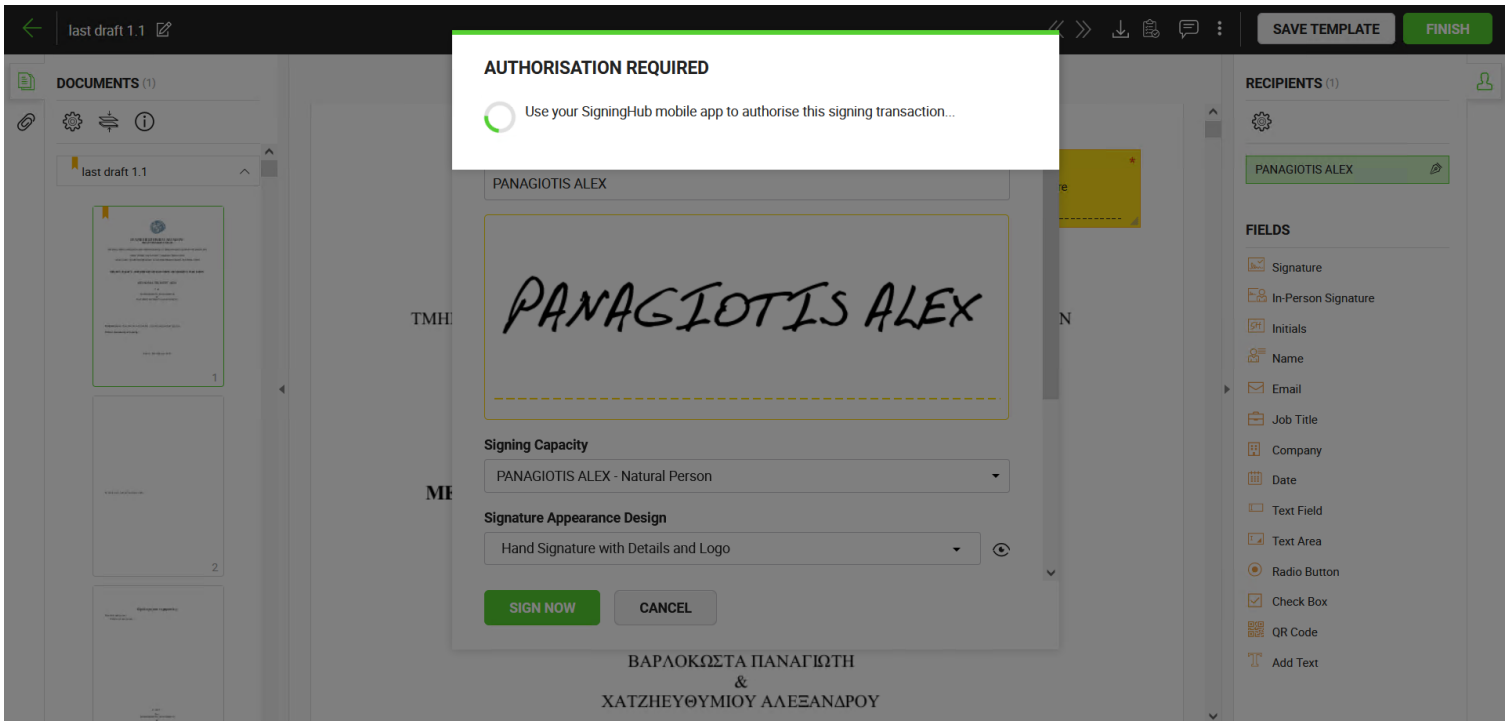
Το επόμενο βήμα είναι να οριστεί το επιθυμητό σημείο υπογραφής πάνω στο έγγραφο.

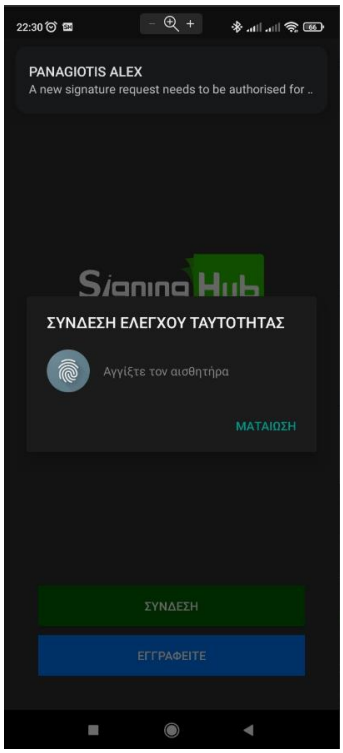


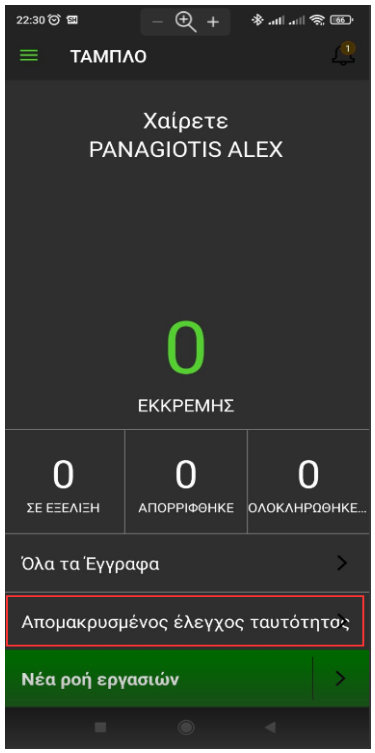
Κάνουμε κλικ πάνω στο πεδίο που ορίσαμε προηγουμένως και επιλέγουμε το πιστοποιητικό μας και το προσχέδιο της υπογραφής και πατάμε το Sign Now

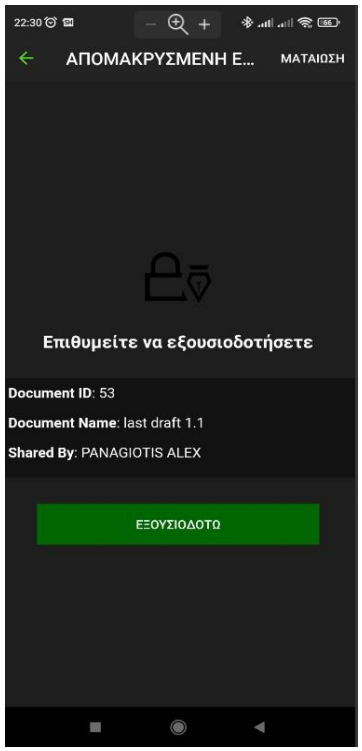


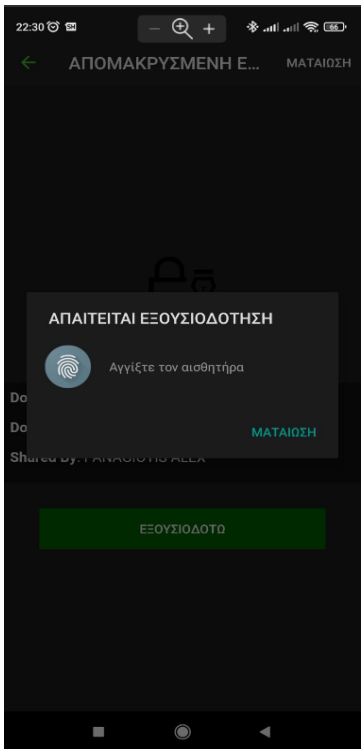
Πατώντας το Sign Now η εφαρμογή περιμένει την βιομετρική αυθεντικοποίηση μας από το κινητό τηλέφωνο.



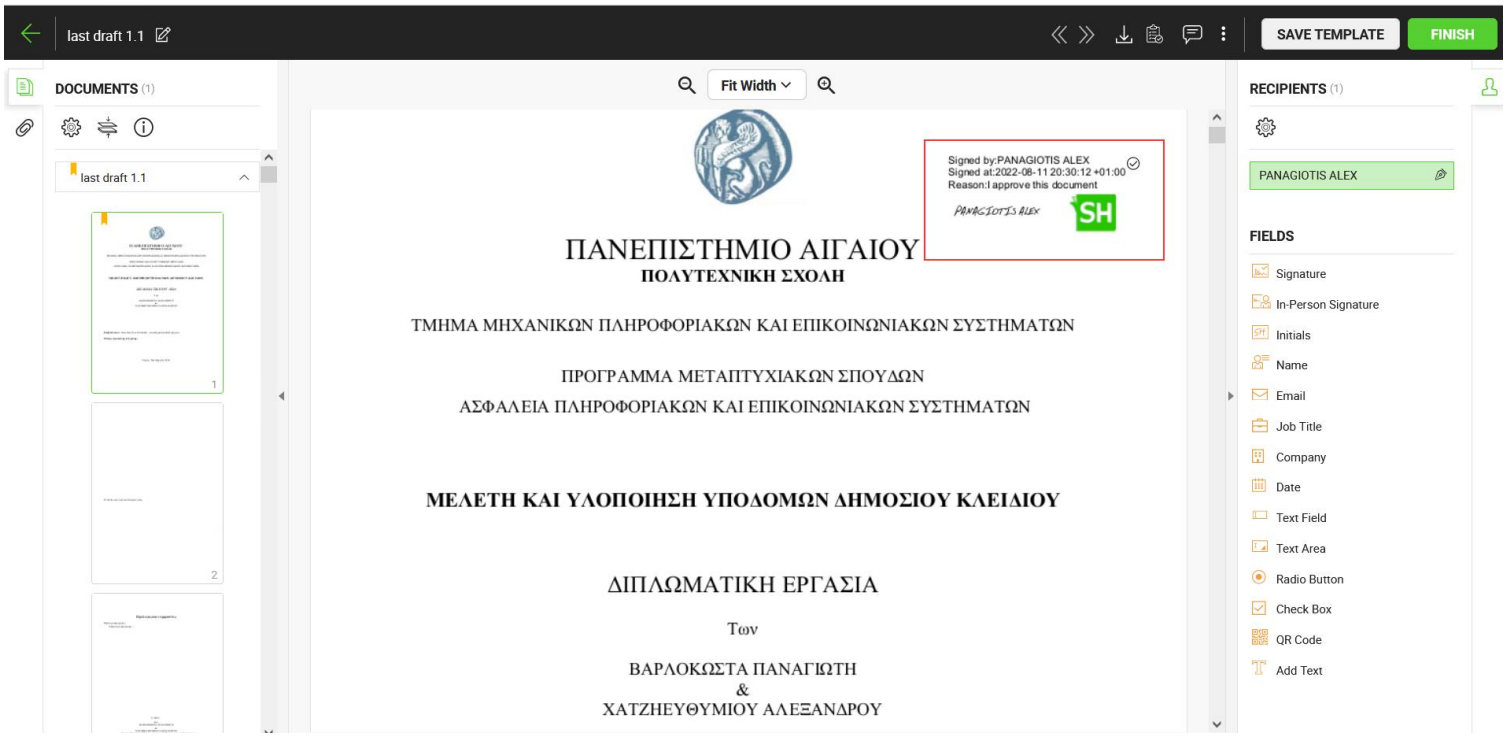




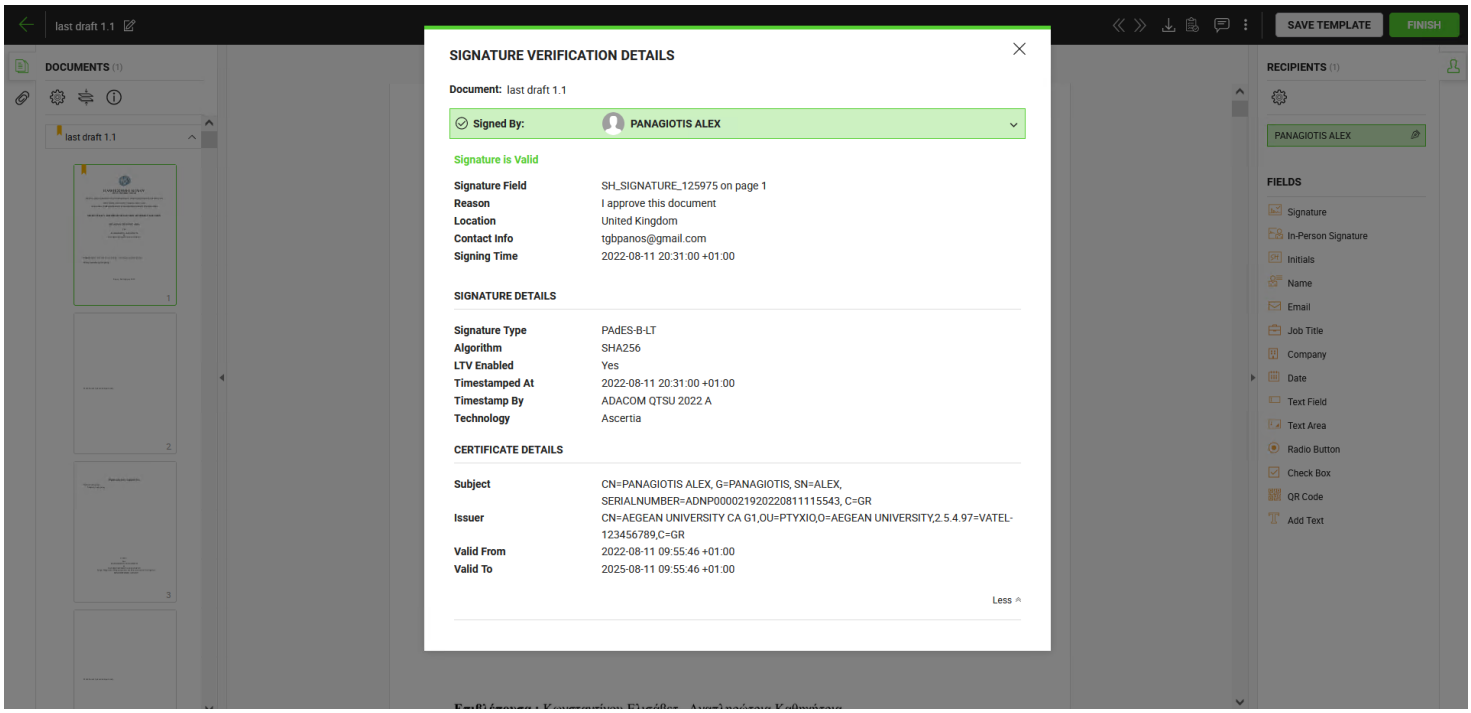




Αφού γίνει η βιομετρική αυθεντικοποίηση μας από το κινητό τηλέφωνο , το έγγραφο αυτόματα υπογράφεται με επιτυχία.



Τέλος στην παρακάτω εικόνα φαίνονται οι πληροφορίες της υπογραφής και του πιστοποιητικού.



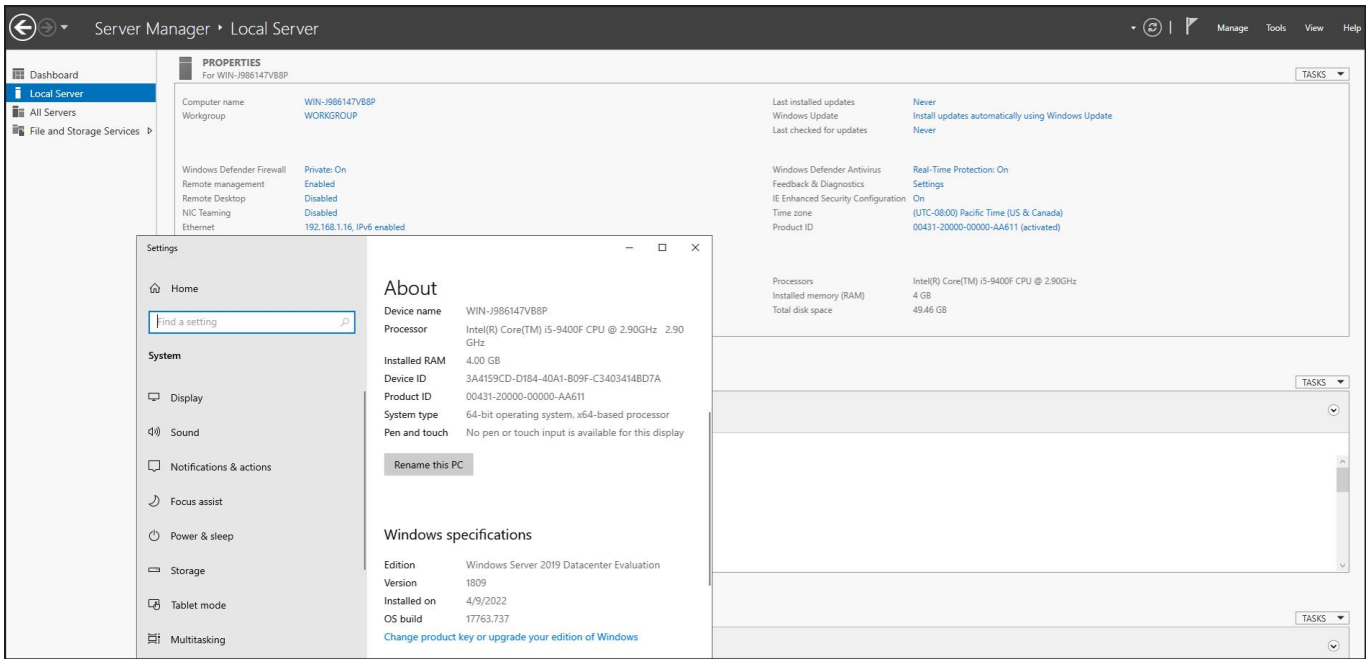
7.2 Σενάριο Εργασίας Β

Σε αυτό το σενάριο θα γίνει η δημιουργία μίας δεύτερης Ενδιάμεσης Αρχή Πιστοποίησης (Intermediate CA) στην τεχνική πλατφόρμα Microsoft PKI κάτω από την ήδη υπάρχουσα Αρχής Πιστοποίησης (Root CA) του Ascertia ADSS server , που αποτελεί και τον συνθετικό κρίκο ανάμεσα στις υποδομές δημοσίου κλειδιού.

