ΠΑΝΕΠΙΣΤΗΜΙΟ ΣΤΕΡΕΑΣ ΕΛΛΑΔΑΣ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΙΑΤΡΙΚΗ

«ΣΧΕΔΙΑΣΜΟΣ & ΑΝΑΠΤΥΞΗ ΠΡΟΤΥΠΗΣ ΥΠΟΔΟΜΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ»

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΝΙΚΟΛΕΤΑ ΚΑΓΙΑ

ΠΒ0060

Επιβλέπων : Ράντος Κωνσταντίνος

Λαμία, Φεβρουάριος 2011

ΠΑΝΕΠΙΣΤΗΜΙΟ ΣΤΕΡΕΑΣ ΕΛΛΑΔΑΣ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΪΑΤΡΙΚΗ

Σχεδιασμός & Ανάπτυξη Πρότυπης Υποδομής Δημόσιου Κλειδιού

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΝΙΚΟΛΕΤΑ ΚΑΓΙΑ

ΠΒ0060

Επιβλέπων :
Ράντος Κωνσταντίνος

Λαμία, Φεβρουάριος 2011

Εκπονειθήσα πτυχιακή εργασία απαραίτητη για την κτήση του βασικού πτυχίου

Αφιερώνεται στο
Πανεπιστήμιο Στερεάς Ελλάδας
στο Τμήμα Πληροφορικής με εφαρμογές στη Βιοϊατρική

Περίληψη

Η παρούσα πτυχιακή εργασία αναλύει την έννοια και λειτουργία μιας **Υποδομής Δημόσιου Κλειδιού.** Μελετά τη σημασία της και την ανάγκη ύπαρξης μιας Υποδομής Δημόσιου Κλειδιού. Για το σκοπό αυτό περιγράφει μια σειρά μεθόδων, μηχανισμών, εργαλείων και τεχνολογιών τα οποία χρησιμοποιούνται σε μια Υποδομή Δημόσιου Κλειδιού. Η οργάνωση μιας υποδομής αποσκοπεί στην έκδοση και διαχείριση ψηφιακών πιστοποιητικών που παρέχονται στους χρήστες προκειμένου να εξασφαλίσει απαιτήσεις ασφάλειας, όπως η εμπιστευτικότητα, η αυθεντικοποίηση, ακεραιότητα δεδομένων και μη-αποποίησης στις διάφορες συναλλαγές τους. Παρουσιάζει με όσο το δυνατόν πιο απλό τρόπο τις έννοιες κρυπτογραφίας, ψηφιακής υπογραφής, ψηφιακά πιστοποιητικά, πρωτόκολλα επικοινωνίας και τους μηχανισμούς εφαρμογών τους περιορίζοντας αναφορές σε τεχνικές λεπτομέρειες στο βαθμό που αυτές είναι απαραίτητες για την κατανόηση του θέματος. Επίσης, περιγράφει τις οντότητες, καθώς και το ρόλο που διαδραματίζουν, οι οποίες απαρτίζουν μια Υποδομή Δημόσιου Κλειδιού. Τέλος, αναπτύσσεται μια πρότυπη Υπηρεσία Πιστοποίησης η οποία είναι το βασικό στοιχείο μιας Υποδομής Δημόσιου Κλειδιού που πιστοποιεί την ταυτότητα των εγγραφομένων συνδρομητών της ύστερα από αίτηση τους.

Λέξεις Κλειδιά:

Υποδομή Δημόσιου Κλειδιού
Κρυπτογραφία
Ιδωτικό/Δημόσιο κλειδί
Εμπιστευτικότητα
Ακεραιότητα
Διαθεσιμότητα
Αυθεντικοποίηση
Ψηφιακή Υπογραφή
Ψηφιακό Πιστοποιητικό
Ασφαλές Πρωτόκολλο Επικοινωνίας
Πρότυπο Υποδομής Δημόσιου Κλειδιού X.509
ΑρχήΠιστοποίησης
Έμπιστη Τρίτη Οντότητα
Αρχή Εγγραφής
Πολιτική Πιστοποίησης

Πίνακας Περιεχομένων

Πίνακας Σχημάτων

1 *Κεφάλαιο*

ΠΡΟΛΟΓΟΣ

Η διαρκής επιστημονική εξέλιξη της τεχνολογίας αναδεικνύει ολοένα και περισσότερο την εύκολη πρόσβαση στη γνώση και την πληροφορία. Ιδιαίτερα, με την αξιοποίηση του Διαδικτύου δίνεται η δυνατότητα διακίνησης δεδομένων και πραγματοποίησης μεγάλου όγκου συναλλαγών σε παγκόσμια κλίμακα. Παράλληλα, όμως ένας παράγοντας που δρα ανασταλτικά, κυρίως κατά τη διακίνηση προσωπικών και ευαίσθητων πληροφοριών,είναι οι κίνδυνοι που ελλοχεύουν με αποτέλεσμα να κλονίζεται η εμπιστοσύνη μεταξύ των χρηστών του Διαδικτύου. Οι κίνδυνοι αφορούν θέματα που περιλαμβάνουν την αυξανόμενη τάση υποκλοπής δεδομένων και επιθέσεων στο χώρο του Διαδικτύου. Στόχος της ασφάλειας ενός υπολογιστικού συστήματος (computer system security) είναι η διαφύλαξη των υπολογιστικών πόρων έναντι μη εξουσιοδοτημένης ή κακόβουλης χρήσης τους, καθώς επίσης και η προστασία των δεδομένων από κάθε ακούσια ή εκούσια απειλή, αποκάλυψη ή τροποποίηση τους. κατά τη διάρκεια της μετάδοσης στα δίκτυα υπολογιστών και τα κατανεμημένα συστήματα. Για την αποτελεσματική αντιμετώπιση των ζητημάτων αυτών, απαιτείται χάραξη στρατηγικών, υλοποίηση υπηρεσιών και μηχανισμών και η χρησιμοποίηση των κατάλληλων τεχνολογιών για τη δημιουργία ενός ολοκληρωμένου περιβάλλοντος ασφάλειας και εμπιστοσύνης κατά τη διάρκεια μιας επικοινωνίας.

1.1. Εισαγωγή

Με το πέρας του χρόνου έχει αναπτυχθεί ένα σύνολο πρωτοκόλλων και μηχανισμών που εξετάζει ζητήματα ασφάλειας πληροφοριών κατά τη μεταβίβαση τους ένα ευρύ δίκτυο. Ωστόσο η επιτακτική ανάγκη προστασίας των δεδομένων καθώς και η ασφαλής ηλεκτρονική επικοινωνία που επιτάσσουν οι ολοένα και αυξανόμενες ηλεκτρονικές συναλλαγές στο διαδίκτυο, οδήγησαν στην δημιουργία της Υποδομής Δημόσιου Κλειδιού και χρήση ψηφιακών πιστοποιητικών. Μια Υποδομή Δημοσίου Κλειδιού υπάρχει για να συμβάλλει στην ενίσχυση της εμπιστοσύνης των συμβαλλόμενων μερών (αυθεντικοποίηση) και να τους εξασφαλίσει ότι οι ιδιωτικές τους πληροφορίες μεταβιβάζονται με ασφάλεια στο διαδίκτυο (εμπιστευτικότητα). Για να επιτύχει τους στόχους της χρησιμοποιεί πολλά διαφορετικά εργαλεία και τεχνικές αλλά κυρίως στηρίζεται σε μια τεχνολογία, γνωστή ως κρυπτογραφία. Η Υποδομή Δημόσιου Κλειδιού θεωρείται πολύ σημαντικό στοιχείο για την δημιουργία ενός ασφαλούς δικτύου.

1.2. Δομή Εργασίας

Η δομή της παρούσας πτυχιακής εργασία έχει ως ακολούθως:

Το **Κεφάλαιο 1 –Πρόλογος-** παρουσιάζει μια προεσκόπιση του θέματος της εργασίας με σκοπό να προιδεάσει τον αναγνώστη.

Το **Κεφάλαιο 2 – Βασικά Ζητήματα Ασφάλειας** - αναφέρει τους όρους που χρησιμοποιούνται στην ασφάλεια πληροφοριακών συστημάτων, τα είδη των απειλών και επιθέσεων που δέχονται καθώς και οι απαιτήσεις ασφάλειας που θεωρούνται απαραίτητες για να είναι ένα σύστημα ασφαλές.

Το **Κεφάλαιο 3 - Κρυπτογραφία** – αναλύει τα μέσα που χρησιμοποιούνται για την ικανοποίηση απαιτήσεων που τέθηκαν για ασφαλή επικοινωνία. Περιγράφει τον τρόπο λειτουργίας των σημαντικότερων σχημάτων κρυπτογραφίας και αναλύει τις τεχνικές και τους μηχανισμούς που χρησιμοποιούν. Ιδιαίτερη προσοχή δίνεται στη κρυπτογραφία δημόσιου κλειδιού αφού αποτελεί βασικό στοιχείο μιας υποδομής δημόσιου κλειδιού.

Το **Κεφάλαιο 4 – Ψηφιακές Υπογραφές -** περιγράφει τι είναι μια ψηφιακή υπογραφή, περιέχει σχηματική και αναλυτική περιγραφή της δημιουργίας και επαλήθευσης υπογραφής**.** Αναφέρονται τα πρότυπα που ακολουθούν οι ψηφιακές υπογραφές καθώς και το νομικό πλαίσιο που ισχύει για τη χρήση τους. Τέλος τονίζεται η χρησιμότητα της και οι τρόποι χρήσης της από τον χρήστη.

Το **Κεφάλαιο 5 – Ψηφιακά Πιστοποιητικά** - ορίζει το ψηφιακό πιστοποιητικό, αναλύει τα περιεχόμενα του και τα πρότυπα που ακολουθούνται για τη δημιουργία του. Κατηγοριοποιεί τα πιστοποιητικά ανάλογα με τον τρόπο χρήσης τους και περιγράφει τη χρησιμότητα τους. Επιπρόσθετα παραθέτει χρήσιμα βήματα για τον χρήστη που διαθέτει στη κατοχή του ψηφιακό πιστοποιητικό.

Το **Κεφάλαιο 6 - Ασφαλές Πρωτόκολλο Επικοινωνίας SSL** – περιγράφει τη θέση του πρωτοκόλλου ασφαλείας και αναλυτικότερα τον τρόπο λειτουργίας του και τη χρησιμότητα του στις επικοινωνίες – συναλλαγές. Αναφέρει επιγραμματικά τα πλεονεκτήματα και τα μειονεκτήματα κατά τη χρήση του και τέλος παρουσιάζεται μια τυπική διαδικασία αίτησης και παραλαβής πιστοποιητικού SSL.

Το **Κεφάλαιο 7 – Υποδομή Δημόσιου Κλειδιού -** αναλύει διεξοδικά μια Υποδομή Δημόσιου κλειδιού δίνοντας τον ορισμό και τα μέρη από τα οποία απαρτίζεται. Περιγράφει τη λειτουργία της αναλυτικά και σχηματικά. Αναφέρει εκτενώς τις παροχές και τα πλεονεκτήματα της Τέλος παρουσιάζει τα είδη των αρχιτεκτονικών που μπορεί να ακολουθήσει μια Υποδομή Δημόσιου Κλειδιού καθώς και κριτήρια για την επιλογή αρχιτεκτονικής.