Κατ' επέκταση το ιδιωτικό κλειδί της Intermediate CA θα παραχθεί στην υποδομή της Microsoft και θα υπογραφεί στην υποδομή Ascertia.

Επίσης θα παραχθεί ένα προφίλ ψηφιακού πιστοποιητικού που θα δίνει στον χρήστη την δυνατότητα να αποστέλλει την ψηφιακή του αλληλογραφία υπογεγραμμένη.

Το εργαστήριο θα υλοποιηθεί σε περιβάλλον Windows Server 2019 το οποίο είναι ένα λειτουργικό σύστημα που εμπιστεύονται παρά πολλοί οργανισμοί για την σταθερότητα και την υποστήριξη που διαθέτει. Μετά από την επιτυχημένη εγκατάσταση του ORACLE VM VirtualBox, θα δημιουργήσουμε μια εικονική μηχανή με 4GB μνήμη και θα ορίσουμε τις επιθυμητές παραμέτρους λειτουργίας.



Δυνατότητες Λειτουργικού Συστήματος

Windows Domain

Ο τομέας των Windows (Windows Domain) είναι μια μορφή δικτύου υπολογιστών στον οποίο όλοι οι λογαριασμοί χρηστών, τα τερματικά, οι εξυπηρετητές κ.α. είναι εγγεγραμμένοι σε μια κεντρική βάση δεδομένων, γνωστή και ως ελεγκτής τομέα (domain controller). Κάθε χρήστης μπορεί να χρησιμοποιήσει το λογαριασμό για να συνδεθεί σε επιτρεπόμενους πόρους του συστήματος.

Active Directory

Είναι μια ιδιόκτητη υπηρεσία καταλόγου που αναπτύχθηκε από τη Microsoft

Το Active Directory (AD) είναι ένας κατάλογος της Microsoft που έχει ιεραρχική δομή, αποθηκεύει πληροφορίες για αντικείμενα στο δίκτυο παρέχει τις μεθόδους για την αποθήκευση δεδομένων καταλόγου και τη διάθεση αυτών των δεδομένων σε χρήστες και διαχειριστές δικτύου. Επίσης επιτρέπει σε άλλους εξουσιοδοτημένους χρήστες στο ίδιο δίκτυο να έχουν πρόσβαση σε αυτές τις πληροφορίες.

Η υπηρεσία καταλόγου Active Directory αποθηκεύει πληροφορίες σχετικά με αντικείμενα στο δίκτυο και διευκολύνει την εύρεση και χρήση αυτών των πληροφοριών από τους διαχειριστές και τους χρήστες. Επιπλέον χρησιμοποιεί ένα δομημένο χώρο αποθήκευσης δεδομένων ως βάση για μια λογική, ιεραρχική οργάνωση των πληροφοριών καταλόγου.

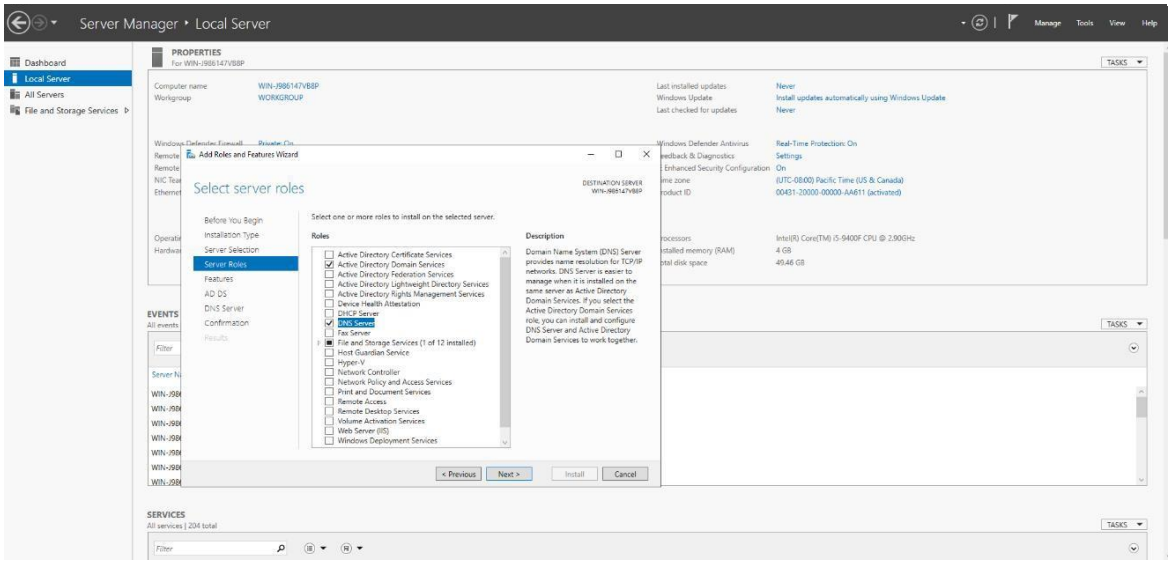
Αυτός ο χώρος αποθήκευσης δεδομένων, γνωστός και ως κατάλογος, περιέχει πληροφορίες σχετικά με αντικείμενα της υπηρεσίας καταλόγου Active Directory. Αυτά τα αντικείμενα περιλαμβάνουν συνήθως κοινόχρηστους πόρους, όπως διακομιστές, τόμους, εκτυπωτές , λογαριασμούς χρηστών και υπολογιστές δικτύου.

Η ασφάλεια είναι ενσωματωμένη στο Active Directory μέσω ελέγχου ταυτότητας σύνδεσης και ελέγχου πρόσβασης σε αντικείμενα στον κατάλογο. Με μία μόνο σύνδεση δικτύου, οι διαχειριστές μπορούν να διαχειρίζονται δεδομένα καταλόγου και οργάνωση σε όλο το δίκτυό τους και οι εξουσιοδοτημένοι χρήστες του δικτύου μπορούν να έχουν πρόσβαση σε πόρους οπουδήποτε στο δίκτυο.

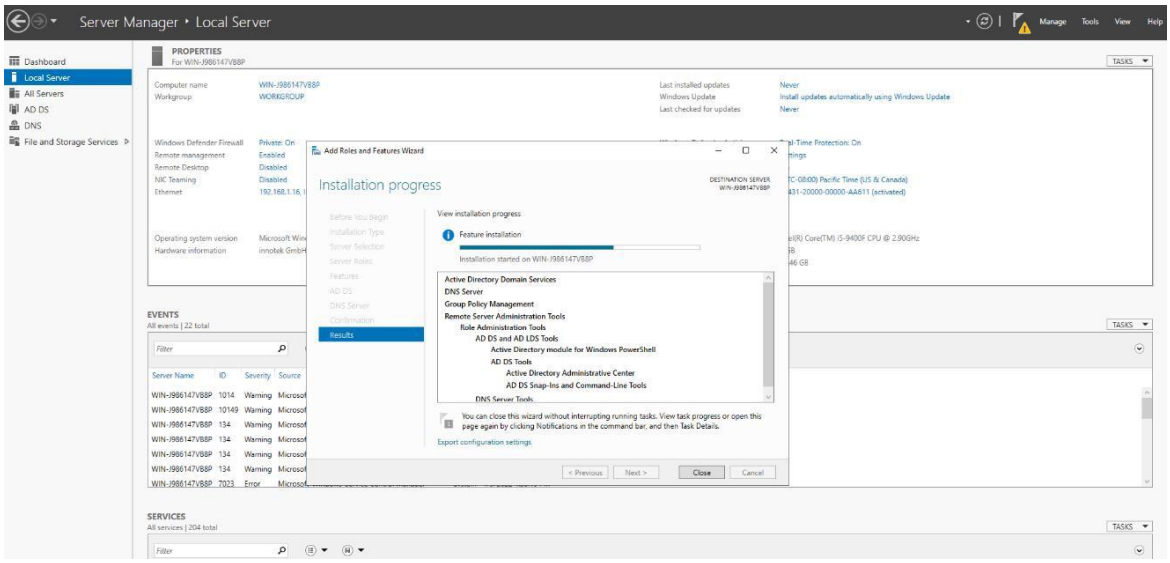
Έναρξη εγκατάστασης

Βήμα 1 – Συνδεόμαστε στο VM win-ADDC και εγκαθιστούμε το ρόλο Active Directory Domain Services (ADDS)

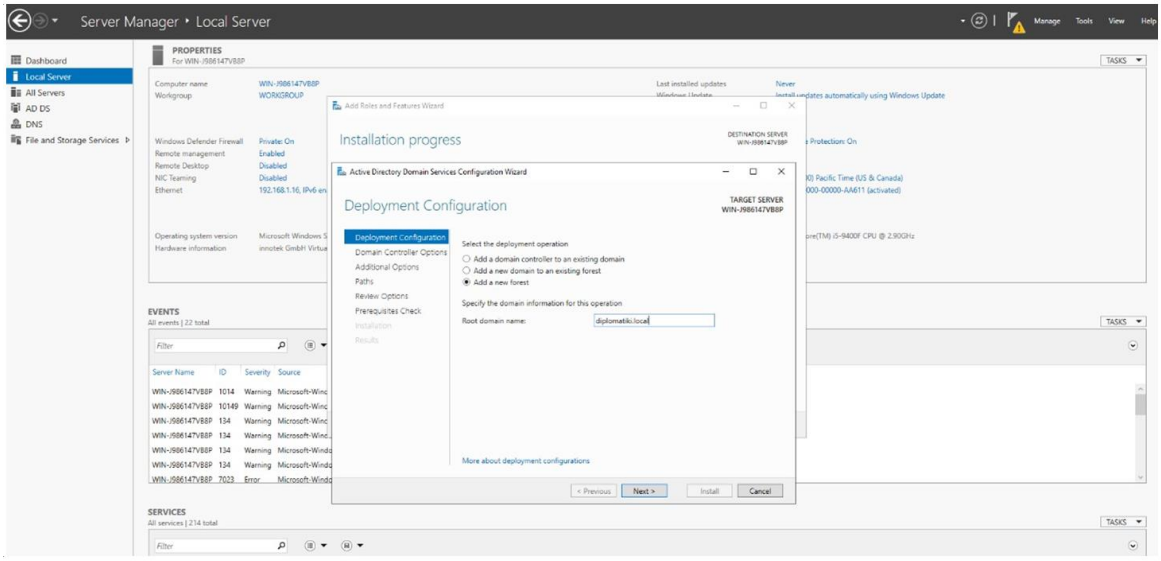
Βήμα 2 – Στην παρακάτω εικόνα επιλέγουμε την επιλογή DNS Server.



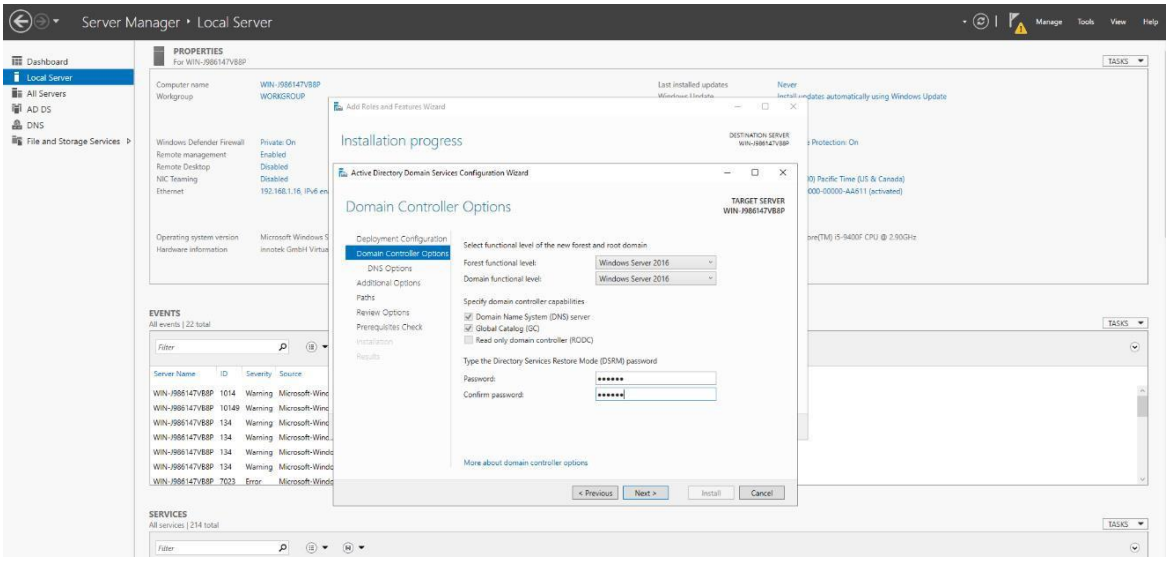
Βήμα 3 – Μόλις ολοκληρωθεί η εγκατάσταση, επιλέγουμε την επιλογή "Promote this server to a domain controller"



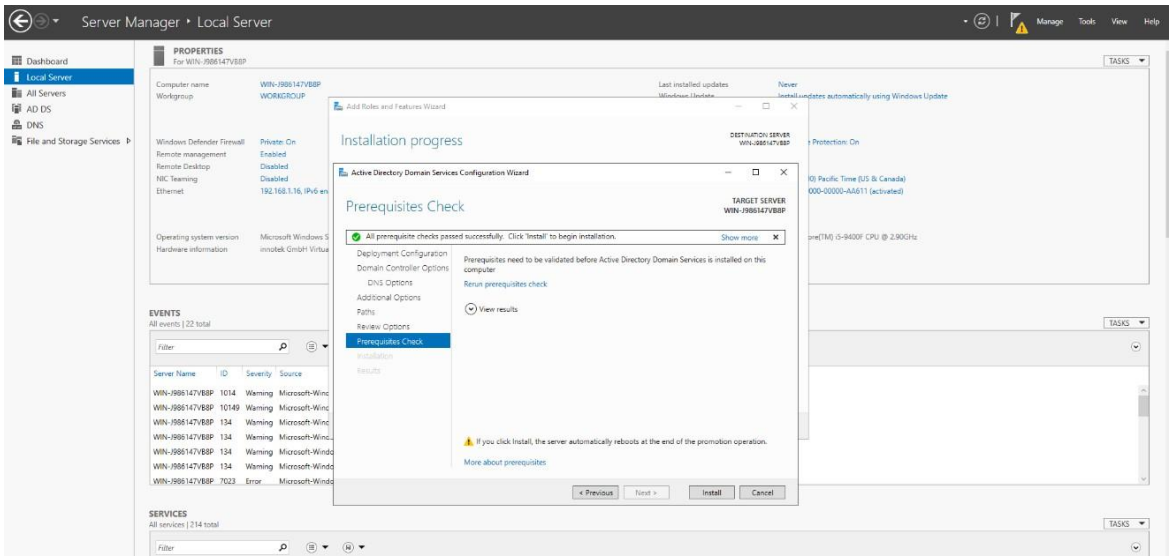
Βήμα 4 – Επιλέγουμε την επιλογή Add a new forest διότι δημιουργούμε για πρώτη φορά το συγκεκριμένο domain συγκεκριμένο domain



Βήμα 5 – Δηλώνουμε το κωδικό DSRM και συνεχίζουμε την εγκατάσταση



Βήμα 6 – Η διαδικασία εγκατάστασης έχει ολοκληρωθεί

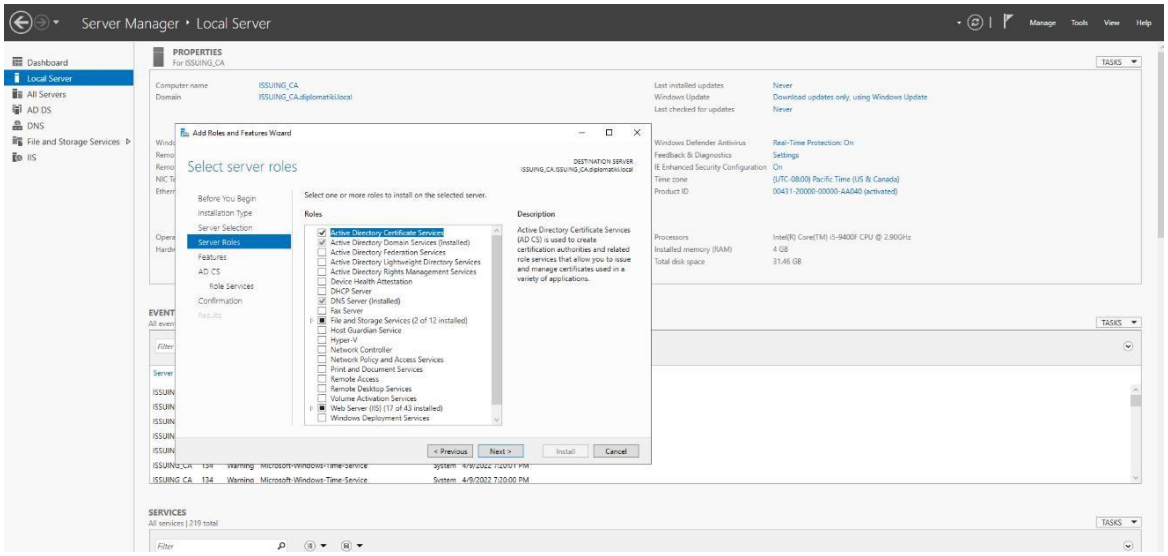


Εγκατάσταση Active Directory Certificate Services

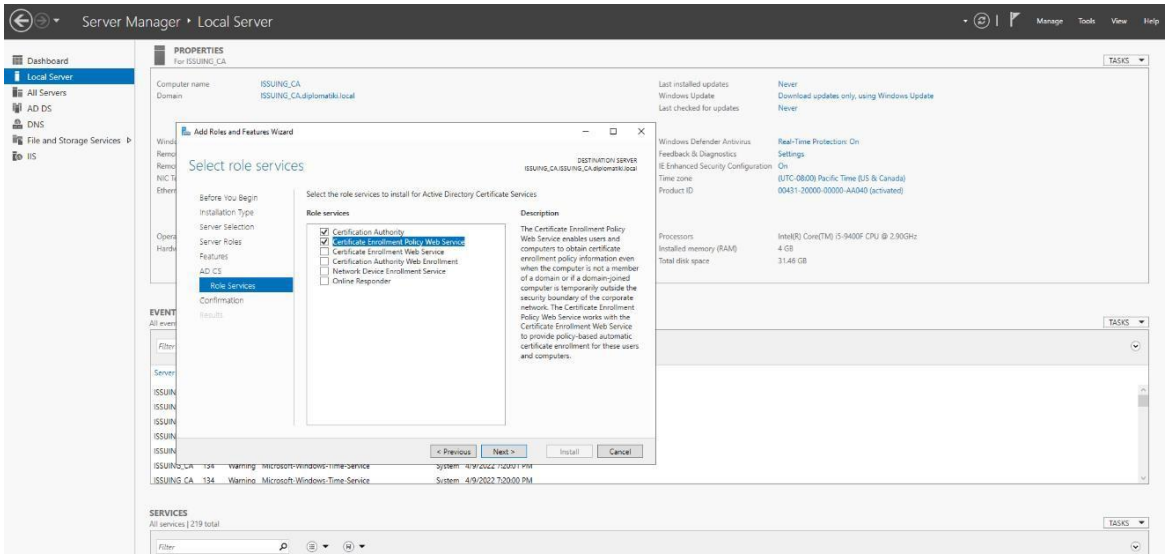
Δημιουργία Εκδούσας Ενδιάμεση Αρχή Πιστοποίησης ((Intermediate CA)

Σε αυτό το βήμα θα δημιουργήσουμε την Αρχής Πιστοποίησης

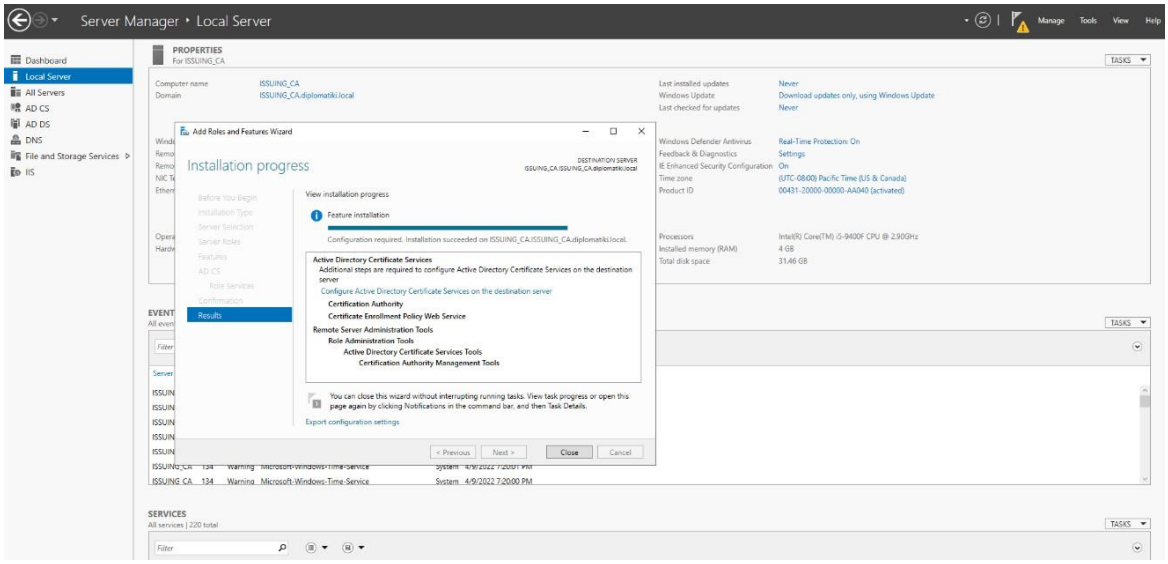
Βήμα 1 – Συνδεόμαστε στο Intermediate CA VM και εγκαθιστούμε το ρόλο Active Directory Certificate Services



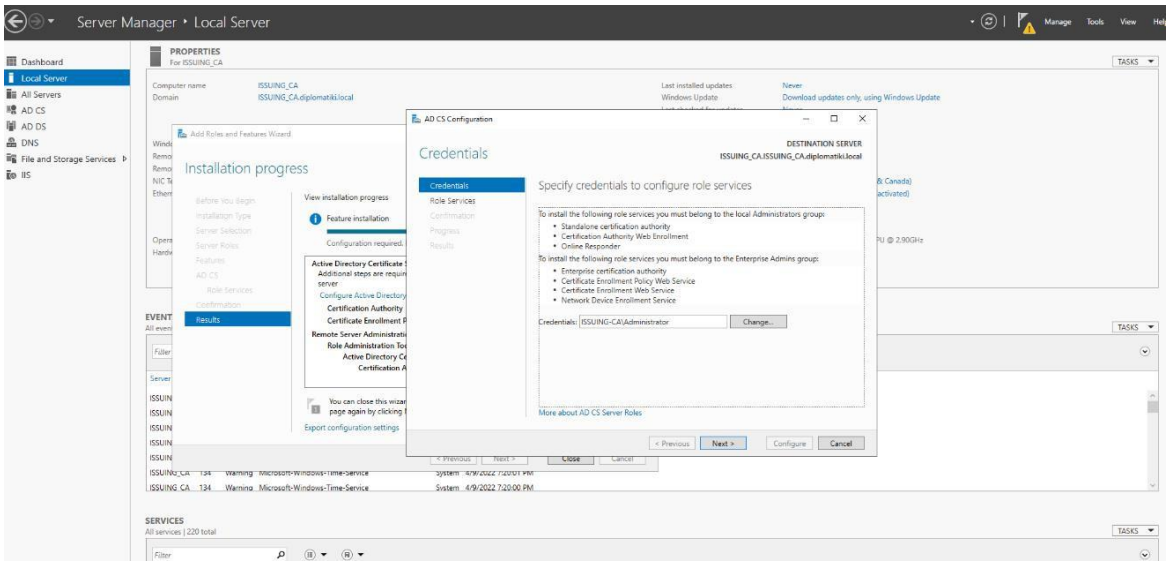
Βήμα 2 – Στην παρακάτω εικόνα επιλέγουμε τις επιλογές Certificate Authority και Certificate Enrollment Policy Web Services



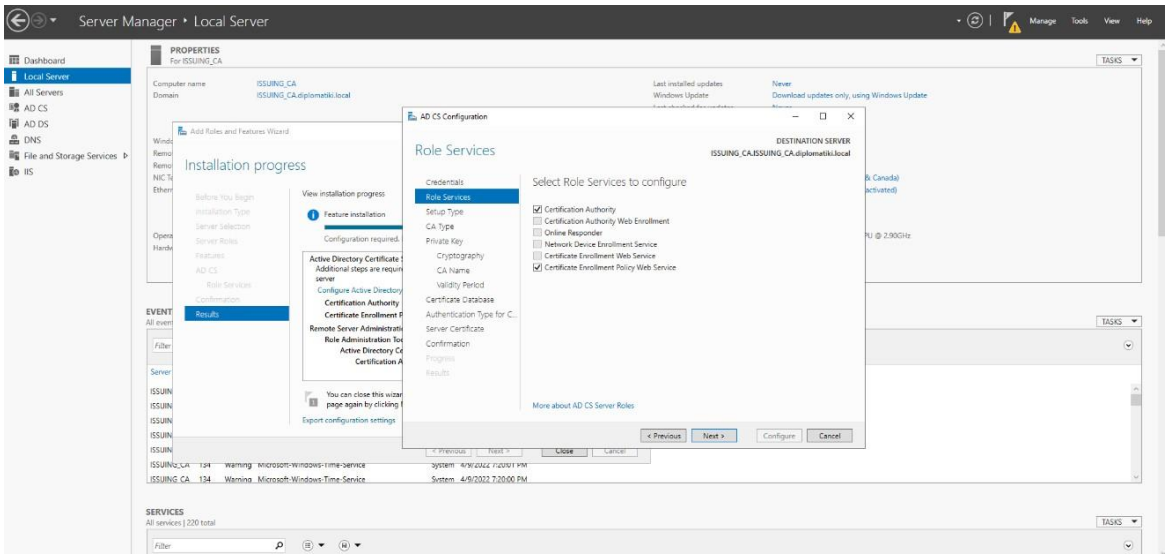
Βήμα 3 – Όπως φαίνεται στην παρακάτω εικόνα η εγκατάσταση έχει ολοκληρωθεί επιτυχώς. Προχωράμε με την παραμετροποίηση του ADCS service.



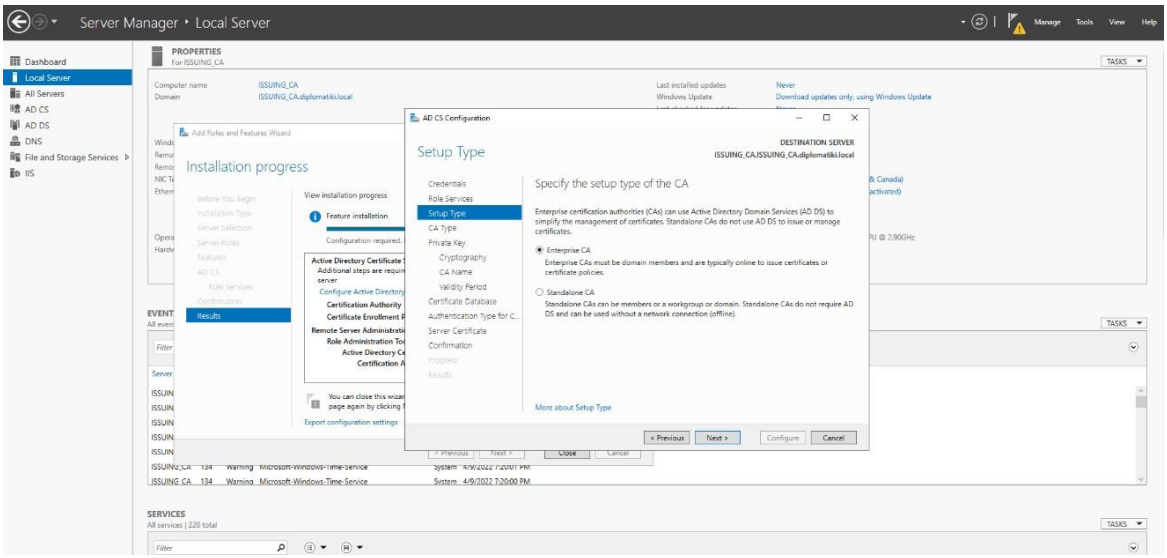
Βήμα 4 – Επιλέγουμε το χρήστη με τον οποίο θα διαμορφώσουμε το Service στην συγκεκριμένη περίπτωση θα χρησιμοποιήσουμε ένα διαχειριστή τομέα



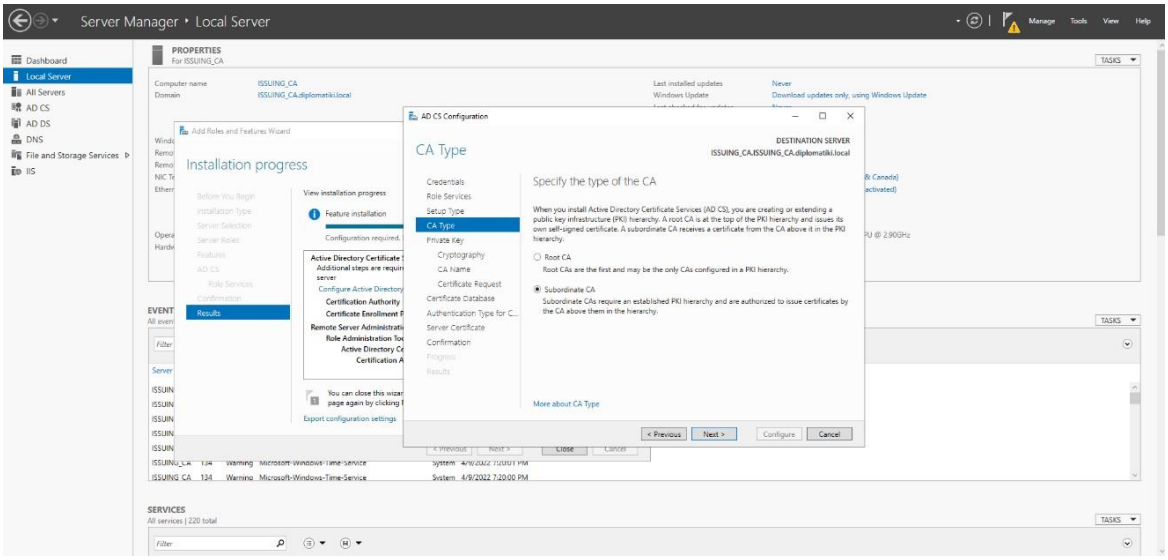
Βήμα 5 – Επιλέγουμε τις επιλογές Certification Authority και Certificate Enrollment Policy Web Service και συνεχίζουμε την παραμετροποίηση



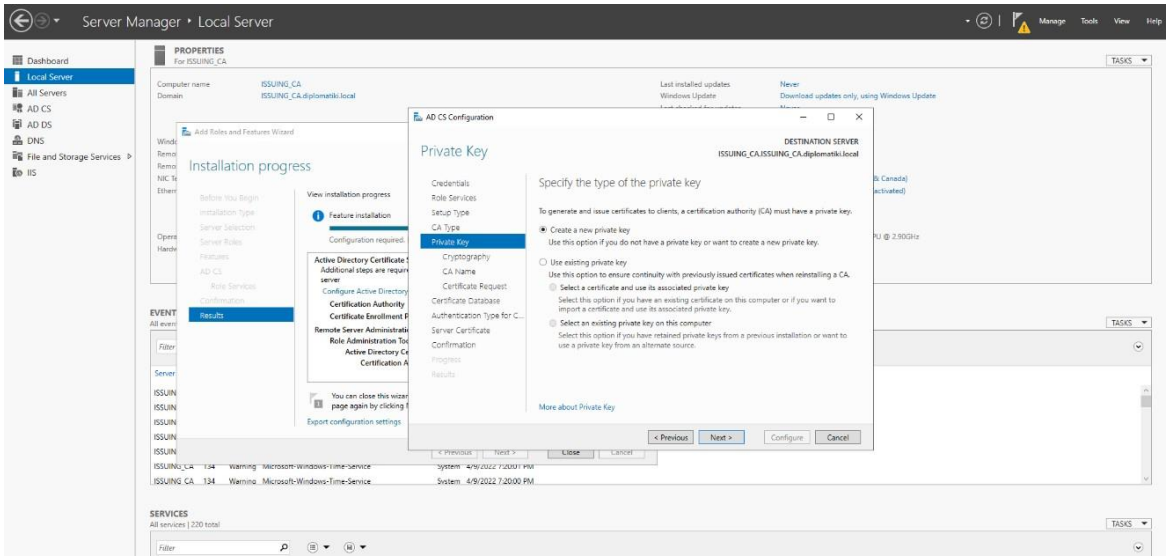
Βήμα 6 – Επιλέγουμε την επιλογή Enterprise CA και συνεχίζουμε την παραμετροποίηση