Το **Κεφάλαιο 8 - Αρχές Πιστοποίησης και Εγγραφής -** επεξηγεί το ρόλο και τις παροχές που έχουν οι δύο πιο σημαντικές συνιστώσες μιας Υποδομής Δημόσιου Κλειδιού. Περιγράφεται ο τρόπος λειτουργίας αλλά και συνεργασίας μεταξύ τους. Τέλος, δίνει μια μικρή αναφορά στο νομικό πλαίσιο που κινούνται.

Το **Κεφάλαιο 9 - Διαδικασίες Εγγραφής-Έκδοσης και Διαχείρισης Πιστοποιητικών –** εξηγεί λεπτομερώς τις διαδικασίες που απαιτούνται για την εγγραφή και έκδοση ενός ψηφιακού πιστοποιητικού στο όνομα ενός χρήστη ή μιας υπηρεσίας. Τονίζει τις υποχρεώσεις των αρχών που τις εκτελούν αλλά και του χρήστη. Επιπλέον περιγράφει τις διαδικασίες ανάκλησης, ανανέωσης και αναζήτησης ενός ψηφιακού πιστοποιητικού οι οποίες είναι απαραίτητες για την ομαλή και σωστή λειτουργία μιας Υποδομής Δημόσιου Κλειδιού.

Το **Κεφάλαιο 10 - Πρότυπη Πολιτική Πιστοποίησης** - αναφέρει ένα πρότυπο σύνολο των κανόνων και διαδικασιών με βάση τα δεδομένα του Πανεπιστημίου Στερεάς Ελλάδας για τη λειτουργία μιας πρότυπης Υποδομή Δημόσιου Κλειδιού. Ακολουθεί το πρότυπο Πολιτικής Πιστοποίησης RFC3647 και πολλά σημεία είναι προτεινόμενα για μελλοντική ανάπτυξη μιας Υποδομής Δημόσιου Κλειδιού για τις ανάγκες του τμήματος.

Το **Κεφάλαιο 11 – Βήματα Υλοποίησης** – Αναφέρει το λογισμικό υλικό που χρησιμοποιήθηκε για τη υλοποίηση μιας Υπηρεσίας Πιστοποίησης σε λειτουργικό σύστημα Linux.

Το **Κεφάλαιο 12 – Αποτελέσματα-Οδηγίες Χρήσης** – Παρουσιάζει ένα παραδείγμα δημιουργίας πιστοποιητικού για την Υπηρεσία Πιστοποίησης (CA) και ένα παράδειγμα δημιουργίας

και υπογραφής πιστοποιητικού για τον χρήστη. Το κεφάλαιο αυτό παρουσιάζει τα αποτελέσματα από την προσπάθεια υλοποίησης μιας Υπηρεσίας Πιστοποίησης και συμβάλλει στη κατανόηση του τρόπου διαχείρισης της.

Το **Κεφάλαιο 13 – Επίλογος** – παρουσιάζει μια σύνοψη του θέματος της παρούσας εργασίας και προτείνει ορισμένες μελλοντικές επεκτάσεις.

2 *Κεφάλαιο*

ΒΑΣΙΚΑ ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

Η ασφάλεια ενός Πληροφοριακού Συστήματος αναφέρεται στη προστασία των πληροφοριών και πόρων από ενδεχόμενες αλλοιώσεις και καταστροφές. Για να θεωρηθεί ένα Π.Σ. ασφαλές θα πρέπει να παρέχει σωστές και αξιόπιστες πληροφορίες. Για την επίτευξη αυτού του στόχου, απαιτείται να ληφθούν ορισμένα μέτρα για την εξασφάλιση σημαντικών παραμέτρων ασφάλειας, κατά την επικοινωνία, όπως είναι η εμπιστευτικότητα, η ακεραιότητα, η μη αποποίηση και η διαθεσιμότητα

2.1. Ορολογία

Στο γνωστικό πεδίο της ασφάλειας συναντώνται συχνά οι εξής όροι παραβίασης ασφάλειας:

- **Αδυναμία (Vulnerability):** Είναι κάποια σχεδιαστική ατέλεια κατά την υλοποίηση ενός πληροφοριακού συστήματος ή μιας υπηρεσίας η οποία μπορεί να εντοπιστεί από έναν δυνητικά επιτιθέμενο και να την εκμεταλλευτεί με σκοπό την παραβίαση ενός συστήματος ασφάλειας και την απόκτηση πρόσβασης σε πληροφορίες και πόρους.
- **Απειλή (Treat):** Είναι οτιδήποτε μπορεί να προκαλέσει τυχαία ή από πρόθεση τη παραβίαση της ασφάλειας ενός συστήματος με αποτέλεσμα τη μετατροπή ή καταστροφή δεδομένων αλλά και ζημιά στους πόρους. Ένα παράδειγμα απειλής είναι οι ηλεκρονικοί ιοί. Ένας ιός είναι ένας

κώδικας που παρασιτεί σε κάποιο πρόγραμμα ή αρχείο και έχει ως σκοπό την καταστροφή δεδομένων.

- **Επίθεση (Attack):** Είναι η προσπάθεια από έναν κακόβουλο χρήστη να πραγματοποιήσει μια απειλή εκμεταλλευόμενος μια πιθανή αδυναμία σε ένα σύστημα. Οι επιθέσεις μπορεί να προέρχονται είτε από ενεργούς (active) επιτιθέμενους, οι οποίοι έχουν στόχο να προκαλέσουν φθορές και να εξαπατήσουν είτε από μη ενεργούς ή αλλιώς παθητικούς (passive) επιτιθέμενους οι οποίοι στοχεύουν στην παρακολούθηση δεδομένων που μεταδίδονται κατά τη διάρκεια μιας επικοινωνίας χωρίς να τα τροποποιήσουν.
- **Αντίμετρα (Countermeasures):** Είναι τα μέτρα που λαμβάνονται και οι μηχανισμοί που αναπτύσσονται με σκοπό την πρόληψη, την ανίχνευση και την αντιμετώπιση των αποτελεσμάτων μιας απειλής, έτσι ώστε το σύστημα να ανακάμψει έγκαιρα και να θεωρηθεί και πάλι αξιόπιστο. Χαρακτηριστικό παράδειγμα είναι η χρήση της κρυπτογραφίας κατά τη πραγματοποίηση συναλλαγών με σκοπό τη προστασία της ακεραιότητας και τη διαφύλαξη της μυστικότητας των δεδομένων που μεταβιβάζονται**[2]**.

2.1.1. Κατηγορίες απειλών

Αρχικά οι απειλές θα μπορούσαμε να τις διακρίνουμε σε τρείς πιο ευρύτερες κατηγορίες που αποτελούν καταστάσεις όπου θα μπορούσαν να πραγματοποιηθούν απώλειες ή ζημιές σε πόρους του δικτύου:

- **Φυσικές:** Οι απειλές από φυσικούς παράγοντες (φωτιά, πλημμύρα, κλπ.)
- **Ακούσιες:** Οι απειλές που προκαλούνται είτε από άγνοια ή αμέλεια ανθρώπινου παράγοντα είτε από σχεδιαστική ατέλεια υλικού ή λογισμικού.
- **Εκούσιες:** Οι απειλές από είσοδο κακόβουλων –μη εξουσιοδοτημένων χρηστών στο εσωτερικό ενός συστήματος και επιχειρούν κάποιο είδος επίθεσης.

Επίσης, αξίζει να αναφερθεί ότι οι απειλές μπορούν να χαρακτηριστούν ως ενεργές (active) ή παθητικές (passive) ανάλογα με το το σκοπό και το είδος της επίθεσης που πραγματοποιείται. Ενεργές καλούνται οι απειλές που πραγματοποιούνται με σκοπό τη μεταβολή των δεδομένων ή τη πρόκληση ζημιάς στο σύστημα. Ένας επιτιθέμενος ενδεικτικά μπορεί να προσποιηθεί τον αποστολέα ή παραλήπτη δεδομένων ή ακόμη να δημιουργήσει κατάσταση άρνησης παροχής κάποιας υπηρεσίας του συστήματος. Παθητικές θεωρούνται οι απειλές που έχουν ως στόχο την αποκάλυψη του περιεχομένου των μηνυμάτων που ανταλλάσσονται μεταξύ εξουσιοδοτημένων χρηστών αλλά χωρίς να προκάλουν καμία αλλαγή στη λειτουργία ενός συστήματος.

2.1.2. Κατηγορίες επιθέσεων

Όπως προαναφέρθηκε παραπάνω επίθεση η πραγματοποίηση μιας απειλής εκμεταλλευόμενος κάποια αδυναμία του συστήματος. Οι σημαντικότεροι τύποι επιθέσεων περιλαμβάνουν:

- **Προσποίηση (Masquerade):** Στη περίπτωση αυτή ο επιτιθέμενος ο οποίος δεν είναι εξουσιοδοτημένος χρήστης επιδιώκει να αποκτήσει πρόσβαση σε πόρους και πληροφορίες, προσποιούμενος την ταυτότητα κάποιου άλλου. Ένα απλό παράδειγμα είναι η υποκλοπής κάποιου σμυστικού κωδικού που χρησιμοποιείται σε μια συναλλαγή.
- **Παθητική παρακολούθηση (Passive tapping):** Σε αυτού του είδους την επίθεση, ο επιτιθέμενος δεν επιφέρει αλλαγές ούτε στα δεδομένα ούτε στην κατάσταση του συστήματος αλλά έχει ως στόχο την αποκάλυψη των πληροφοριών που εμπεριέχονται σε μηνύματα που μεταδίδονται μέσω ενός δικτύου παρακολουθώντας την κίνηση και το είδος των δεδομένων που διακινούνται.
- **Ενεργός παρακολούθηση (Active tapping):** Σε αυτή την περίπτωση περιλαμβάνεται η παρακολούθηση των δεδομένα που μεταδίδονται αλλά και η τροποποίηση ή καταστροφή τους. Σε αντίθεση με τη προηγούμενη επίθεση η ενεργός παρακολούθηση θεωρείται εύλογα μεγαλύτερη απειλή αλλά γίνεται ευκολότερα αντιληπτή έτσι ώστε να ληφθούν τα κατάλληλα μέτρα.
- **Αποποίηση (Repudiation):** Οι επιθέσεις τέτοιου είδους γίνονται κυρίως προς το σύστημα διαχείρισης και αφορά την αποποίηση συμμετοχής κάποιας οντότητας σε μια συναλλαγή. Παράδειγμα ένας χρήστης μπορεί να πραγματοποιήσει αποστολή δεδομένων προς κάποιον άλλο χρήστη και στη συνέχεια να αρνηθεί ότι εκτέλεσε την αποστολή.
- **Άρνηση Παροχής Υπηρεσίας (Denial of service):** Σε αυτή την περίπτωση έγκειται η χρησιμοποίηση μια υπηρεσίας χωρίς σκοπό με αποτέλεσμα η υπηρεσία να μην είναι προσβάσιμη από άλλους χρήστες. Συνεπώς αποτυγχάνει ένα δίκτυο να λειτουργεί ομαλά όπως για παράδειγμα καθυστέρηση κατά την εξυπηρέτηση ακόμη και άρνηση παροχής μιας υπηρεσίας σε κάποιο εξουσιοδοτημένο χρήστη.
- **Επανεκπομπή μηνυμάτων (Replay):** Αυτού του είδους η επίθεση ανήκει στις ενεργές απειλές καθώς ο επιτιθέμενος παρακολουθεί τα μηνύματα που μεταδίδονται αποκτά πρόσβαση στα δεδομένα που περιέχουν, τα αλλάζει και στη συνέχεια τα αποστέλλει στον παραλήπτη σε διαφορετικούς χρόνους. Επομένως σε αυτή τη περίπτωση συμπεριλαμβάνεται και η προσποίηση του επιτιθέμενου ως αποστολέας των μηνυμάτων καθώς επίσης και το είδος της επίθεσης άρνησης παροχής υπηρεσιών.