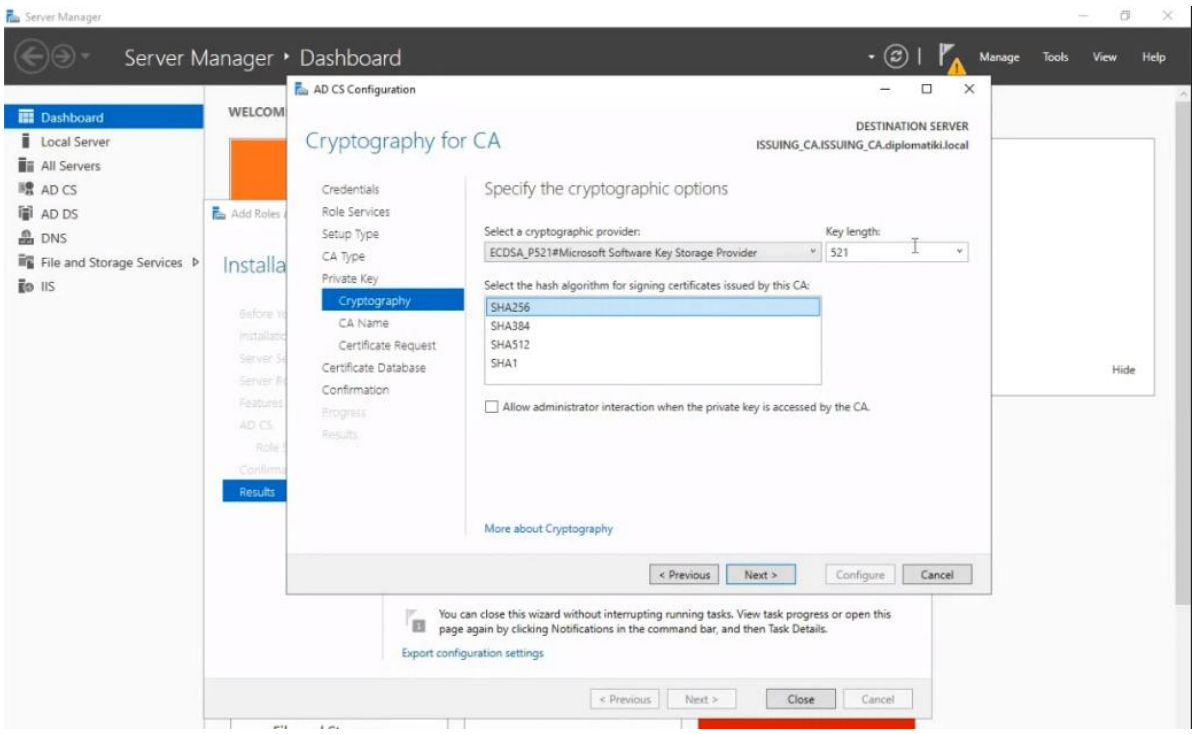
Βήμα 7 – Επιλέγουμε την επιλογή Subordinate CA και συνεχίζουμε την παραμετροποίηση



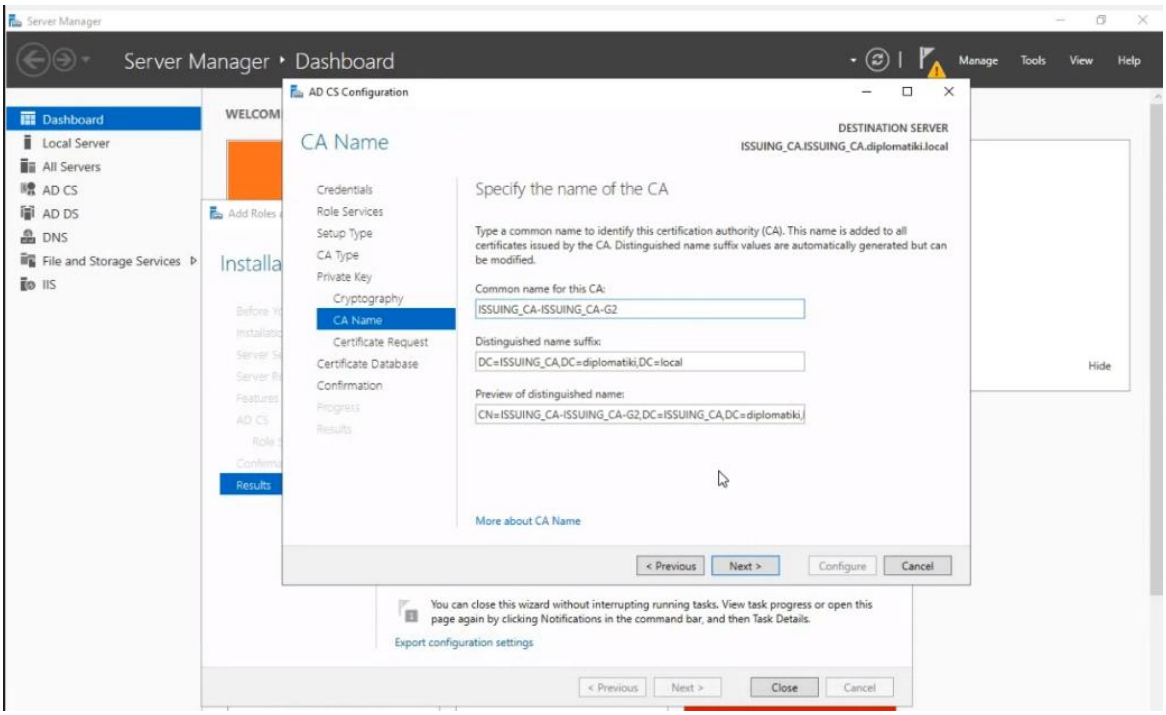
Βήμα 8 – Επιλέγουμε την επιλογή Create a new private key και συνεχίζουμε την παραμετροποίηση



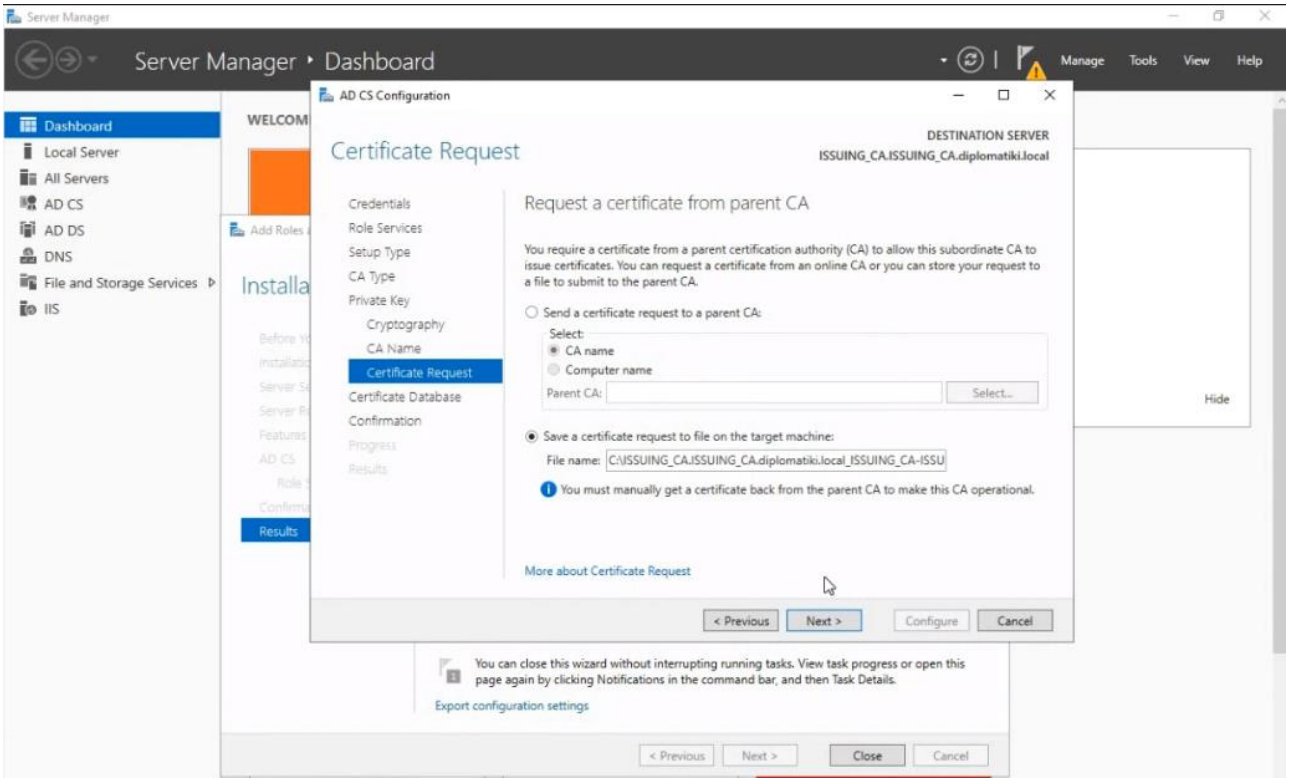
Βήμα 9– Στη παρακάτω εικόνα επιλέγουμε τον αλγόριθμο ελλειπτικής καμπύλης ECDSA με μήκος κλειδιού 521 Bits.



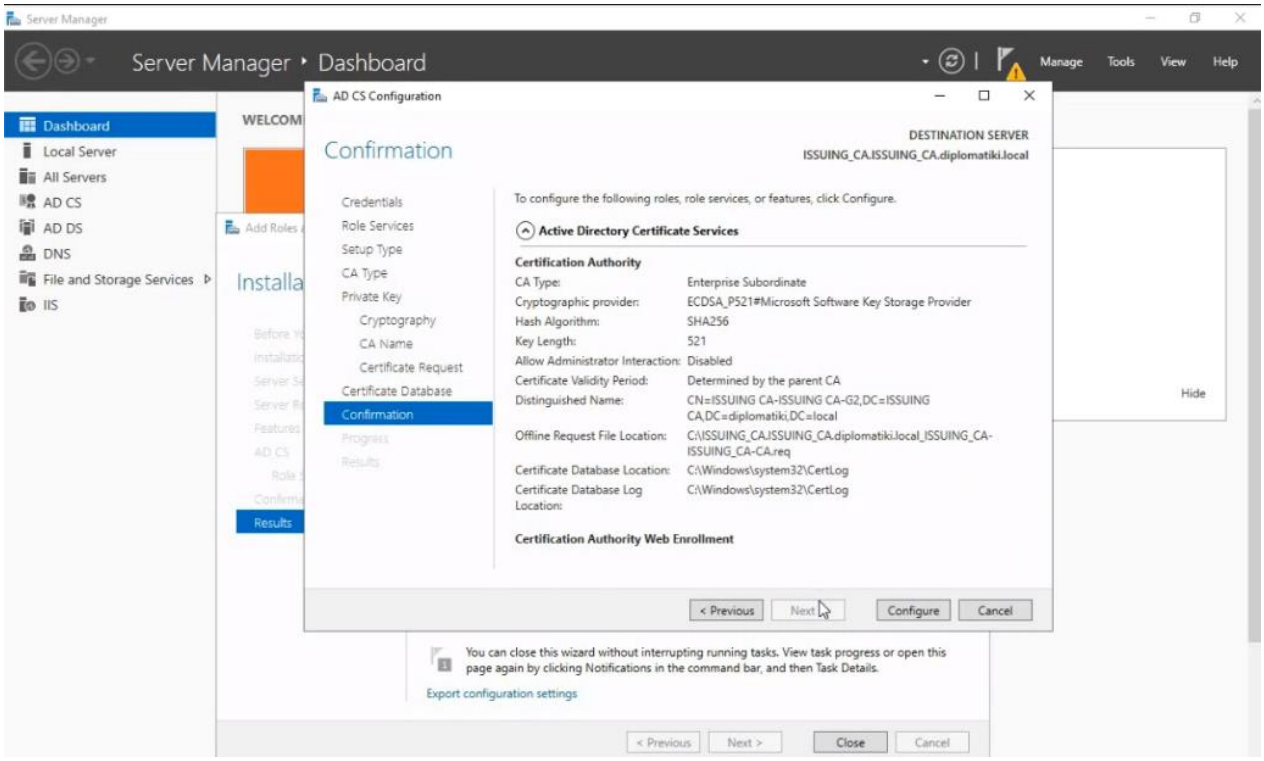
Βήμα 10– Στη παρακάτω εικόνα ορίζουμε τις πληροφορίες που θα περιέχονται το στο Subject DN του πιστοποιητικού.



Βήμα 11– Στη παρακάτω εικόνα θα αποθηκεύσουμε το αίτημα ώστε να το μεταφέρουμε στην Ρίζα Αρχής Πιστοποίησης και να το υπογράψουμε .



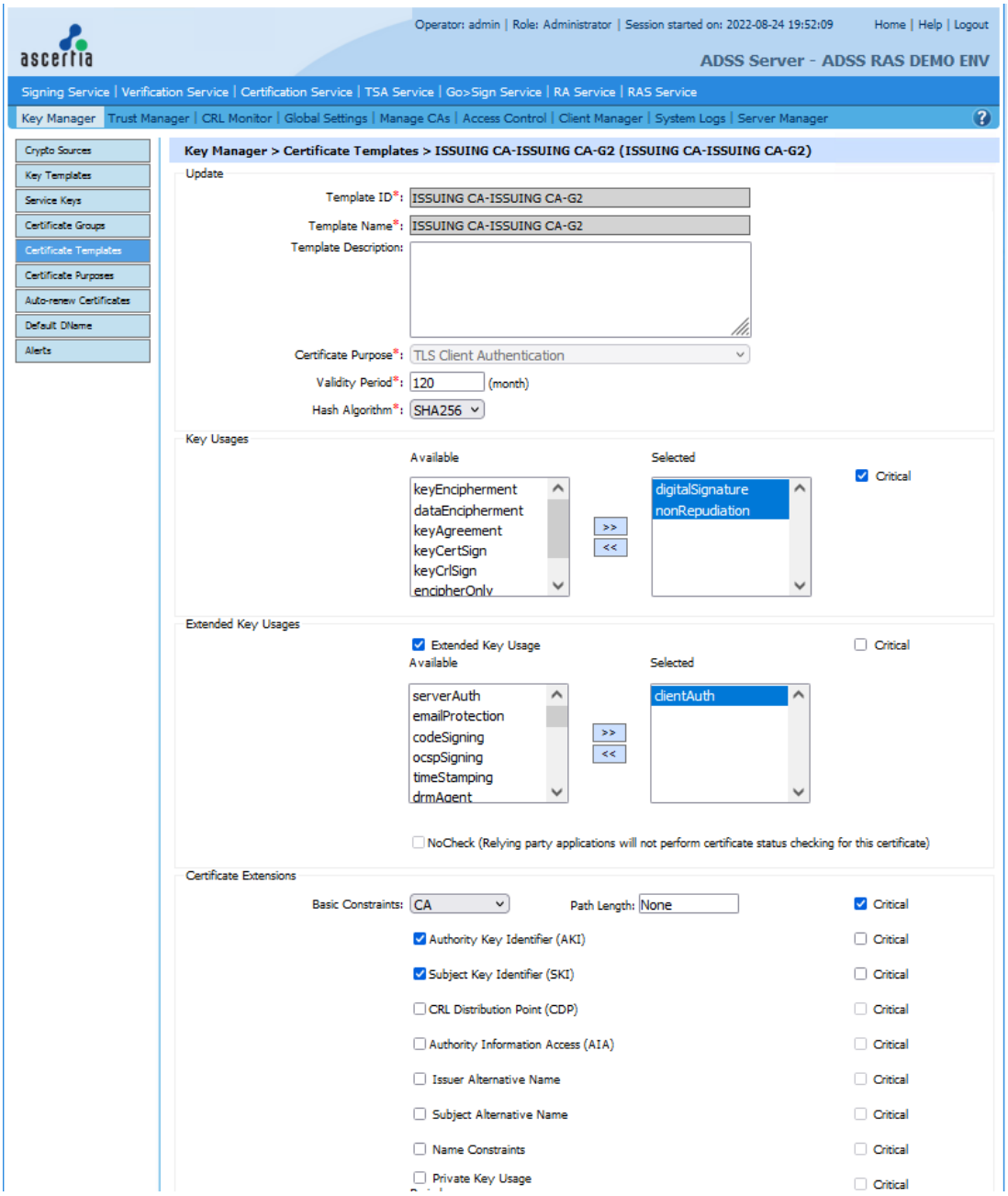
Βήμα 12– Η παραμετροποίηση ολοκληρώθηκε

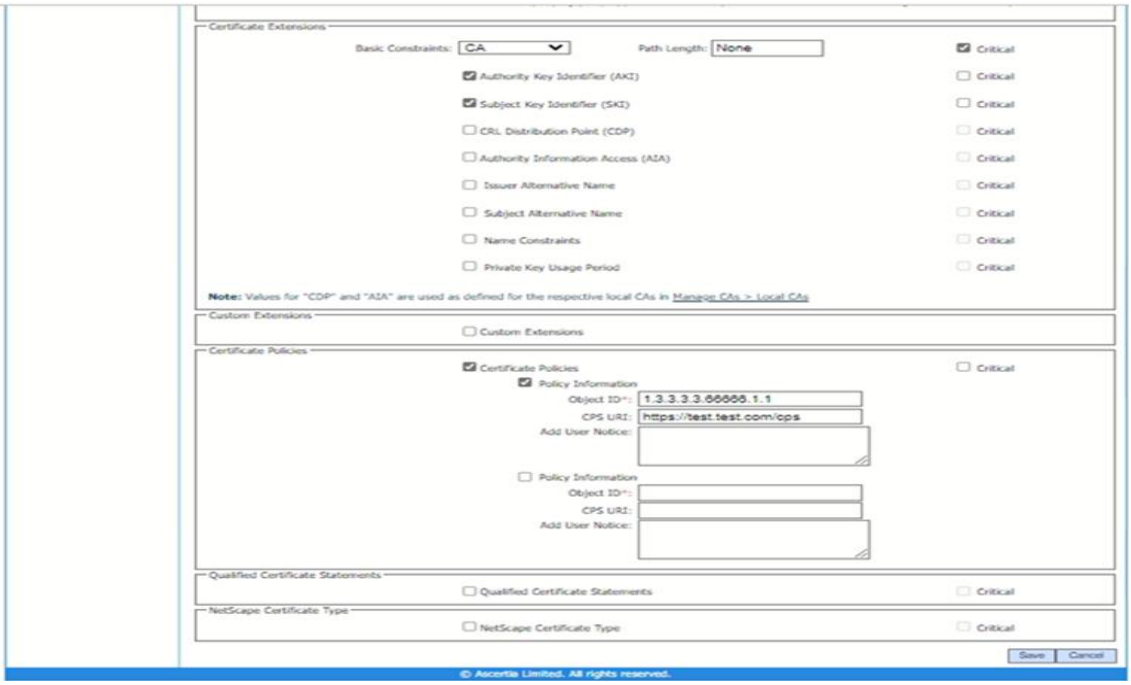


Βήμα 13– Συνδεόμαστε στον ASCERTIA ADSS server για να επεξεργαστούμε το παραπάνω αίτημα.

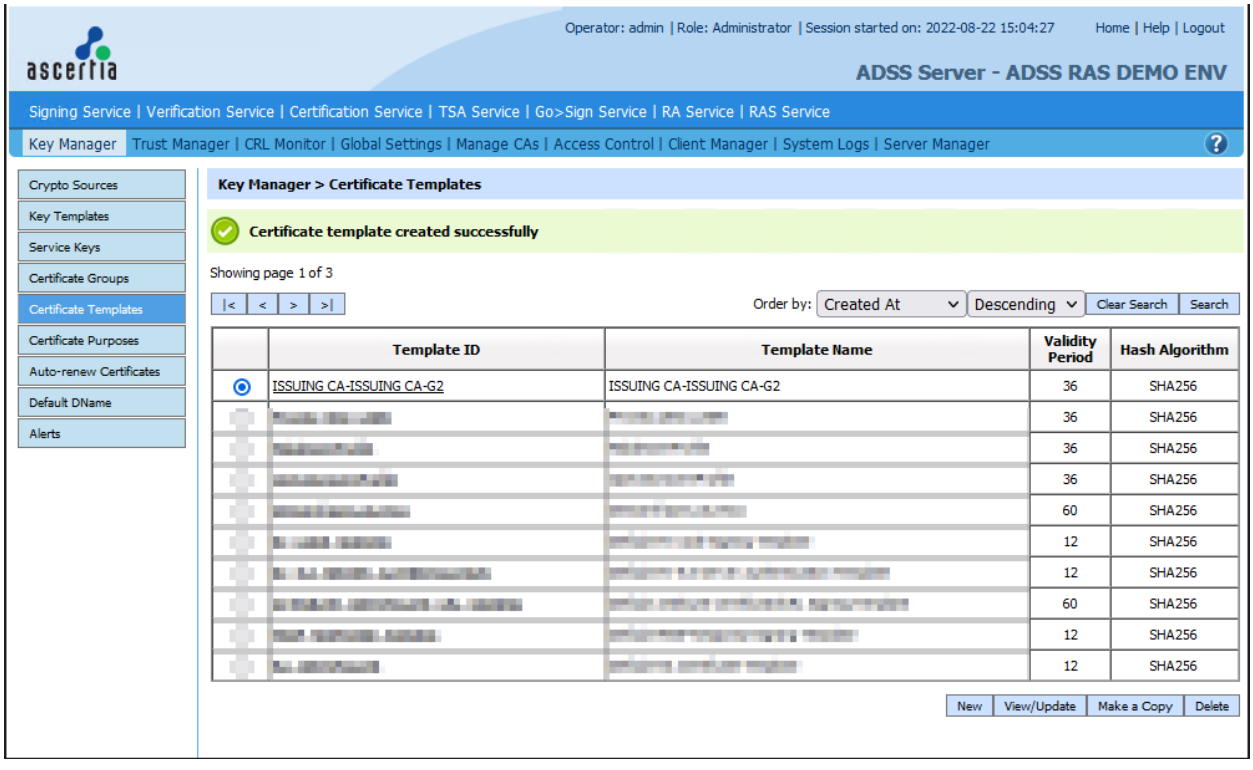
Στην συνέχεια μεταβαίνουμε στην καρτέλα Key Manager → Certificates Templates ώστε να δημιουργήσουμε αυτή την φόρα το προφίλ του πιστοποιητικού της ISSUING CA-ISSUING CA-G2 (Intermediate CA)

Το προφίλ επίσης περιέχει στοιχεία όπως διάρκεια ζωής του πιστοποιητικού , Key Usages, Extended Key Usages και Certificates Polices.





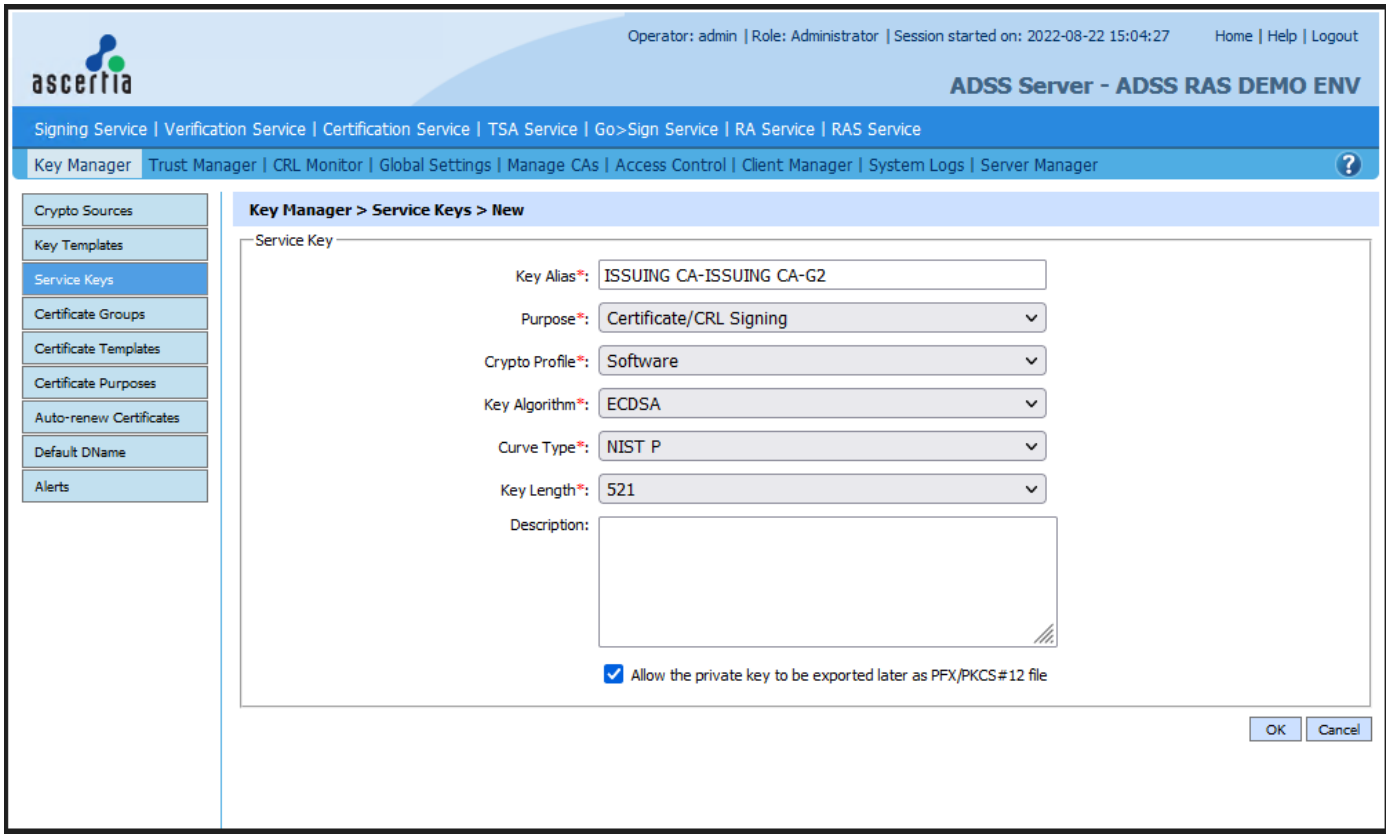
Πατώντας save το προφίλ δημιουργείται με επιτυχία όπως διαπιστώνουμε παρακάτω



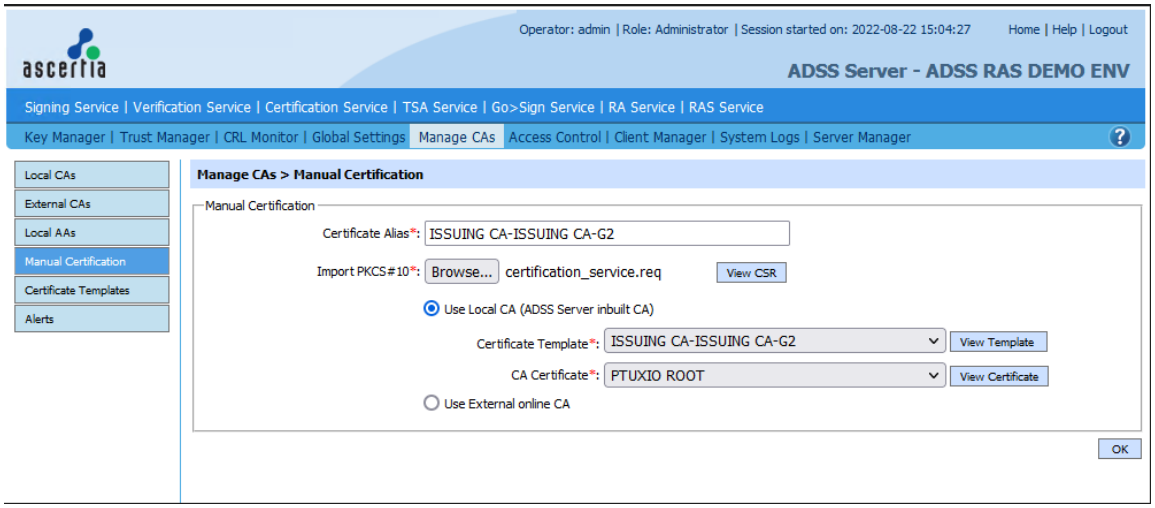
Έχοντας ολοκληρώσει το προφίλ του πιστοποιητικού μεταβαίνουμε στην κατηγορία Service Key για να δημιουργήσουμε τα κλειδία και να συντάξουμε τις πληροφορίες που θα περιέχει το πιστοποιητικού της Ενδιάμεσης Αρχής Πιστοποίησης (Intermediate CA – Certificate Authority)

όπου στην συνέχεια θα την υπογράψει η Αρχή Πιστοποίησης (Root CA) που δημιουργήσαμε και με αυτόν τον τρόπο θα δημιουργηθεί η αλυσίδα εμπιστοσύνης ανάμεσα στα δυο πιστοποιητικά.

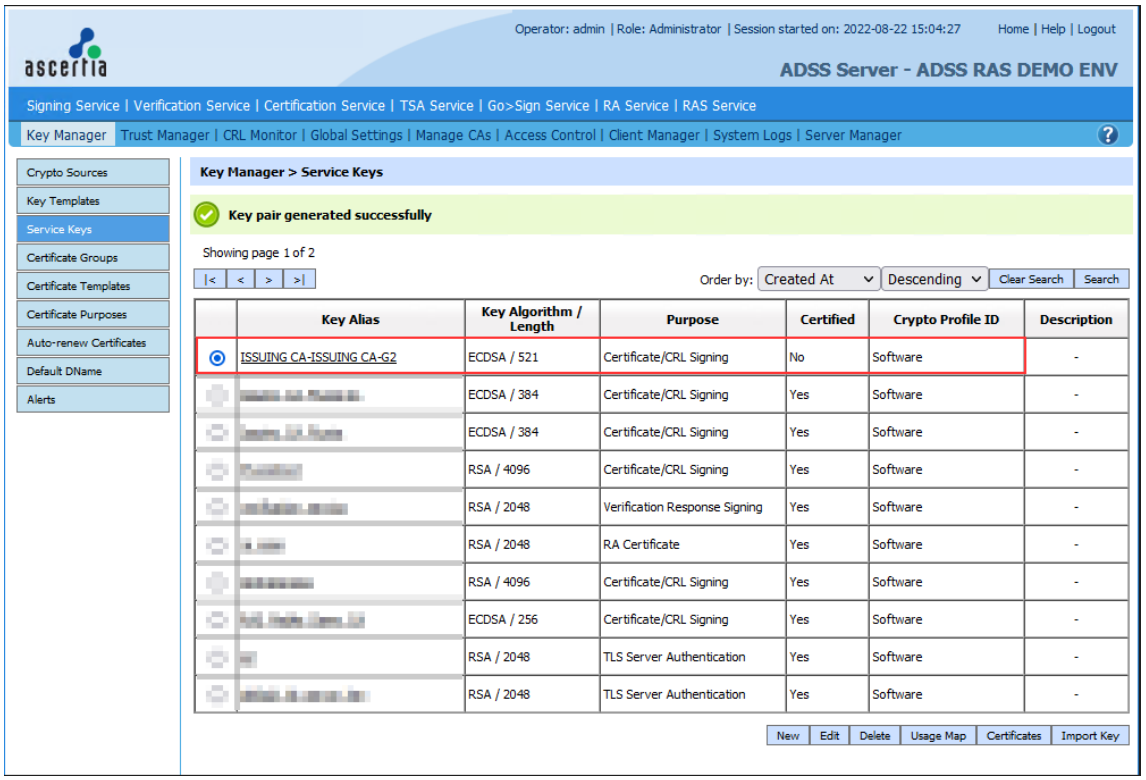
Η Intermediate CA θα δημιουργηθεί με αλγόριθμο ελλειπτικών καμπυλών ECDSA , τύπο καμπύλης NIST P και με μέγεθος κλειδιού 521 Bits.