- **Ανάλυση Κίνησης (Traffic analysis):** Σε αυτού του είδους η επίθεση είναι τύπου παθητικής απειλής καθώς τα δεδομένα δεν υφίστανται καμία τροποποίηση. Ωστόσο παρακολουθείται η συχνότητα, η ποσότητα και των δεδομένων που διακινούνται κατά τη μετάδοση μηνυμάτων μεταξύ των συμβαλλόμενων μερών σε μια επικοινωνία με στόχο να εξαγάγει συμπεράσματα σχετικά με τη πληροφορία που διακινείται και στη συνέχεια να την αποκαλύψει.
- **Κακόβουλο Λογισμικό (Viruses,Trojan horses,worms):** Τα κακόβουλα λογισμικά έχουν σκοπό είτε την καταστροφή είτε τη παρακολούθηση των κινήσεων μεμονωμένου υπολογιστή ή ακόμη και ενός δικτύου. Για παράδειγμα ένας δούρειος ίππος είναι δυνατόν, αφού εισβάλλει στον υπολογιστή κρυμμένος; μέσα σε ένα άλλο πρόγραμμα να καταστρέφει αλλά κυρίως να παρακολουθεί κάθε κίνηση και την αναφέρει στον δημιουργό του.

2.2. Βασικές απαιτήσεις ασφάλειας

Έχοντας αναλύσει παραπάνω τους ορισμούς των απειλών και επιθέσεων σε περιπτώσεις συναλλαγών και διακίνησης δεδομένων σε ένα κατανεμημένο υπολογιστικό σύστημα είναι προφανές ότι ανακύπτουν σημαντικά ζητήματα ασφάλειας. Για αυτό το λόγο έχουν τεθεί ορισμένοι παράμετροι και απαιτήσεις ασφάλειας προκειμένου να διασφαλιστούν οι συναλλάγες που πραγματοποιούνται μεταξύ των χρηστών ενός δικτύου. Οι σημαντικότερες απαιτήσεις ασφάλειας αναφέρονται και αναλύονται παρακάτω:

⇒ **Εμπιστευτικότητα/Μυστικότητα(Confidentiality/Privacy)**: Μη αποκάλυψη των πληροφοριών που μεταδίδονται σε μη εξουσιοδοτημένους χρήστες. Το ζήτημα της εμπιστευτικότητας είναι μείζονος σημασίας καθώς έχει να κάνει με την προστασία της προσωπικής και ευαίσθητης πληροφορίας. Η προστασίας της πληροφορίας κρίνεται ως επιτακτική ανάγκη σε επίπεδο νομικό,οικονομικό αλλά και ακαδημαικό. Απαιτείται η εξασφάλιση του απορρήτου κατά τη διάρκεια μιας ηλεκτρονικής συνναλλαγής ειδικότερα όταν τα δεδομένα που ανταλλάσσονται περιέχουν ευαίσθητα στοιχεία όπως οικονομικά ή ιατρικά δεδομένα αλλά και για τη διαφύλαξη πνευματικών δικαιωμάτων. Επομένως, πρέπει να καθοριστούν σωστά και προσεκτικά οι διαδικασίες για τη διασφάλιση της εμπιστευτικότητας. Η εμπιστευτικότητα εξασφαλίζεται κυρίως με τη χρήση κωδικών και με την κρυπτογράφηση των δεδομένων που μεταδίδονται. Επίσης, κρίσιμο σημείο αποτελεί ο προσδιορισμός και η κατοχύρωση των χρηστών.

⇒ **Ακεραιότητα (Integrity)**: Η εξασφάλιση μη τροποποίησης των δεδομένων κατά τη μετάδοση μετά τη δημιουργία τους. και αποτροπή κάθε κακόβουλης ενέργειας από μη εξουσιοδοτημένους χρήστες. Τα δεδομένα που μεταδίδονται θα πρέπει να προστατεύονται επαρκώς έτσι ώστε να παραδίδονται στον παραλήπτη ακέραια και πλήρη. Η ακεραιότητα διασφαλίζεται με τη χρήση των ψηφιακών υπογραφών οι οποίες αναλύονται παρακάτω στο κεφάλαιο 4. Επίσης

σημαντικό ρόλο για τη διατήρηση της ακεραιότητας των δεδομένων διαδραματίζει η χάραξη μια πολιτικής για τον έλεγχο και προσδιορισμό των χρηστών που έχουν πρόσβαση στα δεδομένα.

⇒ **Αυθεντικοποίηση (Authentication):** Η εξακρίβωση της ταυτότητας των επικοινωνούντων μερών. Ο αποστολέας θα πρέπει να είναι σίγουρος ότι η πληροφορία που μετέδωσε πήγε στον σωστό προορισμό και αντίστοιχα ο παραλήπτης ότι η πηγή από την οποία έλαβε μια πληροφορία είναι έγκυρη. Έτσι ώστε να αποτραπεί ο κίνδυνος προσποίησης από μη κάποιον άλλον χρήστη. Βασικό ρόλο στην αυθεντικοποίηση της ταυτότητας των εξουσιοδοτημένων χρηστών διαδραματίζει το ψηφιακό πιστοποιητικό για το οποίο θα γίνει εκτενής ανάλυση στα παρακάτω κεφάλαια.

⇒ **Μη-αποποίηση (non-repudiation):** Δημιουργούνται συνθήκες όπου αποτρέπονται οι περιπτώσεις άρνησης εκτέλεσης μιας ενέργειας. Ο αποστολέας ενός μηνύματος δεν μπορεί να αρνηθεί τη δημιουργία και αποστολή του στον παραλήπτη όπως επίσης και ο τελευταίος δεν μπορεί να ισχυριστεί τη μη λήψη του μηνύματος.

⇒ **Διαθεσιμότητα (Availability):** Η διαβεβαίωση ότι όλοι οι εξουσιοδοτημένοι χρήστες μπορούν να πρόσβαση σε μία υπηρεσία ενός Πληροφοριακού Συστήματος όποτε το απαιτήσουν χωρίς αδικαιολόγητη κωλλυσιεργία. Παρέχεται προστασία από επιθέσεις πλήρης άρνησης υπηρεσιών (Denial of service) από μη εξουσιοδοτημένους χρήστες οι οποίοι καθιστούν το σύστημα ή μια υπηρεσία ακατάλληλο προς χρήση. Επιπλέον για την εξασφάλιση της διαθεσιμότητας λαμβάνονται υπόψη και άλλοι παράγοντες όπως φυσικές απειλές και τεχνικά ζητήματα. Επομένως είναι προφανές ότι απαιτείται σωστή λήψη μέτρων για κάθε πιθανή αιτία που μπορεί να επιφέρει τη μη διαθεσιμότητας ενός συστήματος**[3]**.

3 *Κεφάλαιο*

ΚΡΥΠΤΟΓΡΑΦΙΑ

Στο προηγούμενο κεφάλαιο εξετάσαμε διάφορα είδη απειλών που μπορεί να αντιμετωπίσει ένας υπολογιστής συνδεδεμένος σε ένα δίκτυο και τις βασικότερες απαιτήσεις που πρέπει να ικανοποιούνται προκειμένου να χαρακτηριστεί ένα σύστημα ασφαλές. Στον παρόν κεφάλαιο θα εξεταστεί η κύρια τεχνολογία η οποία μας παρέχει πολλά εργαλεία, συμβάλλοντας στην ενίσχυση της άμυνας ενός συστήματος από τους δυνητικά επιτιθέμενους. Η τεχνολογία στην οποία θα αναφερθούμε και θα αναλύσουμε είναι η **Κρυπτογραφία**.

Ο κυριότερος σκοπός της κρυπτογραφίας είναι να αναπτύξει και να παράχει μηχανισμούς που εξασφαλίζουν τη μετατροπή της πληροφορίας που μεταδίδεται από την αρχική της μορφή σε μια μορφή η οποία δεν είναι ευανάγνωστη από μη εξουσιοδοτημένα πρόσωπα με τη προυπόθεση πως η αντίστροφη διαδικασία δηλαδη η επαναφορά της αρχικής πληροφορίας να είναι εφικτή με απώτερο στόχο να διασφαλίσει την εμπιστευτικότητα την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών, το τρίπτυχο που προσδιορίζει τα χαρακτηριστικά της ασφάλειας πληροφοριών. Η κρυπτογράφηση και η αποκρυπτογράφηση είναι τα βασικές τεχωικές που χρησιμοποιούνται σε ένα σύστημα κρυπτογραφίας. Όταν ένα στοιχείο/μήνυμα δημιουργείται από το χρήστη και μεταδίδεται μέσα από ένα δίκτυο είναι απροστάτευτο από πιθανές επιθέσεις όπως αποκάλυψη και μετατροπή του. Έτσι ο δημιουργός του στοιχείου/μηνύματος προτού το μεταδώσει καλείται να το κρυπτογραφήσει δηλαδή να το σχηματίσει σε μια μορφή η οποία δεν θα αναγνωρίζεται εύκολα. Η μορφή που προκύπτει μετα την κρυπτογράφηση ονομάζεται κρυπτογράφημα. Στη συνέχεια ο

αποδέκτης του κρυτογραφήματος αναλαμβάνει να εκτελέσει τη διαδικασία της αποκρυπτογράφησης προκειμένου να μπορέσει να αναγνώσει το στοιχείο/μήνυμα. Επομένως η χρησιμοποίηση της κρυπτογράφησης και της αποκρυπτογράφησης εξασφαλίζει ότι όταν διαβιβάζει κάποιος μια ευαίσθητη πληροφορία μέσω του Διαδικτύου, το αρχικό μήνυμα ή τα στοιχεία δεν θα αναγνωριστούν.