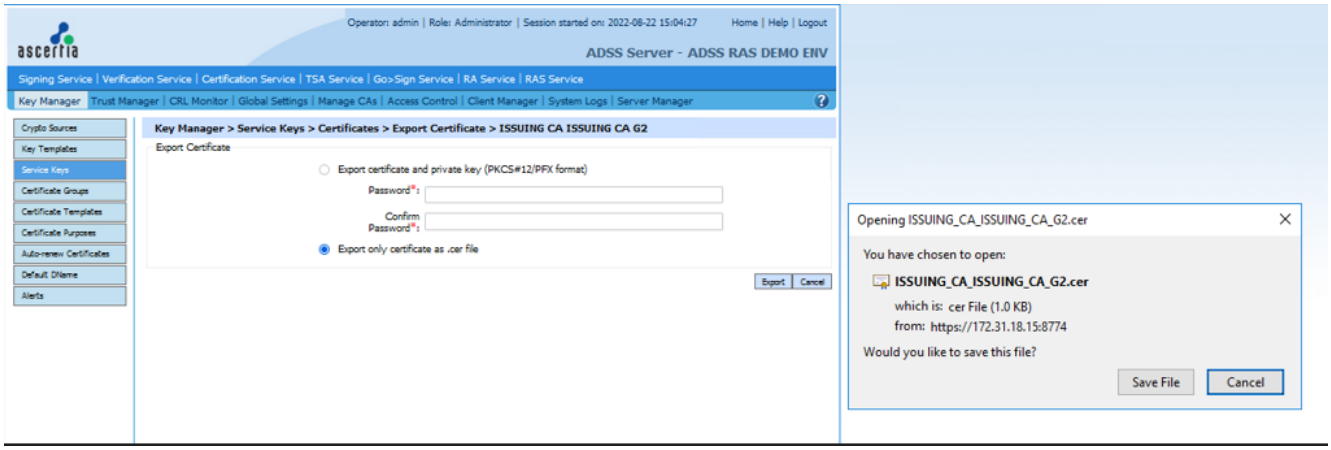
Στην συνέχεια κάνουμε εισαγωγή του αιτήματος που δημιουργήθηκε από το Microsoft PKI server για να υπογραφεί από την ROOT CA



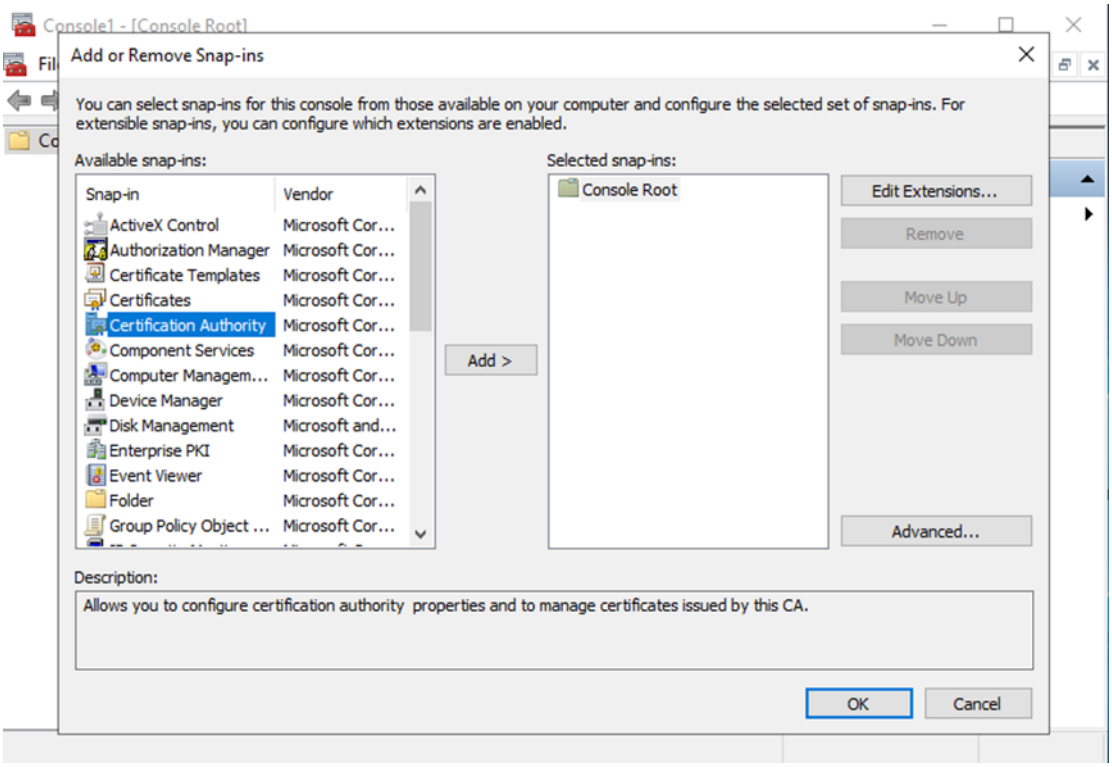
Στην παρακάτω εικόνα βλέπουμε την επιτυχημένη δημιουργία των κλειδιών.



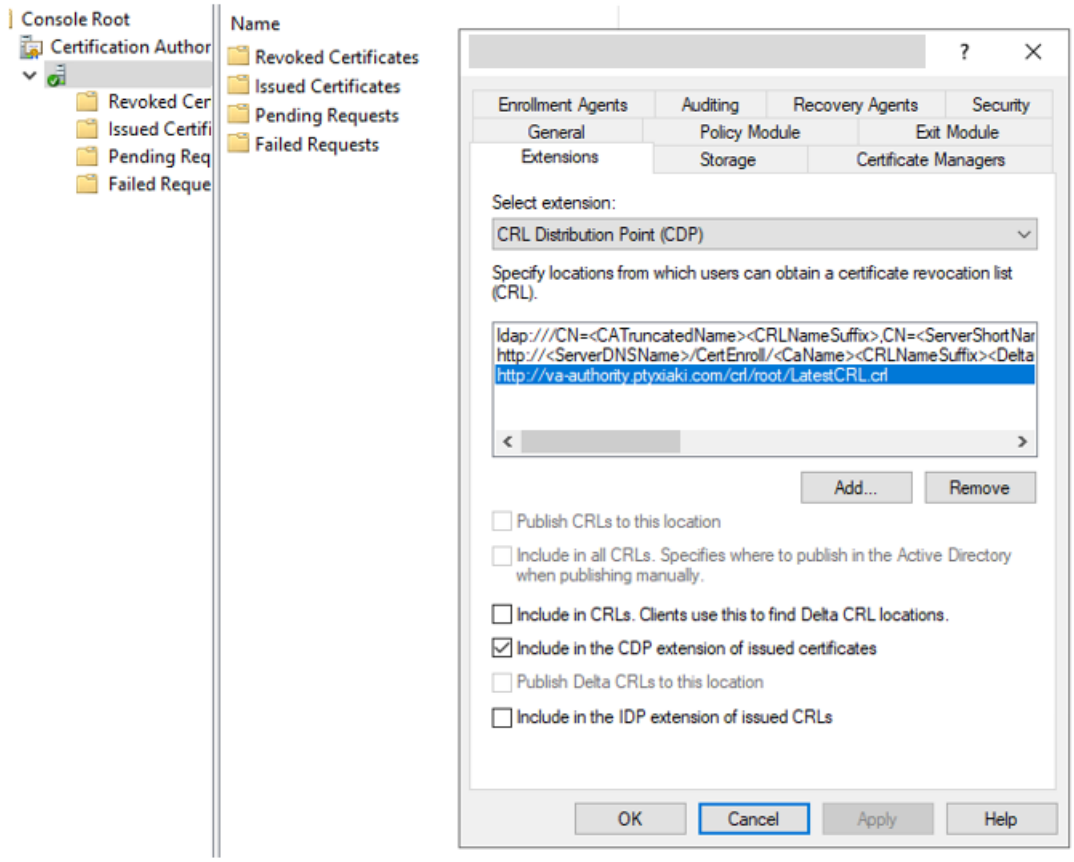
Το πιστοποιητικό δημιουργήθηκε με επιτυχία το αποθηκεύουμε και το μεταφέρουμε στο Microsoft PKI server για να το εγκαταστήσουμε.



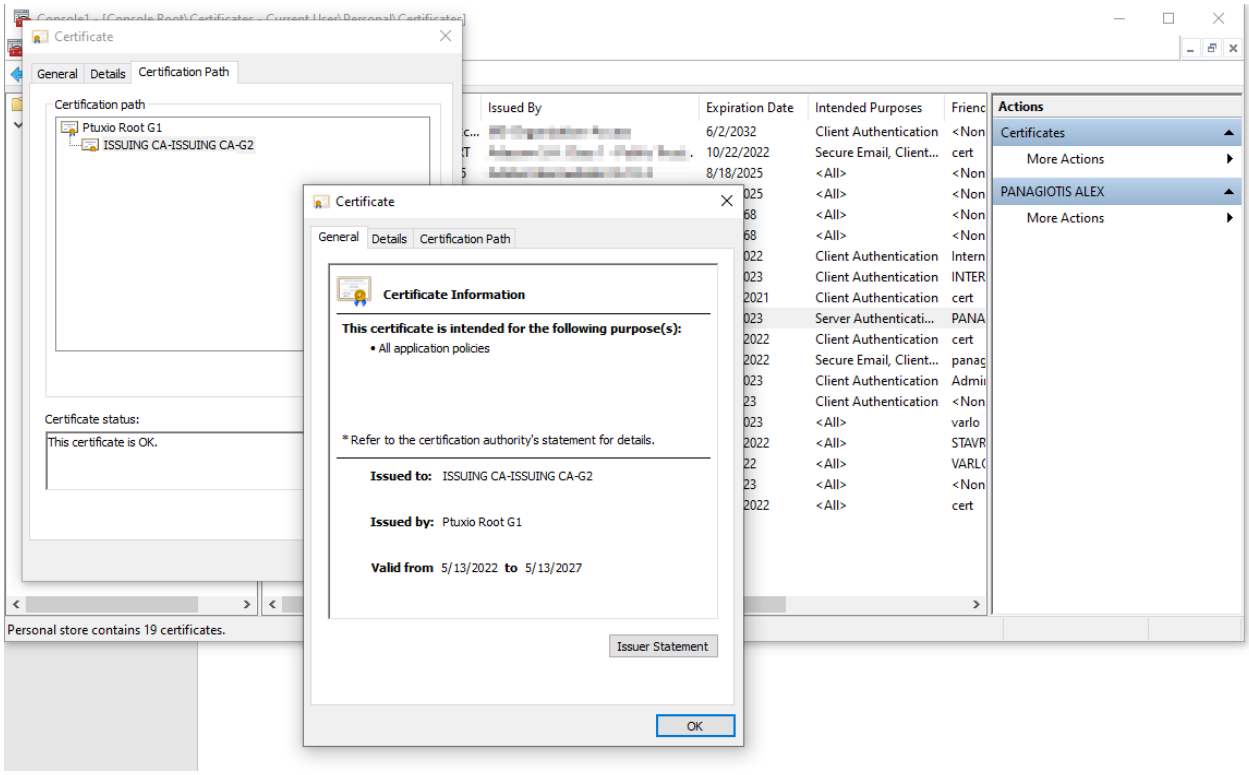
Βήμα 14 - Συνδεόμαστε στο Intermediate CA VM για να επεξεργαστούμε το παραπάνω αίτημα. Ανοίγουμε MMC κονσόλα , από το μενού επιλέγουμε File -> Add/Remove Snap-in



Βήμα 15– Επιλέγουμε την επιλογή Ρίζα Αρχής Πιστοποίησης και από τις ρυθμίσεις ορίζουμε το σημείο διανομής ανακληθέντων πιστοποιητικών



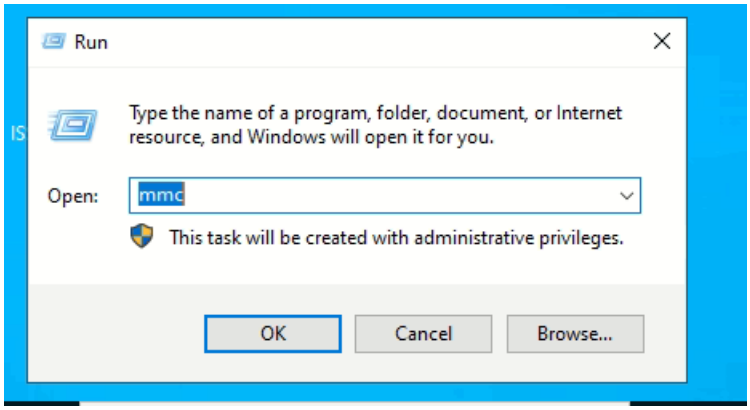
Βήμα 16– Επιλέγουμε την επιλογή Certification Authority και από τις ρυθμίσεις επιλέγουμε Submit new request και issue. Η Αρχή Πιστοποίησης εκδόθηκε.

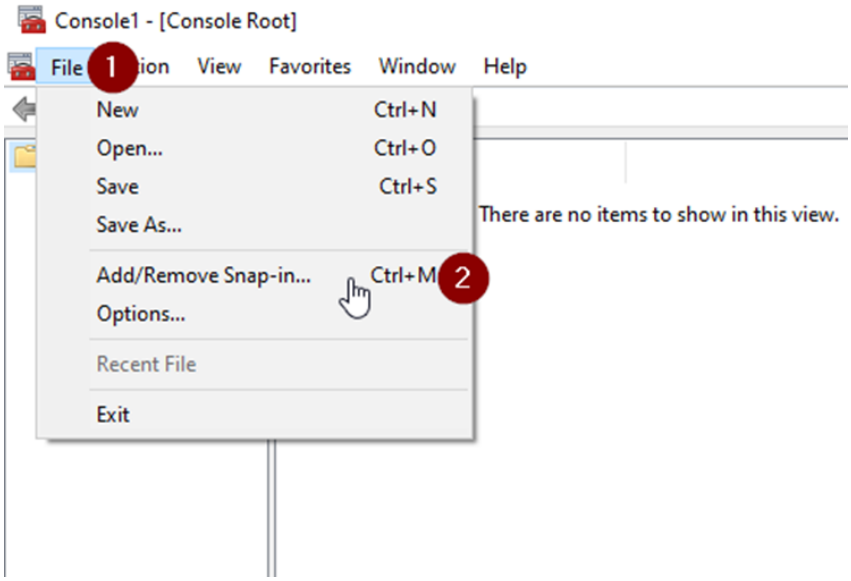


Δημιουργία πιστοποιητικών τελικών χρηστών

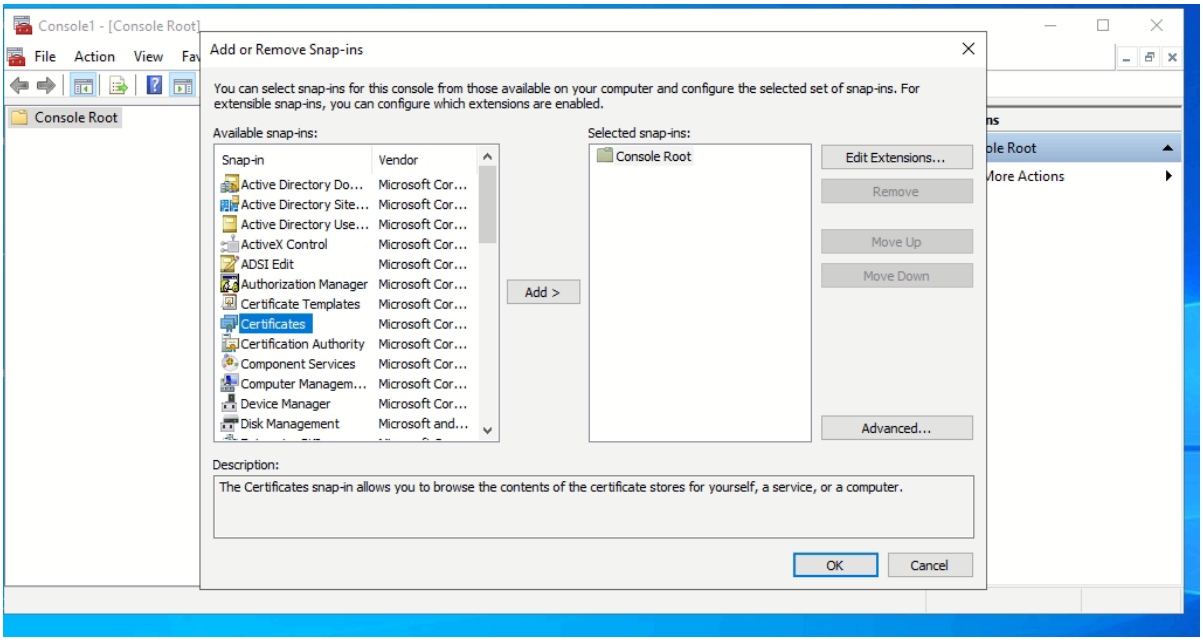
Παρακάτω θα δούμε το τρόπο πως μπορούμε να στείλουμε ένα μη αυτοματοποιημένο αίτημα για ψηφιακό πιστοποιητικό μέσω της MMC κονσόλας των windows.

Βημά1 – Ανοίγουμε την MMC κονσόλα

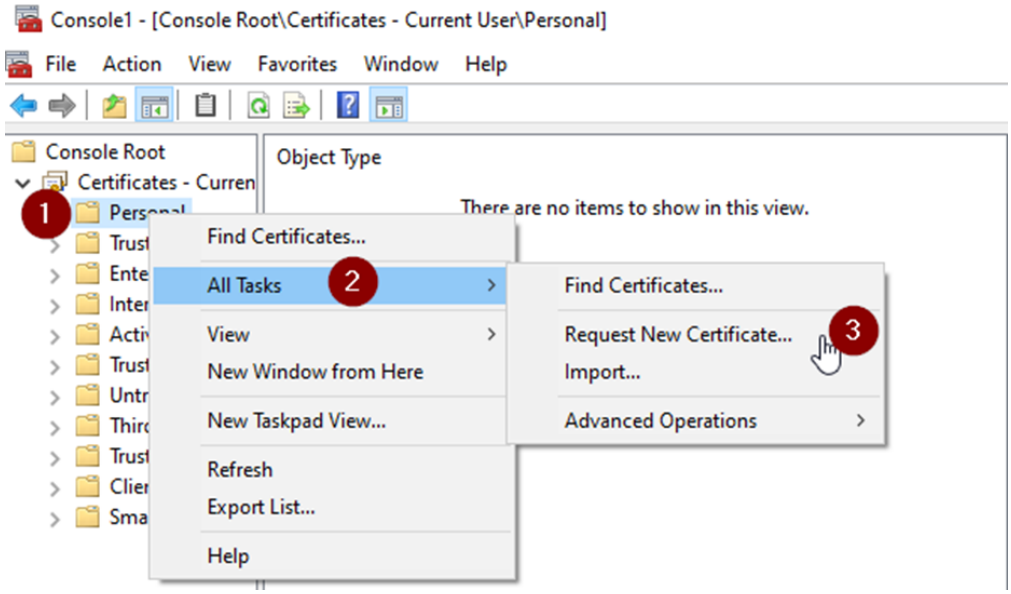




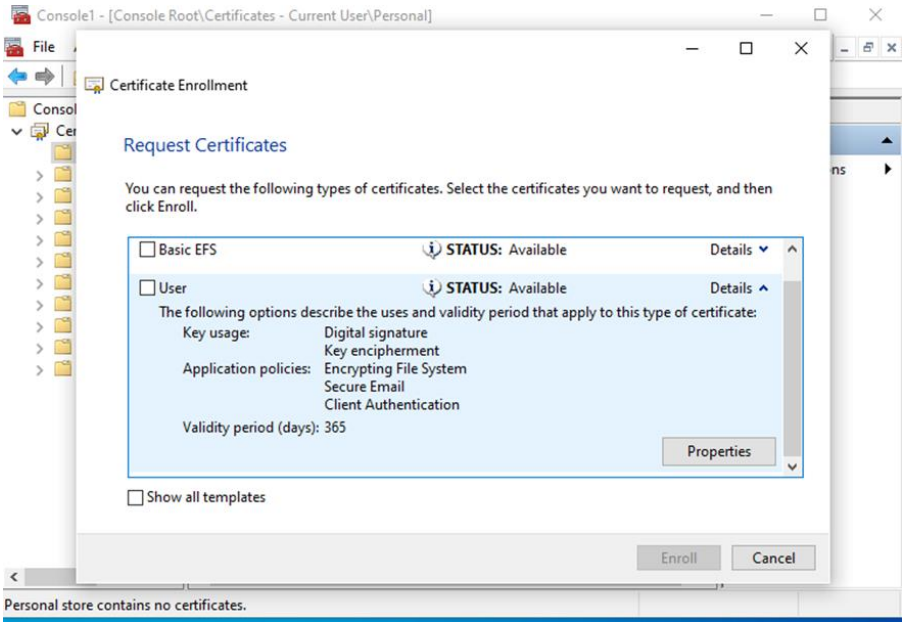
Βήμα2 – Επιλέγουμε την επιλογή Certificates και πατάμε OK



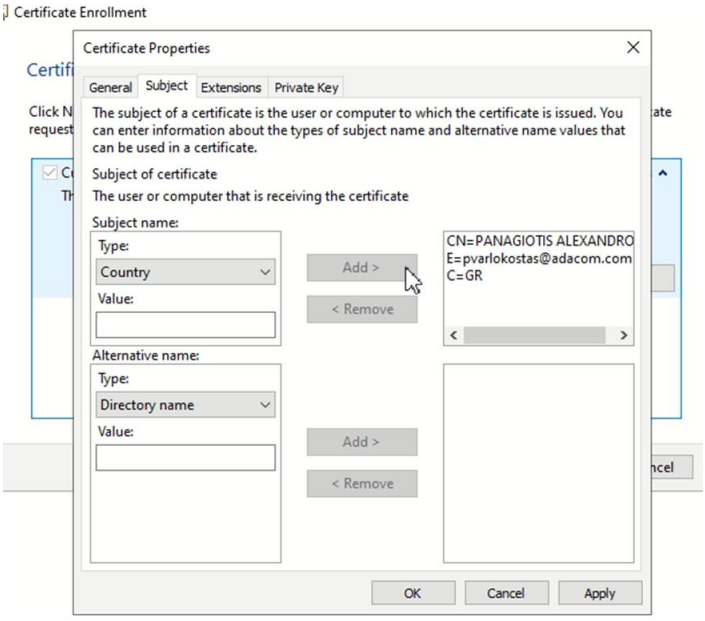
Βήμα3 -Επιλέγουμε Request New Certificate

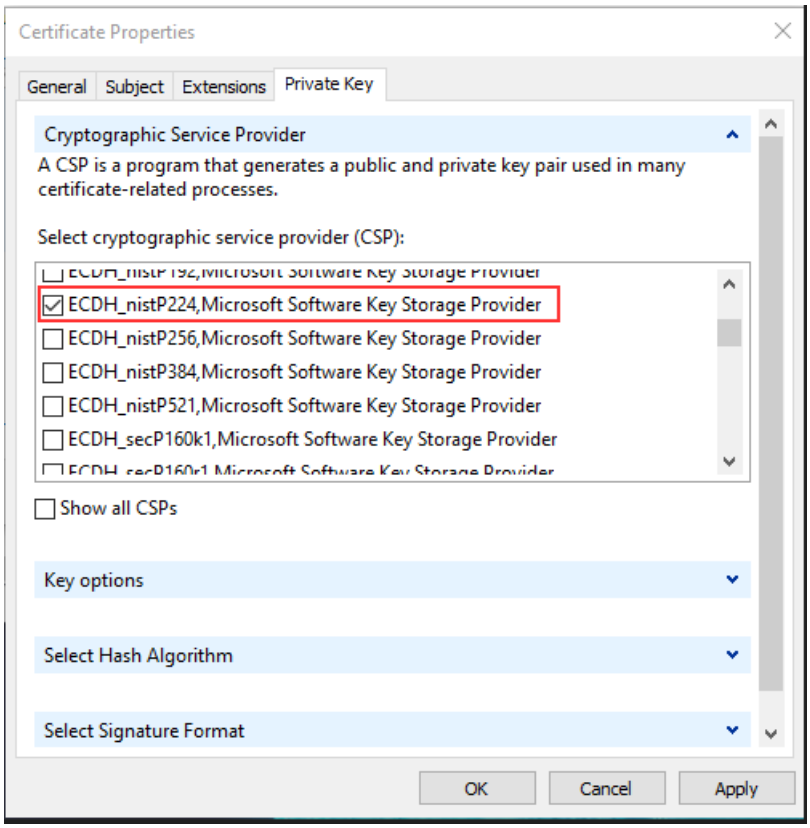


Βήμα 4 – Επιλέγουμε ένα διαθέσιμο τύπο πιστοποιητικού που μας ενδιαφέρει, οι συγκεκριμένοι τύποι ορίζονται μέσω Πολιτικών και μπορούν να εφαρμοστούν για όλους αλλά και για συγκεκριμένες ομάδες χρηστών.

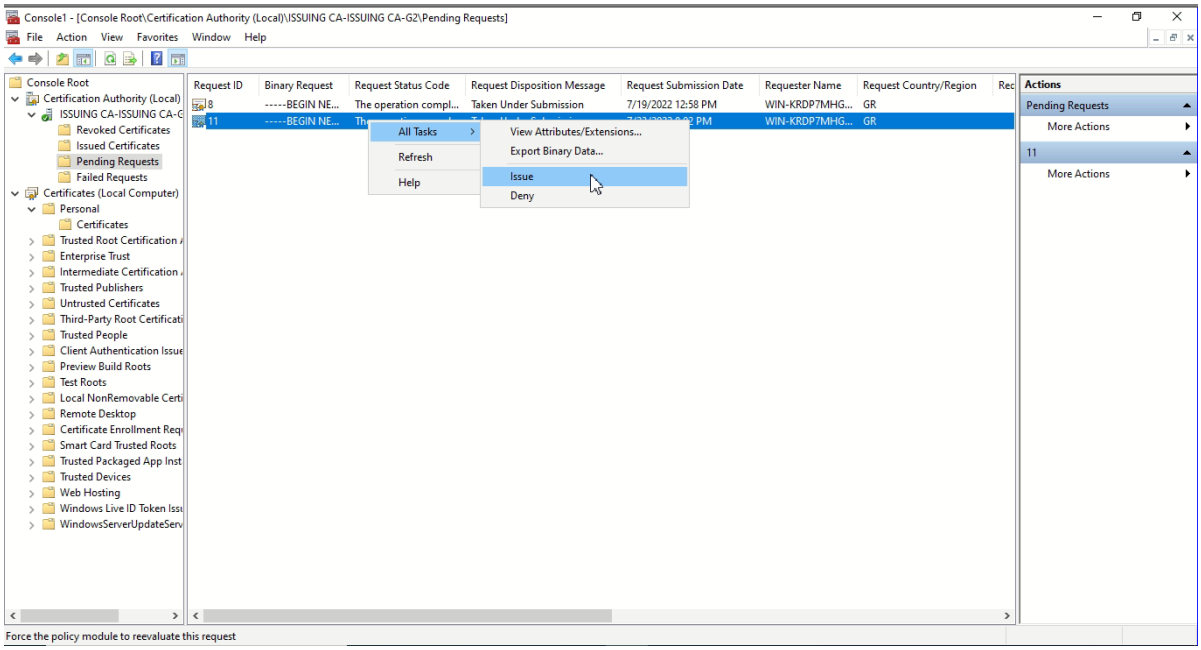


Βήμα 5 – Κάνουμε καταχώρηση των στοιχείων που θέλουμε να έχει το πιστοποιητικό

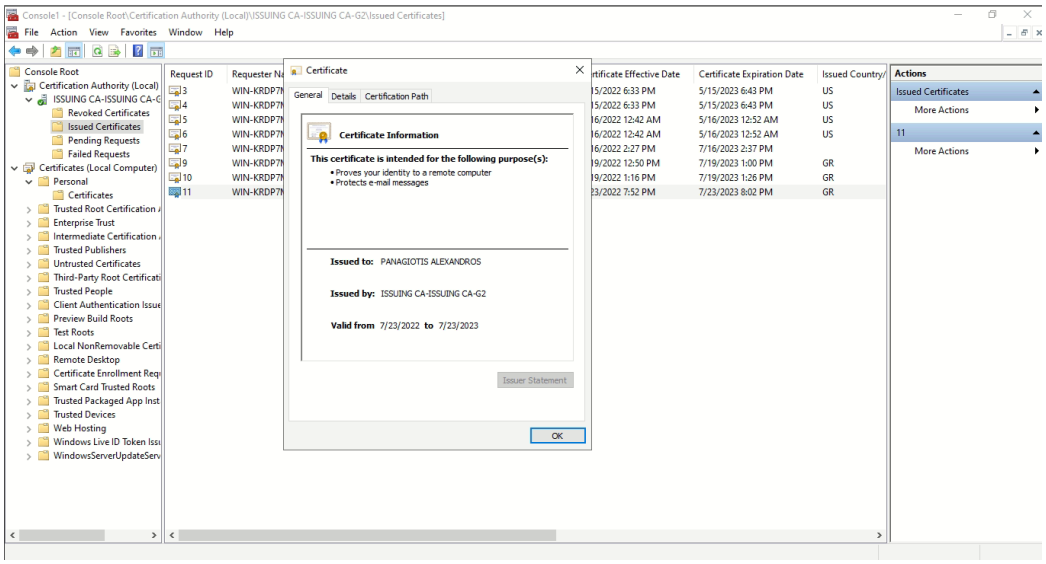


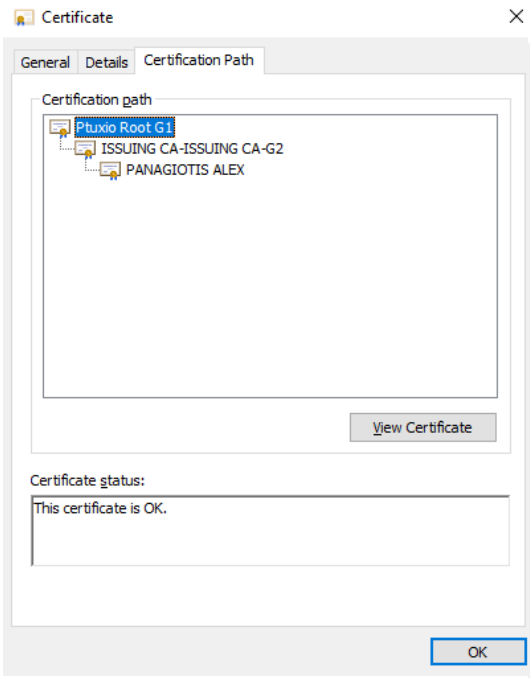


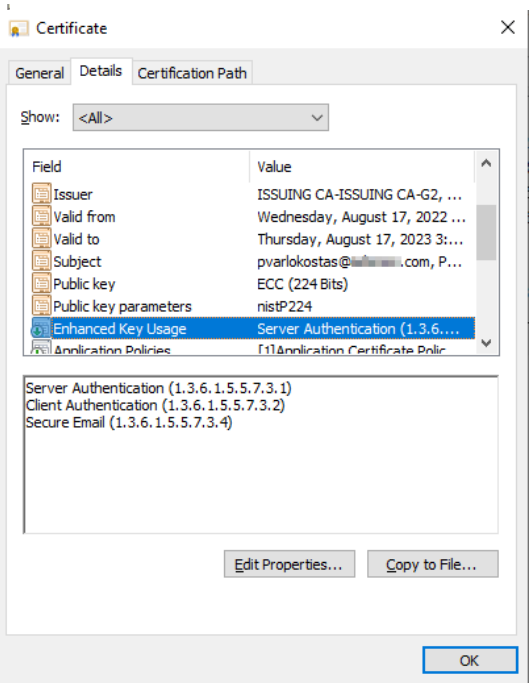
Βήμα 5 – Επιλέγουμε την λειτουργεία ISSUE για να εκδοθεί το πιστοποιητικό από την CA

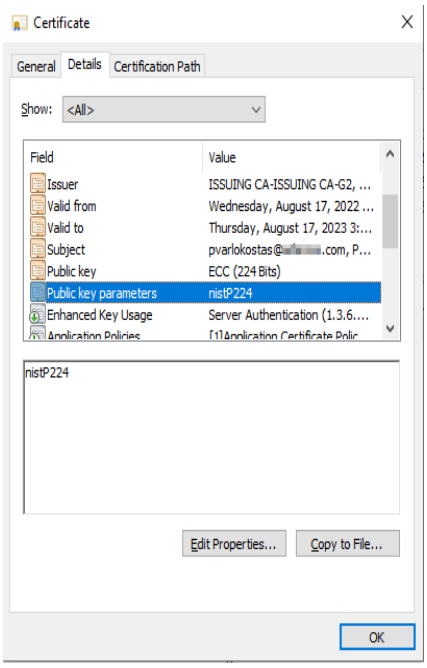


Βήμα 6 – Γίνεται η έκδοση του πιστοποιητικού





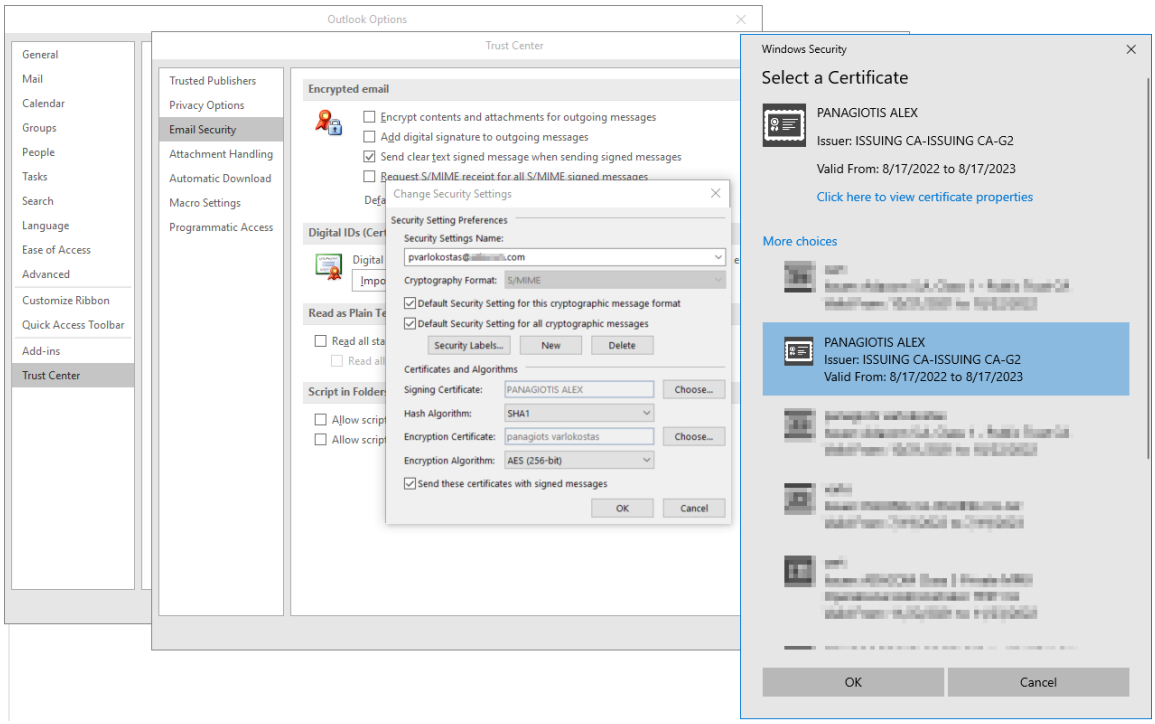




Εγκατάσταση πιστοποιητικού στο Microsoft Outlook και αποστολή δοκιμαστικού ηλεκτρονικου υπογεγραμμένου μηνυματος αλληλογραφίας.