Η λέξη **κρυπτογραφία** προέρχεται από τα συνθετικά "κρυπτός" και "γράφω" και η χρήση της συναντάται και σε παλαιότερες μορφές βασιζόμενη κυρίως στην επεξεργασία της γλωσσικής δομής της πληροφορίας. Οι τεχνικές που είχαν αναπτυχθεί είναι η αντικατάσταση και η αντιμετάθεση οι οποίες και αποτελούν τη βάση για τη μετέπειτα ανάπτυξη των μεθόδων της νεότερης κρυπτογραφίας. Η αντικατάσταση γίνεται, όπως δηλώνει και το όνομα της, αντικαθιστώντας τμήματα συγκεκριμένου μήκους του αρχικού κειμένου με άλλα ακολουθώντας κάποιο βασικό κώδικα, ο οποίος παραμένει κρυφός, με αποτέλεσμα να παραχθεί ένα κείμενο του οποίου η μορφή είναι δυσνόητη.

*Ένα χαρακτηριστικό παράδειγμα ενός αλγορίθμου αντικατάστασης είναι ο αλγόριθμος του Καίσαρα (**Caesar's Cipher**). Ο αλγόριθμος αντικαθιστά ένα τμήμα πληροφορίας με κάποιο άλλο τμήμα. Αυτό συναντάτε συχνά με τη μετατόπιση γραμμάτων της αλφαβήτου σε ένα κείμενο.Το κλειδί του αλγορίθμου θεωρείται ο αριθμός των χαρακτήρων που θα μετατοπίσει. Ένα απλό παράδειγμα του αλγόριθμου του Καίσαρα παρατίθεται αμέσως παρακάτω:*

Έστω, ότι θέλουμε να κρυπτογραφήσουμε τη αγγλική λέξη "SECRET" χρησιμοποιώντας κλειδί μήκους 3, μετατοπίζουμε το αγγλικό αλφάβητο κατά τρία γράμματα έτσι ώστε να ξεκινάει το αλφάβητο με το γράμμα (D).

Αγγλικό αλφάβητο:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Μετατοπίζοντας τα παραπάνω κατά τρία παίρνεις:

DEFGHIJKLMNOPQRSTUVWXYZABC

Όπου D=A, E=B, F=C, και συνεχίζεται.Το κρυπτογραφημένο κείμενο του αρχικού "SECRET" είναι το " VHFUHW".

Για να καταφέρει κάποιος να διαβάσει το κρυπτογράφημα θα πρέπει να γνωρίζει ότι το κλειδί είναι τρία. Ωστόσο, είναι φανερό, ότι με τα σημερινά δεδομένα ένας τέτοιος αλγόριθμος είναι αρκετά αδύναμος και ευάλωτος σε πιθανές επιθέσεις **[Phil Zimmermann,1,13]**.

Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών, όπως διακριτά μαθηματικά, θεωρία αριθμών,

θεωρία πληροφορίας, υπολογιστική πολυπλοκότητα, στατιστική και συνδυαστική ανάλυση**[Κύτταρο, Περιοδικό Επιστήμης και Τεχνολογίας, 2010, αρθρο:Κρυπτογραφία][46].** Βασικός στόχος είναι η δημιουργία ισχυρών μαθηματικών αλγόριθμων οι οποίοι να δέχονται ως είσοδο ένα αρχικό μήνυμα και το κλειδί, το οποίο είναι μία συμβολοσειρά πεπερασμένου μήκους, και αποτελεί βασική του παράμετρο, ώστε να δίνει στην έξοδο ένα τροποποιημένο μήνυμα. Στην αποκρυπτογράφηση αντίστροφα χρησιμοποιείται ο αλγόριθμος αποκρυπτογράφησης ο οποίος δέχεται ως είσοδο ένα κρυπτογραφημένο μήνυμα και το κλειδί δίνοντας στην έξοδο το αρχικό μήνυμα. Σχεδόν πάντα οι αλγόριθμοι που χρησιμοποιούται είναι γνωστοί επομένως η κρυπτογράφηση ενός μηνύματος βασίζεται στη μέγεθος και τη διατήρηση της μυστικότητας του κλειδιού που γίνεται χρήση. Αξίζει στο σημείο αυτό να σημειωθεί ότι το σύστημα της κρυπτογραφίας είναι ο ακρογωνιαίος λίθος επάνω στον οποίο δομείται μια υποδομή δημοσίου κλειδιού.

Ιστορικά…

*Κατά τη διάρκεια του εικοστού αιώνα κατασκευάστηκαν αρκετές μηχανικές συσκευές που έκαναν αυτόματα αντικατάσταση, πιο διάσημη από τις οποίες ήταν πιθανότατα η συσκευή Enigma που χρησιμοποιήθηκε από τους Γερμανούς κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου για την αποστολή μυστικών μηνυμάτων στα στρατεύματα τους. Ο κώδικας του έσπασε από τους συμμάχους, ωστόσο οι Γερμανοί δεν ήξεραν ότι τα μυστικά τους αποκρυπτογραφούνταν και αυτό συντέλεσε σύμφωνα με τους ιστορικούς στην τελική τους ήττα***[36]**.

3.1. Ορολογία

Για την πληρέστερη κατανόηση των συστημάτων της κρυπτογραφίας δίνονται παρακάτω οι ορισμοί των βασικών και πιο συχνά χρησιμοποιούμενων όρων στην κρυπτογραφία:

Κρυπτογράφηση (encryption) ονομάζεται η διαδικασία που πραγματοποιείται για τη μετατροπή ενός μηνύματος σε μία δυσνόητη μορφή κάνοντας χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην είναι αναγνώσιμο από κανέναν εκτός του νόμιμου παραλήπτη.

Αποκρυπτογράφηση (decryption) ονομάζεται η αντίστροφη διαδικασία όπου ο παραλήπτης πραγματοποεί στο κρυπτογράφημα για να παράγει το αρχικό μήνυμα.

Κρυπτογραφικός αλγόριθμος (cipher) είναιη μέθοδος με την οποία μετασχηματίζονται τα δεδομένα σε μία δυσνόητη μορφή ώστε να μην αποκαλύπτεται η αρχική τους μορφή από μη εξουσιοδοτημένα μέρη. Συνήθως αλγόριθμος κρυπτογράφησης είναι μία πολύπλοκη μαθηματική συνάρτηση.

Αρχικό κείμενο (plaintext) είναι το περιεχόμενο του μηνύματος που παράγει ο αποστολέας και το οποίο και επιθυμεί να διατηρηθεί μυστικό. Έτσι εισάγει τα δεδομένα στον αλγόριθμο κρυπτογράφησης έτσι ώστε να παραχθεί το μετασχηματισμένο μήνυμα το οποίο δεν θα μπορεί να αναγνωστεί από μη εξουσιοδοτημένους χρήστες.

Κλειδί (key) είναι ένα σύνολο στοιχείων πεπερασμένου μεγέθους που δέχεται ως παράμετρο μαζί με το αρχικό κείμενο η συνάρτηση κρυπτογράφησης. Εάν χρησιμοποιηθούν διαφορετικά κλειδιά για τη κρυπτογράφηση του ίδιου κειμένου θα παραχθούν διαφορετικά κρυπτοκείμενα. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits και μεταβάλλεται ανάλογα με τον αλγόριθμο κρυπτογράφησης.

Κρυπτογραφημένο κείμενο/κρυπτοκείμενο (ciphertext) είναι το αποτέλεσμα που λαμβάνεται με την εφαρμογή ενός κρυπτογραφικού αλγόριθμου και τη χρήση κλειδιού στο αρχικό κείμενο.

Κρυπτανάλυση (cryptanalysis) είναι η μελέτη που ασχολείται με την ανάλυση κάποιας τεχνικής κρυπτογράφησης ή μέσω του «σπάσιμου» ενός αλγόριθμου προκειμένου να κατανοήσει το αρχικό μήνυμα μη έχοντας γνώση του κλειδιού που χρησιμοποιήθηκε για να πραγματοποιηθεί η κρυπτογράφηση. Υπάρχουν διάφοροι τύποι κρυπταναλυτικών επιθέσεων οι οποίοι αναφέρονται παρακάτω με την ανάλυση των αλγορίθμων. Σήμερα, ισχύει ότι οι αλγόριθμοι είναι γνωστοί στο ευρύ κοινό και η μόνη πληροφορία που απαιτείται να παραμείνει μυστική είναι το κλειδί κρυπτογράφησης. Επομένως, η εμπιστευτικότητα της μεταδιδόμενης πληροφορίας εξαρτάται πλέον από το μέγεθος του κλειδιού και στην απαίτηση να διατηρείται μυστικό

3.2. Τυπικό σύστημα κρυπτογράφησης - αποκρυπτογράφησης.

Μέσω της κρυπτογραφίας οι εξουσιοδοτημένοι χρήστες (π.χ χρήστης Α και χρήστης Β) έχουν τη δυνατότητα να επικοινωνήσουν με ασφάλεια ακόμη και μέσα από ένα κανάλι που θεωρείται μη ασφαλές. Κύριος σκοπός είναι ένα μη εξουσιοδοτημένο πρόσωπο (π.χ χρήστης Γ) να μην μπορεί να παρεμβληθεί στην επικοινωνία ή να αποκαλύψει το περιεχόμενο των μηνυμάτων που μεταδίδονται.

Οι ενέργειες που εκτελούνται κατά τη κρυπτογράφηση και αποκρυπτογράφηση χαρακτηρίζονται από πέντε μεταβλητές (**M,C,k,E,D**):

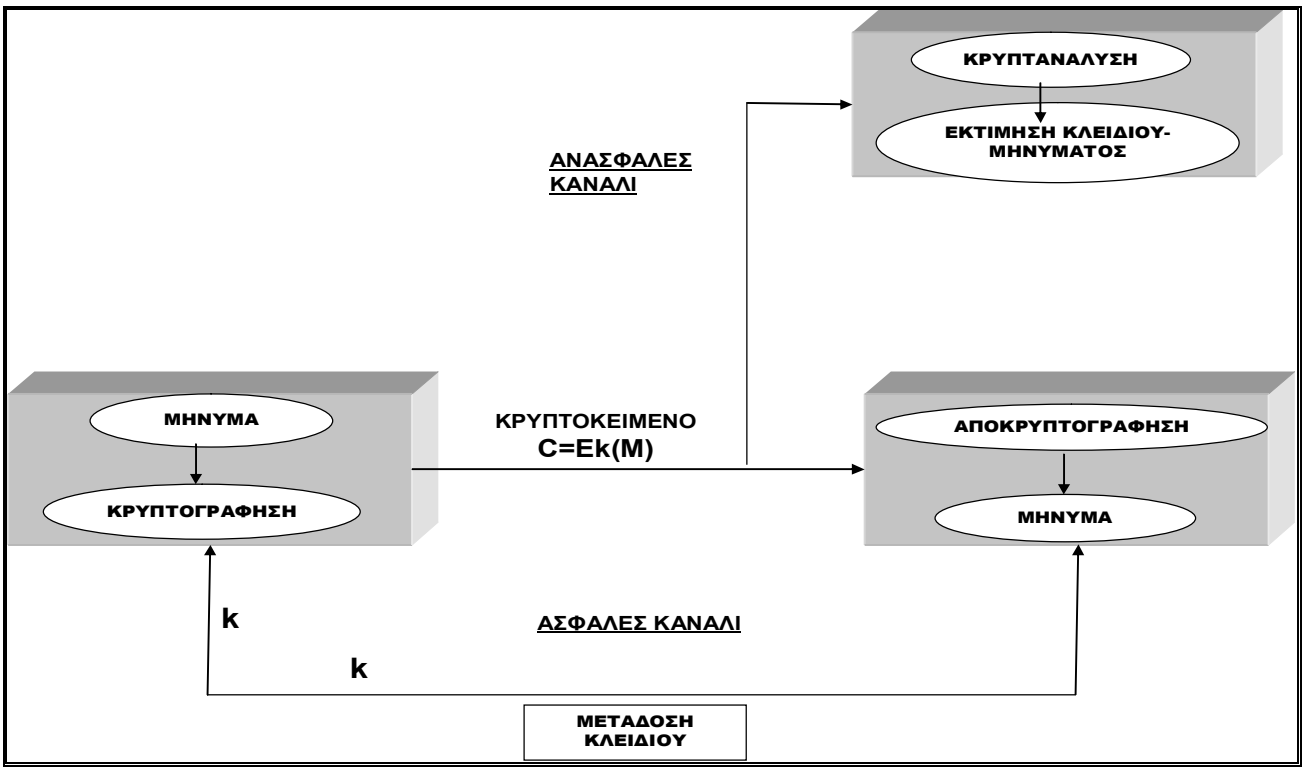
- Το **M** (**Message**) συμβολίζει το μεταδιδόμενο μήνυμα στην αρχική του μορφή.
- Το **C** (**Ciphertext**) συμβολίζει το κρυπτογραφημένο μήνυμα ή αλλιώς κρυπτοκείμενο.
- Το **k** (**key**) συμβολίζει το κλειδί που χρησιμοποιείται κατά τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης.
- Το **E** (**Encryption**) συμβολίζει τη διαδικασία κρυπτογράφησης ή κρυπτογραφικό μετασχηματισμό.
- Το **D** (**Decryption**) συμβολίζει την αντίστροφη διαδικασία ή μετασχηματισμό αποκρυπτογράφηση