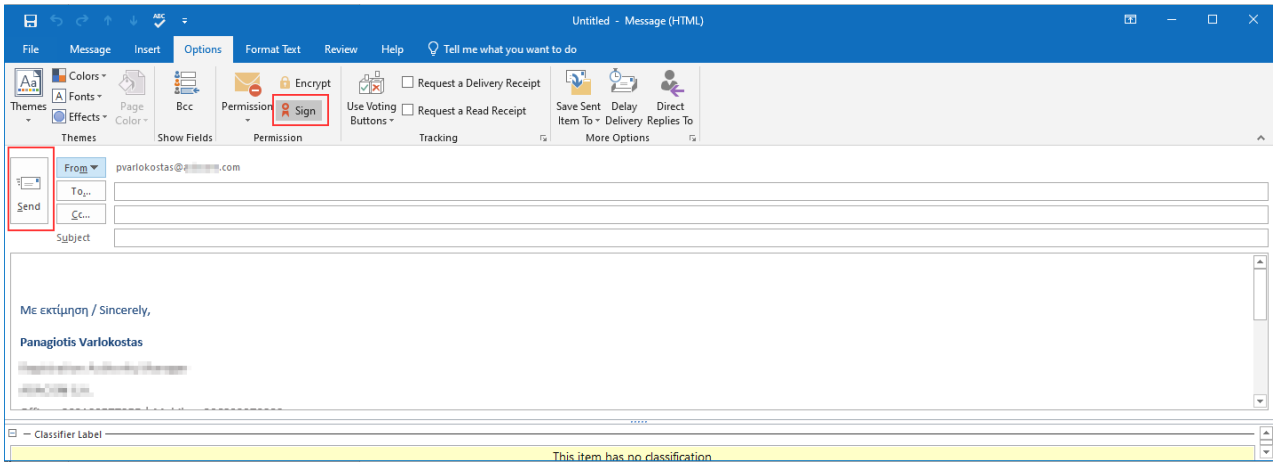
Βήμα 1- Συνδεόμαστε στο **Microsoft Outlook** και πηγαίνουμε file → options

1. Θα εμφανιστεί ένα παράθυρο με τίτλο Επιλογές του Outlook. Στο αριστερό τμήμα του παραθύρου, κάντουμε κλικ στο Trust Center
2. Στην συνέχεια κάνουμε κλικ στο κουμπί Trust Center Settings στην κάτω δεξιά πλευρά.
3. Θα εμφανιστεί ένα παράθυρο με το όνομα Trust Center. Στην αριστερή πλευρά θα δούμε πολλαπλές επιλέξιμες επιλογές.
4. Κάνουμε κλικ στο Email Security .
5. Επιλέγουμε το Email Security, θα εμφανιστεί ένα αναπτυσσόμενο πεδίο δίπλα στην Προεπιλεγμένη ρύθμιση.
6. Κάνουμε κλικ στις Ρυθμίσεις δίπλα σε αυτό το πεδίο.
7. Θα εμφανιστεί ένα νέο παράθυρο με το όνομα Change Security Settings. Σε αυτό το παράθυρο, θα εμφανιστούν δύο επιλογές για Επιλογή.
8. Ένα στην ενότητα Certificates .
9. Επιλέγουμε το πιστοποιητικο μας και πατάμε OK

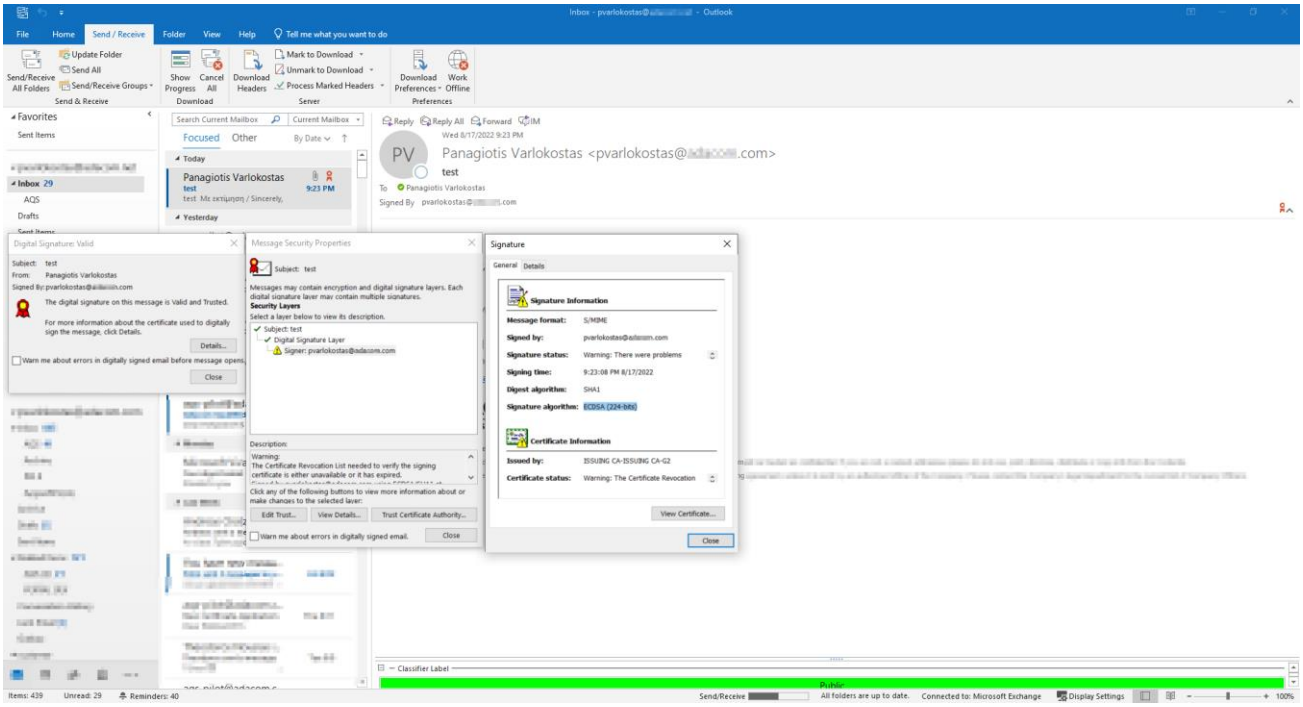


Βήμα 2- Αφού επιλέξουμε το πιστοποιητικό στην συνέχεια κάνουμε μια δοκιμαστική αποστολή μηνύματος για να δούμε αν το πιστοποιητικό μας το υπογράφει με επιτυχία.

Επιλέγουμε New Email πηγαίνουμε στην καρτέλα options πατάμε την επιλογή Sign και στην συνέχεια κάνουμε αποστολή



Βήμα 3- Το μήνυμα μας αποστάλθηκε και υπογράφηκε με επιτυχία



8

Συμπεράσματα

Η παρούσα διπλωματική εργασία αποτελεί μια ολοκληρωμένη ανάλυση μια Υποδομής Δημοσίου Κλειδιού βασισμένη στις πλατφόρμες Ascertia ADSS server και Microsoft PKI Windows Server 2019 . Η διαδικασία της μελέτης αλλά και της υλοποίησης της υποδομής οδήγησαν σε μερικές ενδιαφέρουσες παρατηρήσεις.

Αρχικά βάση της έρευνας που έγινε, οι περισσότερες Υποδομές Δημοσίου κλειδιού παγκοσμίως παράγουν πιστοποιητικά ιεραρχίας με κρυπτογραφικό αλγόριθμο και σχήμα υπογραφής RSA και συνήθως από μία πλατφόρμα .

Με βάση αυτή την πληροφορία αυτό κατέστησε πρόκληση στην συγκεκριμένη υποδομή να κάνει χρήση αλγόριθμους κρυπτογράφησης ελλειπτικών καμπυλών δημιουργώντας έτσι ενδιάμεσες Αρχές πιστοποίησης και πιστοποιητικά τελικού χρήστη.

Ως εκ τούτου η χρήση των αλγόριθμων ελλειπτικής καμπύλής θα μπορούσε να καταστεί μια λύση εξοικονόμησης μνήμης , μεγαλύτερης ασφάλειας και ταχύτερης επίδοσης στην δημιουργία και χρήση ψηφιακών πιστοποιητικών και των λειτουργικών συστημάτων που τα υποστηρίζουν.

Ακόμα μεγαλύτερο ενδιαφέρον ήταν το γεγονός ότι και οι πλατφόρμες συνεργάστηκαν για την παραγωγή των πιστοποιητικών ιεραρχίας σε βαθμό άνω του αναμενόμενου.

Η συνεργασία αυτή θεωρείτε ένα υβριδικό μοντέλο παραγωγής και χρήσης των πιστοποιητικών όπου κάλλιστα θα μπορεί σε πραγματικές συνθήκες να είναι ένα λειτουργικό περιβάλλον ή μια λύση μετάβασης από την μία πλατφόρμα στην άλλη.

Επίσης θα πρέπει να τονιστεί η χρησιμότητας μια τέτοια υποδομής εντός ενός εταιρικού δικτύου ή ενός οργανισμού. Με απλά βήματα μπορούμε να δούμε πως ένα οργανισμός ή ένας χρήστης μπορεί να αυξήσει στο μέγιστο την ακεραιότητα, την αυθεντικοποίηση αλλά και την ασφάλεια μια συναλλαγής εντός του δικτυού του.

Η ΥΔΚ πέρα από ένα σύνολο τεχνολογιών αποτελείτε από πολλές πολιτικές που αποσκοπούν στην διαφάνεια κάθε πράξης και στην ακεραιότητα τους. Η παραπάνω ΥΔΚ θεωρείτε έγκυρη εντός ενός εταιρικού δικτύου ή/και οργανισμού με τις αντίστοιχες ενέργειες που γίνονται από τους διαχειριστές αυτής της υποδομής.

Εν Κατακλείδι, πιθανές βελτιώσεις σε μια αντίστοιχη ΥΔΚ θα μπορούσε να είναι η δημιουργία των ιδιωτικών κλειδιών των ΑΠ σε ένα Cloud HSM, η υιοθέτηση πολιτικών για χρήστες εκτός οργανισμού , η δυνατότητα έκδοσης ψηφιακών πιστοποιητικών σε τρίτους και η διαδικασία ένταξης των ΑΠ σε λίστες που χρησιμοποιούν παγκοσμίως άλλες εφαρμογές για τον έλεγχο των τελικών πιστοποιητικών.

Βιβλιογραφία

[1] A. Menezes, S. Vanstone και D. Hankerson,, Guide to Elliptic Curve Cryptography, Springer-Verlag New York, Inc, 2004.

[2] Β. Κάτος και Γ. Στεφανίδης, «Τεχνικές Κρυπτογραφίας και Κρυπτανάλυσης,» Θεσσαλονίκη, ΖΥΓΟΣ, 2003, pp. 20-31.

[3] Y. Stamatiou, E. Konstantinou και C. Zaroliagis, «On the Construction of Prime Order,» p. 4, 2003.

[4] A. Menezes, P. Oorschot και S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996, p. 103.

[5] S. Basharat, M. Riaz και A. Khan, «Analysis of asymmetric cryptography in information security based on computational study to ensure confidentiality during information exchange,» 2018.

[6] A. Ayushi, «A Symmetric Key Cryptographic Algorithm,» 2010.

[7] N. Asaithambi, «A Study on Asymmetric Key Cryptography Algorithms,» p. 2, 2015.

[8] N. Koblitz, A. Menezes και A. Vanstone, «The State of Elliptic Curve Cryptography,» 2000.

[9] V. Miller, «Use of Elliptic Curves in Cryptography,» 1985.

[10] B. Esparham, M. Marwan και A. Abdulrahman, «A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention,» 2018.

[11] R. L. Rivest, «The RC5 Encryption Algorithm,» 1997.

[12] G. Singh και Supriya, «A Study of Encryption Algorithms (RSA, DES, 3DES and,» 2013.

[13] S. Charbathia και S. Sharma, «A Comparative Study of Rivest Cipher Algorithms,» pp. 2-6, 2014.

[14] Π. Παπαδημητράτος, «Ψηφιακές Υπογραφές,» pp. 4-11.

[15] U. European, «Πρόσβαση στο δίκαιο της Ευρωπαϊκής Ένωσης,» 2014. [Ηλεκτρονικό]. Available: https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32014R0910&qid=1661276703886.

[16] Enisa, «Electronic signatures,» 2014. [Ηλεκτρονικό]. Available: https://digital-strategy.ec.europa.eu/en/policies/esignatures.

[17] OpenPGP, 2020. [Ηλεκτρονικό]. Available: https://www.openpgp.org/about/.

[18] C. HSM, 2022. [Ηλεκτρονικό]. Available: https://cloud.google.com/kms/docs/hsm.

[19] Microsoft, «Basic Components of a Public Key Infrastructure,» 2012. [Ηλεκτρονικό]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc962020(v=technet.10).

[20] J. Forné, R. V. Páez και C. Satizábal, «PKI trust relationships: From a hybrid architecture to a hierarchical model,» 2006.

[21] Microsoft, «Network Trust Model,» 2010. [Ηλεκτρονικό]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc776987(v=ws.10).

[22] I. T. U. (ITU), «X.509 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks,» 2019. [Ηλεκτρονικό]. Available: https://www.itu.int/rec/T-REC-X.509.

[23] Ε. Δ. Έ. κ. Τ. Ε. Α.Ε., «Το πρότυπο X.509,» 2016. [Ηλεκτρονικό]. Available: https://pyxida.grnet.gr/mod/page/view.php?id=107.

[24] . S. Chokhani, . W. Ford, . R. Sabett και C. Merrill, «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,» 2003. [Ηλεκτρονικό]. Available: https://www.rfc-editor.org/rfc/rfc3647.

[25] E. Barker, «Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms,» 2014. [Ηλεκτρονικό]. Available: https://csrc.nist.gov/glossary/term/certification_practice_statement.

[26] A. L. G. f. A. Server, «Microsoft SQL Server Installation,» 2021. [Ηλεκτρονικό].

[27] L. ASCERTIA, «ADSS Server Installation Guide,» 2021.

[28] L. ASCERTIA , «Microsoft SQL Server Installation Guide for ADSS Server,» 2021.

[29] Microsoft, «Install a basic PKI certificate infrastructure,» 2016. [Ηλεκτρονικό]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj574179(v=ws.11).