Η συνάρτηση κρυπτογράφησης **C=Ek(M)** δέχεται δύο παραμέτρους, το μήνυμα **M** στην αρχική του μορφή και το κλειδί **k** και παράγει το κρυπτοκείμενο **C**. Η συνάρτηση αποκρυπτογράφησης **M=Dk(C**) δέχεται δυο παραμέτρους, το κρυπτοκείμενο **C** και το κλειδί **k** και παράγει το μήνυμα **M** στην αρχική του μορφή.

Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης που απεικονίζεται στη παρακάτω **Εικόνα 1** λειτουργεί με τον ακόλουθο τρόπο:

1. Ο χρήστης Α ως αποστολέας επιλέγει ένα κλειδί (**k)** το οποίο θα χρησιμοποιήσει για να κρυπτογραφήσει το μήνυμα και το αποστέλλει στον χρήστη Β μέσα από ένα ασφαλές κανάλι.
2. Στη συνέχεια ο χρήστης Α δημιουργεί ένα μήνυμα, το κρυπτογραφεί εφαρμόζοντας τη συνάρτηση κρυπτογράφησης **C=Ek(M)**, χρησιμοποιώντας το κλειδί (**k)** που επέλεξε.
3. Ο χρήστης Α αποστέλλει το αποτέλεσμα της συνάρτησης (κρυπτοκείμενο) στον χρήστη Β μέσω ενός μη ασφαλούς καναλιού.
4. Ο παραλήπτης του κρυπτοκειμένου χρήστης Β αποκρυπτογραφεί το κρυπτοκείμενο εφαρμόζοντας τη συνάρτηση **M=Dk(C**), χρησιμοποιώντας το κλειδί (**k)** που έλαβε από τον Α μέσω τους ασφαλούς καναλιού, για να ανακτήσει το μήνυμα στην αρχική του μορφή.
5. Ένας τρίτος χρήστης Γ παρακολουθεί την επικοινωνία και ενημερώνεται για τα μηνύματα που μεταδίδονται μέσω του ανασφαλούς καναλιού αλλά δεν έχει γνώση για το κλειδί που χρησιμοποιήθηκε. Ο χρήστης Γ προσπαθεί μέσα από διαδικασίες κρυπτανάλυσης να αποκτήσει μια εκτίμηση για το κλειδί που χρησιμοποιήθηκε ή για τις πληροφορίες που περιέχουν τα

μηνύματα.



Εικόνα 1:Τυπικό σύστημα κρυπτογράφησης-αποκρυπτογράφησης
(http://el.wikipedia.org/wiki/%CE%91%CF%81%CF%87%CE%B5%CE%AF%CE%BF:Sample_1.jpg)

3.3. Κρυπτογραφικά συστήματα

Τα κρυπτοσυστήματα γενικά διακρίνονται σε δυο ευρύτερες κατηγορίες: Τα Κλασσικά και τα Μοντέρνα/Σύγχρονα Κρυπτοσυστήματα. Τα Κλασσικά κρυπτοσυστήματα διακρίνονται σε Αντικατάστασης και Μετάθεσης ενώ στη σύγχρονη κρυπτογραφία υπάρχουν τέσσερα βασικά κρυπτογραφικά συστήματα. Αυτά είναι η Κρυπτογραφία ιδιωτικού κλειδιού/συμμετρική(Private key cryptography/symmetric), η Κρυπτογραφία δημόσιου κλειδιού/ασύμμετρη (Public key cryptography/ asymmetric) και η Υβριδική Κρυπτογραφία κλειδιού(Hybrid cryptography). Τα κρυπτογραφικά συστήματα που θα μελετηθούν σε αυτό το κεφάλαιο είναι το Συμμετρικό και το Ασύμμετρο Κρυπτοσύστημα. Ωστόσο μεγαλύτερη έμφαση δίνεται στην ασύμμετρη κρυπτογραφία εφόσον είναι η κύρια χρησιμοποιούμενη σε μια υποδομή δημόσιου κλειδιού.

Υπάρχουν τρία κριτήρια με τα οποία διαφοροποιούνται τα κρυπτογραφικά συστήματα, τα οποία είναι τα εξής**[Σ. Γκρίτζαλη, Σ. Κ. Κάτσικα, Δ. Γκρίτζαλη,(2003),2,72]**:

- *Ο τύπος των διαδικασιών που χρησιμοποιούνται για το μετασχηματισμό το αρχικού κειμένου σε ένα κρυπτογράφημα.*

Το μεγαλύτερο μέρος των αλγορίθμων που χρησιμοποιούνται στην κρυπτογράφηση βασίζονται στην αντικατάσταση (substitution) και στη μετάθεση (transposition). Κατά την αντικατάσταση κάθε στοιχείο του αρχικού κειμένου αλλάζει από ένα άλλο στοιχείο του αρχικού κειμένου σύμφωνα με κάποιον προκαθορισμένο κανόνα. Ενώ κατά τη μετάθεση γίνεται μία ή περισσότερες φορές αναδιάταξη της σειράς των στοιχείων του αρχικού κειμένου με προκαθορισμένο τρόπο. Οι δυο τύποι διαδικασιών έχουν κοινό χαρακτηριστικό ότι διατηρούν σταθερό το μέγεθος του αρχικού κειμένου έτσι ώστε κατά την αντίστροφη διαδικασία της αποκρυπτογράφησης να λαμβάνεται αυτούσιο το αρχικό κείμενο.

- *Τον αριθμό των κλειδιών που χρησιμοποιούνται.*

Η ειδοποιός διαφορά μεταξύ του συμμετρικού και ασύμμετρου κρυπτοσυστήματος είναι ο αριθμός των κλειδιών που χρησιμοποείται κατά την εκτέλεση των διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης ενός μηνύματος. Στο συμμετρικό κρυπτοσύστημα ο αποστολέας και παραλήπτης κάνουν χρήση ενός κοινού μυστικού κλειδιού (secret key). Ενώ στο ασύμμετρο κρυπτοσύστημα ο αποστολέας και ο παραλήπτης έχουν στη κατοχή τους δύο διαφορετικά ιδιωτικά κλειδιά.

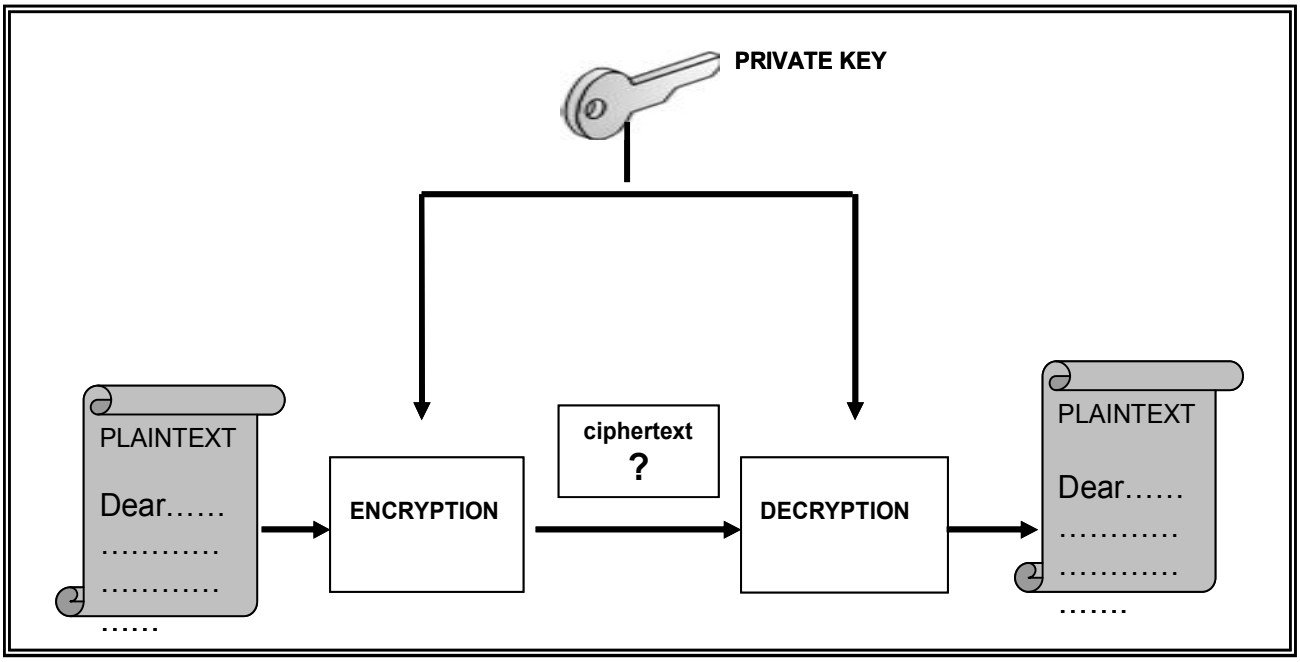
- *Τον τρόπο με τον οποίο επεξεργάζεται το αρχικό κείμενο*

Ένας τρόπος επεξεργασίας του αρχικού κειμένου είναι η εισαγωγή ενός τμήματος στοιχείων συγκεκριμένου μήκους τη φορά σε έναν αλγόριθμο **(block cipher)** για το οποίο δίνει ως έξοδο ένα κωδικοποιημένο τμήμα στοιχείων ίσου μήκους. Ένας άλλος τρόπος επεξεργασίας είναι η εισαγωγή των στοιχείων σε έναν αλγόριθμος (**stream cipher**) με συνεχή ροή, και παράγει ως έξοδος ένα στοιχείο κάθε φορά ανάλογα με τη σειρά που εισήχθησαν.

3.4. Συμμετρικό Κρυπτοσύστημα

Η συμμετρική κρυπτογραφία αναφέρεται συχνά στη βιβλιογραφία και ως συμβατική κρυπτογραφία ή κρυπτογραφία μυστικού/ιδιωτικού κλειδιού. Βασικό χαρακτηριστικό της συμμετρικής κρυπτογραφίας είναι ότι χρησιμοποιείται το ίδιο μυστικό κλειδί για τη διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης. Στην **Εικόνα 2** περιγράφεται σχηματικά η διαδικασία κρυπτογράφηση –αποκρυπτογράφησης της συμμετρικής κρυπτογραφίας. Ο αποστολέας (sender) δημιουργεί το αρχικό κείμενο (plaintext) και εκτελεί σε αυτό τη διαδικασία κρυπτογράφησης (encryption). Δηλαδή εισάγει τα δεδομένα στον αλγόριθμο κρυπτογράφησης και

κάνοντας χρήση του μυστικού κλειδιού (private key), που συμφωνήθηκε από κοινού με τον αποστολέα παράγει το κρυπτογραφημένο μήνυμα (ciphertext). Στη συνέχεια αποστέλλει το μήνυμα, του οποίου πλέον η μορφή είναι δυσανάγνωστη από τους μη εξουσιοδοτημένους χρήστες, στον παραλήπτη. Όταν ο παραλήπτης (receiver) λάβει το κρυπτογραφημένο μήνυμα εκτελεί την αντίστροφη διαδικασία αποκρυπτογράφησης (decryption) χρησιμοποιώντας το ίδιο μυστικό κλειδί (private key) και αλγόριθμο κρυπτογράφησης για να αποκτήσει το αρχικό μήνυμα (plaintext) και να μπορέσει να το διαβάσει. Ωστόσο,πρέπει να τονιστεί ότι για να μπορέσει να λειτουργήσει και να επιφέρει τα επιθυμητά αποτελέσματα η χρήση του συμμετρικού κρυπτοσυστήματος πρέπει το κλειδί που χρησιμοποιείται σε κάθε επικοινωνία να το γνωρίζουν αποκλειστικά και μόνο τα εξουσιοδοτημένα μέρη. Επομένως, επιβάλλεται το μέσο με το οποίο θα διαβιβαστεί το κλειδί να είναι απόλυτα ασφαλές ή να συμφωνηθεί μετά από προσωπική συνάντηση των μερών.



Εικόνα 2:Μοντέλο Συμμετρικού Κρυπτοσυστήματος

3.4.1. Αλγόριθμοι Συμμετρικής Κρυπτογραφίας

Οι συνηθέστεροι τύποι που χρησιμοποιούνται στη συμμετρική κρυπτογραφία και θα αναλύσουμε παρακάτω είναι τα πρότυπα DES, TDES, AES και ο αλγόριθμος IDEA και ακολουθούν τη λογική κρυπτογράφησης τμημάτων (**block cipher**).Επίσης, αξίζει να αναφερθεί, *ότι οι αλγόριθμοι συμμετρικής κρυπτογραφίας βασίζονται σε μία δομή που περιγράφηκε πρώτα από τον H.Feistel της IBM το 1973*.**[P.Muller,1993]**

1. Data Encryption Standard(DES)

Το σχήμα κρυπτογράφησης DES σχεδιάστηκε και αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από το National Institute of Standards and Technology-NIST ,USA ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών 46-FIPS PUB 46. Ο αλγόριθμος που υλοποιείται στο σύστημα DES αναφέρεται ως Data Encryption Algorithm-DEA. **[Σ. Γκρίτζαλη, Σ. Κ. Κάτσικα, Δ. Γκρίτζαλη,(2003),3,80-81]**. Τα χαρακτηριστικά του DES είναι :το αρχικό τμήμα κεμένου που δέχεται ως είσοδο είναι μεγέθους 64-bit, το κλειδί που χρησιμοποιεί έχει μήκος 56-bit. Περιληπτικά, το DES λειτουργεί ως εξής: Η λειτουργία του χωρίζεται σε δύο πλευρές τη αριστερή και την δεξιά. Στην αριστερή πλευρά, σε πρώτη φάση μετασχηματίζει το αρχικό κείμενο καθορισμένου μεγέθους αναδιατάσσοντας τα bits και παράγει τη μετασχηματισμένη είσοδο σε ίσου μεγέθους τμήμα. Στη συνέχεια, ακολουθεί η δεύτερη φάση που λειτουργεί επαναληπτικά για κάθε ένα τμήμα διαδοχικά για 16 φορές. Σε αυτή τη φάση για κάθε επανάληψη παράγεται και εισάγεται στα δεδομένα ένα υπό-κλειδί. Τα υπό-κλειδιά παράγονται στη δεξιά πλευρά, είναι μεγέθους 56-bit και αυτά τροποποιούνται αρχικά από μία άλλη συνάρτηση μετασχηματισμού 1. Η συνάρτηση μετασχηματισμού παραμένει ίδια για κάθε επανάληψη, αλλά κάθε φορά παράγεται διαφορετικό υπό-κλειδί, λόγω της επανειλημμένης μετατόπισης των ψηφίων του κλειδιού και μιας συνάρτησης μετασχηματισμού 2.Στην έξοδο της τελευταίας επανάληψης δίνεται ένα τμήμα μήκους 64-bit που είναι συνδυασμός του αρχικού κειμένου και του υπό-κλειδιού. Έπειτα στο τμήμα αυτό πραγματοποιείται αντιμετάθεση του αριστερού μισού τμήματος (32-bit) με του δεξιού μισού τμήματος (32-bit). Μετά την αντιμετάθεση, τροποποιείται με τον αντίστροφο μετασχηματισμού της πρώτης φάσης της αριστερής πλευράς για να παραχθεί η τελική έξοδος (τμήμα 64-bit) που είναι το κρυπτογράφημα **[1]**.

2. Triple Data Encryption Standard (TDES)

Το TDES προτάθηκε αρχικά από τον W.Tuchman και το 1985 προτυποποιήθηκε στο ANSI X9.17, ώστε να χρησιμοποιηθεί σε οικονομικές εφαρμογές.Το 1999, με τη δημοσίευση του ως FIPS PUB 46-3, το TDES ενσωματώθηκε ως τμήμα της προτυποποίησης κρυπτογράφησης δεδομένων DES. Το TDES ακολούθησε τον αλγόριθμο 2DES ο οποίος δεν αξιοποιήθηκε ευρέως εφόσον κρίθηκε ευάλωτος σε κρυπταναλυτικές επιθέσεις**[Σ. Γκρίτζαλη, Σ. Κ. Κάτσικα, Δ. Γκρίτζαλη,(2003), 3,84]**. Το TDES χρησιμοποιεί τρία κλειδια και τρείς εκτελέσεις του αλγορίθμου DES κάνοντας 48 κύκλους στον υπολογισμό του. Με την υποστήριξη τριών διαφορετικών κλειδιών, διαθέτει κλειδί μήκους 128-bit. Ωστόσο μπορεί να χρησιμοποιήσει και δυο κλειδιά οπότε να διαθέτει κλειδί μήκους 112-bit. Αυτό το χαρακτηριστικό τον κάνει πιο ανθεκτικό σε επιθέσεις εξαντλητικής αναζήτησης, οι

οποίες με μεγάλο μήκος κλειδών είναι υπολογιστικά ανέφικτες. Ο αλγόριθμος κατά την κρυπτογράφηση ενός τμήματος λειτουργεί ως εξής :κρυπτογράφηση, αποκρυπτογράφηση, κρυπτογράφηση (Encryptio-Decryption-Encryption) για να παράγει το κρυπτογράφημα. Εάν χρησιμοποιηθούν τρία κλειδιά το κάθε ένα αντιστοιχεί σε μια διαδικασία. Εάν χρησιμοποιηθούν δύο κλειδιά το κλειδί της κρυπτογράφησης είναι κοινό. Η αποκρυπτογράφηση στη δεύτερη φάση επιτρέπει την αποκρυπτογράφηση των δεδομένων που κρυπτογραφούνται από το DES. Επομένως,είναι κατανοητό ότι κρυπτογραφώντας δυο φορές το ίδιο τμήμα με διαφορετικό κλειδί αφενός αυξάνεται η αντοχή σε πιθανή κρυπταναλυτική επίθεση και αφετέρου μειώνεται η αποδοτικότητα του αλγορίθμου καθώς είναι πιο πολύπλοκος κατά την υλοποίηση του **[24]**.

3. Advanced Encryption Standard (AES)

Έπειτα από πολλά χρόνια χρησιμοποίησης του DES(Data Encryption Standard) ως πρότυπο κρυπτογραφίας για γενικότερους λόγους αποδοτικότητας και ασφάλειας δημιουργήθηκε η ανάγκη σχεδιασμού του AES. Τον Ιανουάριο του 1997 εκδηλώθηκε πρόσκληση από το NIST (National Institute of Technology) σε ενδιαφερόμενους να καταθέσουν τις προτάσεις τους για το Προηγμένο Πρότυπο Κρυπτογράφησης (Advanced Encryption Standard-AES). Οι απαιτήσεις που τέθηκαν ήταν ότι το AES θα αποτελεί αλγόριθμο τμημάτων με μήκος τμήματος 128 bit, συμμετρικού κρυπτοσυστήματος και τα κλειδιά που θα χρησιμοποιεί να είναι μήκους 128-bit, 192-bit και 256-bit. Οι προτάσεις που τελικά επιλέχθηκαν είναι οι **:MARS, RC6, Serpent, Twofish.** Από αυτούς τελικά ο αλγόριθμος **Rijndael** είναι αυτός που υιοθετήθηκε ως αλγόριθμος του AES.Ο αλγόριθμος **Rijndael** είναι απλός, ευέλικτος και έχει υψηλές αντοχές σε όλες τις γνωστές κρυπταναλυτικές επιθέσεις. Τα μήκη κλειδιών που χρησιμοποιούνται είναι 128-bit, 192-bit, 256-bit και περιλαμβάνουν αντίστοιχα με το μέγεθος του μυστικού κλειδιού 10, 12, και 14 κύκλους **[1]**.

4. International Data Encryption Algorithm (IDEA)

Ο αλγόριθμος International Data Encryption Algorithm (IDEA) είναι ένας αλγόριθμος τμημάτων (block cipher) και λειτουργεί σε τμήματα αρχικού μηνύματος μήκους 64-bit.Το 64-bit τμήμα χωρίζεται σε 16 μικρότερα τμήματα όπου το καθένα κάνει 8 κύκλους σε μία μαθηματική συνάρτηση χρησιμοποιώντας κλειδί μήκους 128-bit **[24]**. Οι συναρτήσεις που χρησιμοποιεί διαφέρουν από το DES καθώς συνδυάζονται για να πραγματοποιηθεί ένας πολυπλοκότερος μετασχηματισμός στα δεδομένα με αποτέλεσμα να χαρακτηρίζεται από ρωμαλεότητα απέναντι στις κρυπταναλυτικές επιθέσεις. Επίσης θεωρείται υπολογιστικά πιο γρήγορος από τον DES κατά την εφαρμογή του **[1]**.

3.4.2. Επιθέσεις στους αλγόριθμους συμμετρικού κλειδιού

Οι διάφοροι τύποι επιθέσεων κρυπτανάλυσης, διαφοροποιούνται, μεταξύ άλλων, με βάση την ποσότητα και το είδος της πληροφορίας που είναι γνωστή στον κρυπταναλυτή. **[W.Stallings, 1995]**. Οι αλγόριθμοι που χρησιμοποιούνται είναι γνωστοί η μόνη πληροφορία που παραμένει μυστική είναι το κλειδί. Όσο πιο σύνθετος είναι ο αλγόριθμος, τόσο ασφαλέστερο είναι το κλειδί και κατ'επέκταση η κρυπτογράφηση είναι πιο δύσκολο να "σπάσει". Γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς**[Κύτταρο, Περιοδικό Επιστήμης και Τεχνολογίας**, **2010, αρθρο:Κρυπτογραφία]**.

- **Επιθέσεις αναζήτησης κλειδιού (Key search attack).**

Ο επιτιθέμενος, γνωρίζοντας τον αλγόριθμο που χρησιμοποιήθηκε, δοκιμάζει όλα τα πιθανά κλειδιά έως ότου αποκαλύψει το μυστικό κλειδί που χρησιμοποιείται κατά τις διαδικασίες κρυπτογράφησης - αποκρυπτογράφησης. Επομένως, όταν το μέγεθος του κλειδιού είναι μεγάλο είναι και υπολογιστικά δυσκολότερο να εντοπιστεί.

- **Επιθέσεις γνωστού αρχικού κειμένου (known-plaintext attack).**

Σε αυτού του είδους τις επιθέσεις, ο κρυπταναλυτής (επιτιθέμενος) γνωρίζει τμήματα των αρχικών μηνυμάτων ή τον τύπο της πληροφορίας που περιέχεται (π.χ.ένα λογισμικό) καθώς και τα αντίστοιχα κρυπτογραφήματα τους. Έτσι επιχειρεί να αποκαλύψει το κλειδί που χρησιμοποιείται καθώς μπορεί να βρεί τη θέση που έχει στο κρυπτογράφημα η πληροφορία αυτή.

- **Επιθέσεις επιλεγμένου κειμένου (chosen-text attack).**

Σε αυτή τη περίπτωση ο επιτιθέμενος επιλέγει τα μέρη, είτε από το αρχικό κείμενο είτε από τα κρυπτογραφήματα, τα οποία θα τον βοηθήσουν στην προσπάθεια εύρεσης του μυστικού κλειδιού.

3.5. Ασύμμετρη Κρυπτογράφηση

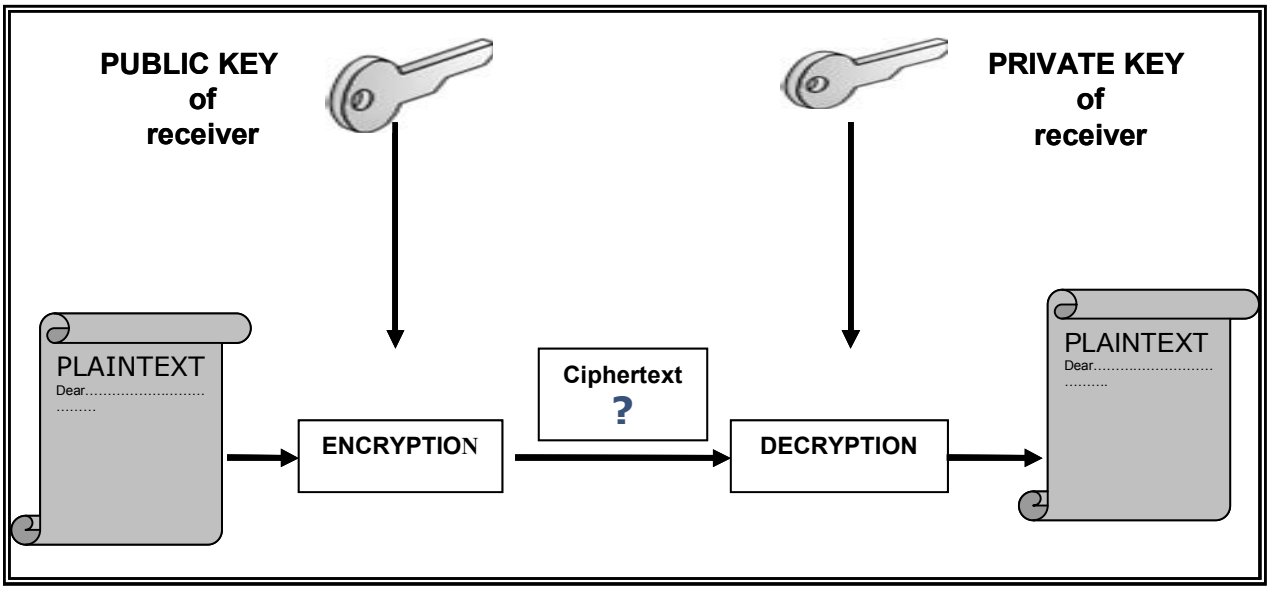
Όπως είδαμε στην προηγούμενη ενότητα, για την αποτελεσματική λειτουργία του συμμετρικού κρυπτοσυστήματος θεωρείται αναγκαία η διαφύλαξη της μυστικότητας των κλειδιών που διαμοιράζονται τα μέρη που επικοινωνούν. Έτσι μεγάλη σημασία για την επιτυχία του έχει ο τρόπος διανομής των μυστικών κλειδιών στους χρήστες της. Η ασύμμετρη κρυπτογράφηση ή όπως αλλιώς αναφέρεται κρυπτογράφηση δημοσίου κλειδιού έρχεται να λύσει το πρόβλημα που υπήρχε

στους κρυπτογραφικούς αλγόριθμους συμμετρικού κλειδιού για τη διανομή των κλειδιών.1 Ωστόσο, αξίζει να αναφερθεί, ότι το ασύμμετρο σύστημα κρυπτογραφία δεν αντικαθιστά το συμμετρικό καθώς και τα δύο είδη κρυπτοσυστημάτων θεωρούνται εξίσου σημαντικά.

Η κρυπτογράφηση δημόσιου κλειδιού που για πρώτη φορά προτάθηκε δημόσια από τους Whitfield Diffie και MartinHellman το 1976, αποτελεί την πρώτη πραγματική επαναστατική πρόοδο στην κρυπτογράφηση κυριολεκτικά εδώ και πολλά χρόνια **[Phil Zimmermann, 1, 14]**. Η κρυπτογραφία δημόσιου κλειδιού περιλαμβάνει τη χρήση δύο ξεχωριστών κλειδιών, σε αντίθεση με τη συμμετρική συμβατική κρυπτογράφηση, η οποία χρησιμοποιεί μόνον ένα κλειδί. Ο κρυπτογραφικός αλγόριθμος στην ασύμμετρη κρυπτογραφία πολλαπλασιάζει δύο πρωταρχικούς αριθμούς και υπολογίζει έπειτα μια σειρά μαθηματικών διαδικασιών και ολοκληρώνει με δύο τελικούς αριθμούς. Δημιουργείται έτσι ένα ζεύγος κλειδιών (key pair) ο ένας από εκείνους τους αριθμούς θα είναι ιδιωτικός ο βασικός και άλλος θα είναι το δημόσιο κλειδί. Το ιδιωτικό κλειδί ανήκει στον ιδιοκτήτη και δεν διαβιβάζεται ποτέ σε ολόκληρο το Διαδίκτυο κρατιέται ασφαλές με τον ιδιοκτήτη, άρα παραμένει μυστικό, αλλά αναφέρεται ως ιδιωτικό ώστε να αποφευχθεί εννοιολογική σύγχυση με τη συμμετρική κρυπτογραφία. Το δημόσιο κλειδί θα διαβιβαστεί σε ολόκληρο το Διαδίκτυο και μπορεί να προσεγγιστεί από κάποιον ενδιαφερόμενο. Το ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση των μηνυμάτων. Το δημόσιο και ιδιωτικό κλειδί λογω της άμεσης σχέσης που έχουν μεταξύ τους αναφέρονται και ως ζεύγος κλειδιών. Η χρήση δύο κλειδιών έχει ισχυρές συνέπειες στις περιοχές της εμπιστευτικότητας, της διανομής κλειδιού και της πιστοποίησης **[3]**.

Έστω ότι δυο χρήστες επιθυμούν να επικοινωνήσουν ασφαλώς κάνοντας χρήση της ασύμμετρης κρυπτογράφησης. Ο αποστολέας (sender) θα δημιουργήσει ένα μήνυμα και στη συνέχεια θα το κρυπτογραφήσει με το δημόσιο κλειδί του παραλήπτη (public key of receiver), το οποίο όπως αναφέρθηκε προηγουμένως είναι γνωστό προς κάθε ενδιαφερόμενο, και το αποστέλλει. Το μήνυμα που στάλθηκε είναι περιέχει το κρυπτογραφημένο κείμενο (ciphertext) άρα και προστατευμένο από τους μη εξουσιοδοτημένες προσβάσεις.. Ο παραλήπτης όταν λάβει το μήνυμα προκειμένου να ανακτήσει το αρχικό κείμενο (plaintext) εκτελεί τη διαδικασία της αποκρυπτογράφησης (decryption) με το ιδιωτικό του κλειδί (private key of receiver). Όλα όσα περιγράφησαν απεικονίζονται στην παρακάτω **Εικόνα 3.**

[1] Υφίστανται τεχνικές διανομής κλειδιών στη συμμετρική κρυπτογραφία αλλά δεν αναλύονται στη παρούσα εργασία.



Εικόνα 3:Μοντέλο Ασύμμετρου Κρυπτοσυστήματος

Οι περιπτώσεις στις οποίες χρησιμοποιείται κυρίως το ζεύγος κλειδιών στα ασυμμετρά κρυπτοσυστήματα είναι οι εξής**[2]**:

- **Κρυπτογράφηση/Αποκρυπτογράφηση μηνυμάτων:** Ο αποστολέας κρυπτογραφεί ένα μήνυμα με το δημόσιο κλειδί του και ο παραλήπτης αποκρυπτογραφεί με το ιδιωτικό του.
- **Ψηφιακή Υπογραφή(Digital Signature):** Ο αποστολέας υπογράφει ένα μήνυμα κάνοντας χρήση του ιδιωτικού του κλειδί.Οι Ψηφιακές Υπογραφές μελετούνται εκτενέστερα στο επόμενο κεφάλαιο και έχουν ως κύριο σκοπό την αυθεντικοποίηση του αποστολέα με τη χρήση του δημόσιου κλειδιού του από τον παραλήπτη.
- **Ανταλλαγή κλειδιών (Key Exchange):** Όταν δύο συμβαλλόμενα μέρη συνεργάζονται ώστε να ανταλλάξουν ένα κλειδί συνόδου (session key)[2].Για την πραγματοποίηση αυτής της ανταλλαγής είναι πιθανό να αξιοποιηθούν τα ιδιωτικά κλειδιά των συμβαλλόμενων.

3.5.1. Αλγόριθμοι για Ασύμμετρα Κρυπτοσυστήματα

Στους αλγόριθμους που χρησιμοποιούνται στα ασύμμετρα κρυπτοσυστήματα συμπεριλαμβάνονται οι αλγόριθμοι: RSA, Diffie-Hellman (key exchange), Digital SignatureStandard (DSS) και Elliptic-Curve Cryptography (ECC). Ωστόσο οι πιο γνωστοί εξ΄αυτών θεωρούνται ο αλγόριθμος RSA και ο αλγόριθμος των Diffie-Hellman (key exchange) και είναι αυτοί οι οποίοι θα αναπτυχθούν στη παρούσα ενότητα.

[2] Το κλειδί συνόδου (session key) χρησιμοποιείται στη διανομή κλειδιών συμμετρικής κρυπτογράφησης.

Μετά την πρόταση του ασύμμετρου συστήματος κρυπτογράφησης από τους W. Diffie και M. Hellman καθορίστηκαν οι προϋποθέσεις που πρέπει να πληροί ένας αλγόριθμος δημοσίου κλειδιού. Οι προυποθέσεις αυτές αφορούν την υπολογιστική πολυπλοκότητα των αλγορίθμων όσον αφορά την υλοποίηση τους και την αντοχή τους ενάντια των επιθέσεων. Δηλαδή, απαιτείται να είναι υπολογιστικά εύκολο για τον αποστολέα και τον παραλήπτη να εκτελέσουν τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης. Επίσης να είναι υπολογιστικά εύκολο η δημιουργία ενός ζεύγους κλειδιών (δημόσιο κλειδί, ιδιωτικό κλειδί). Ενώ αντίθετα απαιτείται να είναι υπολογιστικά ανέφικτο (computationally infeasible) να παραχθεί το ιδιωτικό κλειδί μέσου του δημόσιου όπως και να παραχθεί το αρχικό κείμενο γνωρίζοντας το δημόσιο κλειδί και το κρυπτογράφημα του.

1. Αλγόριθμος RSA

Μια από τις δημοφιλέστερες μορφές ενός αλγορίθμου κρυπτογράφησης είναι ο RSA. Ο αλγόριθμος RSA αντλεί το όνομά του από το πρώτο αρχικό γράμμα του επωνύμου των τριών ιδρυτών του, Ron Rivest, Adi Shamir, and Leonar Adelman. Χρησιμοποιείται ευρέως και συμπεριλαμβάνεται και στη Microsoft και στις μηχανές αναζήτησης Netscape.

Ο RSA είναι ο αλγόριθμος κρυπτογράφησης στον οποίο το αρχικό κείμενο (m) και το αντίστοιχο κρυπτογραφημένο κείμενο (c) είναι ακέραιοι αριθμοί με τιμές μεταξύ 0 και n-1, για κάποιο n. Επίσης, ο RSA είναι ένας αλγόριθμος με δημόσιο κλειδί KU={e,n} και ιδιωτικό κλειδί KR={d,n}.

Η συνάρτηση κρυπτογράφησης είναι: $c = m^e \pmod n$

Η συνάρτηση αποκρυπτογράφησης είναι: $m = cd \pmod n = (m\ e)d \pmod n = med \pmod n$

Η λειτουργία του αλγόριθμου που παρουσιάζεται συνοπτικά στο στην **Εικόνα 4** είναι: Αρχικά επιλέγονται δύο πρώτοι αριθμοί p,q και υπολογίζεται το γινόμενο τους n. Στη συνέχεια χρησιμοποιείται η τιμή της συνάρτησης $f(n)$, γνωστή ως συνάρτηση του Euler για το n ($f(n)=(p-1)(q-1)$), η οποία δείχνει το πλήθος των θετικών ακεραίων που είναι μικρότεροι από n και πρώτοι με αυτόν .Επιλέγεται ένας ακέραιος αριθμός e, ο οποίος είναι πρώτος ως προς το $f(n)$, δηλαδή μέγιστος κοινός διαιρέτης του e και του $f(n)$ να είναι το 1.Τέλος υπολογίζεται ο αριθμός d, ως φυσικός αντίστροφος αριθμός του *e modulo* $f(n)$, από τη σχέση $d = e^{-1} \bmod f(n)$.

Βασική προϋπόθεση είναι ο αποστολέας και ο παραλήπτης να γνωρίζουν τις τιμές των e και n.Αντίθετα η τιμή του d θα πρέπει να είναι γνωστή μόνο από τον παραλήπτη. Τα p, q,και $f(n)$ παραμένουν άγνωστα.Έτσι, αν υποθέσουμε ότι ο χρήστης Α έχει δημοσιεύσει το δημόσιο κλειδί του και ο χρήστης Β επιθυμεί να αποστείλει ένα μήνυμα m στον Α, τότε ο Β υπολογίζει την παράσταση

$c= m^e$ *(mod n)* και μεταδίδει το c.Για την αποκρυπτογράφηση αντίστοιχα του μηνύματος, ο χρήστης Α υπολογίζει την παράσταση $m= c^d$ *(mod n)*.

Ωστόσο για να θεωρηθεί ικανοποιητικός ο αλγόριθμος πρέπει να ικανοποιούνται οι ακόλουθες απαιτήσεις: Να είναι εφικό να βρεθούν τιμές για τα e, d, n τέτοιες ώστε να ισχύει: $m^{ed} = m$ *(mod n)*, για κάθε $m<n$.Να μην είναι υπολογιστικά πολύπλοκο να υπολογίσουν οι χρήστες το κρυπτογράφημα από το αρχικό κείμενο και αντιστρόφως, για κάθε $m<n$. Τέλος να είναι υπολογιστικά ανέφικτο να βρεθεί το *d* , δοθέντων των *e* και *n*.Οι δύο πρώτες απαιτήσεις ικανοποιούνται εύκολα ενώ η τελευταία μπορεί να ικανοποιηθεί μόνο για μεγάλες τιμές των e και n.Μπορεί να αποδειχθεί ότι το d και το e πληρούν τις απαιτούμενες ιδιότητες**[19][2]**.

Παραγωγή κλειδιού	
Επιλογή q,p: αριθμοί	p και q δύο πρώτοι
Υπολογισμός:	n = pxq
Υπολογισμός:	f(n) = (p-1)x(q-1)
Επιλογή ακέραιο e: 1<e<φ(n)	gcd(e, φ(n))=1;
Υπολογισμός d:	$d = e^{-1} \bmod \varphi(n)$
Δημόσιο κλειδί:	KU={e,n}
Ιδιωτικό κλειδί:	KR={d,n}

Κρυπτογράφηση	
Αρχικό κείμενο:	$c= m^e \pmod n$
Κρυπτογράφημα:	m<n

Αποκρυπτογράφηση	
Κρυπτογράφημα:	c
Αρχικό κείμενο:	$m= c^d \pmod n$

Εικόνα 4:Συνοπτική περιγραφή αλγορίθμου RSA [2]

2.Diffie-Hellman key exchange

Ο αλγόριθμος **Diffie-Hellman** δημοσιεύτηκε πρώτος στην εργασία των Diffie Hellman που όριζε την κρυπτογραφία με ασύμμετρο κρυπτοσύστημα και είναι γνωστός ως ανταλλαγή κλειδιών κατά Diffie-Hellman . Ο αλγόριθμος περιορίζεται ακριβώς στην ανταλλαγή κλειδιών **[12]**. Σκοπός του αλγορίθμου είναι να καταστήσει εφικτή και ασφαλή μεταξύ δύο χρηστών την ανταλλαγή ενός μυστικού κλειδιού, το οποίο ακολούθως θα χρησιμοποιηθεί για κρυπτογράφηση μηνυμάτων. Οι δύο

χρήστες επιλέγουν κάποιες κοινές αριθμητικές τιμές και τότε ο καθένας δημιουργεί ένα κλειδί. Έπειτα ανταλλάσουν τους μαθηματικούς μετασχηματισμούς .Έτσι κάθε χρήστης δύναται να υπολογίσει ένα κλειδί συνόδου (session key). Η αποτελεσματικότητα του βασίζεται στη δυσκολία υπολογισμού διακριτών λογαρίθμων τους οποίους χρησιμοποιεί ο αλγόριθμος.

3.5.2. Επιθέσεις στους αλγόριθμους δημόσιου κλειδιού

Οι επιθέσεις στους αλγόριθμους δημοσίου κλειδιού βασίζονται κυρίως στην εύρεση ενός ελαττώματος στον αλγόριθμο που χρησιμοποιείται καθώς και στην ανάλυση μεγάλων αριθμών. Επίσης, όπως αναφέρθηκε και στα συμμετρικά κρυπτοσυστήματα μπορεί να υπάρξει επίθεση εξαντλητικής αναζήτησης κλειδιών.Για αυτό είναι απαραίτητη η χρήση κλειδιών μεγάλου μήκους.

- **Επιθέσεις παραγοντοποίησης (factoring attacks)**

Χρησιμοποιεί το δημόσιο κλειδί ώστε να αντλήσει το ιδιωτικό. Συγκεκριμένα, επικεντρώνεται στη διαδικασία ανεύρεσης δύο πρώτων αριθμών οι οποίοι να είναι παράγοντες του n.

- **Επίθεση αλγοριθμική**

Αυτός ο τρόπος επίθεσης επικεντρώνεται στο να ανακαλυφθεί κάποια βασική αδυναμία στους μαθηματικούς υπολογισμούς στους οποίους βασίζεται ο αλγόριθμος.

3.6. Συναρτήσεις Κατακερματισμού (Hash functions)

Μία θεμελιώδη μέθοδος που χρησιμοποιείται στην κρυπτογραφία δημόσιου κλειδιού είναι οι συναρτήσεις κατακερματισμού. Παράγουν από κάθε μήνυμα ανεξαρτήτως του μεγέθους του μια σύνοψη (message digest), που είναι μια σειρά από bits με συγκεκριμένο πλήθος. Δηλαδή, μία συνάρτηση σύνοψης H(m) δέχεται ως είσοδο ένα μεταβλητού μεγέθους μήνυμα και παράγει ως έξοδο μία σύνοψη σταθερού μήκους. Η σύνοψη του μηνύματος, που είναι γνωστή με τον όρο fingerprint ή message digest, αποτελεί μια ψηφιακή αναπαράσταση του μηνύματος και είναι μοναδική για το μήνυμα που αντιπροσωπεύει**[21]**.

Αν αλλάξουμε έστω και μια τελεία στο μήνυμα, θα αλλάξει και η σύνοψή του, ενώ είναι πρακτικά αδύνατο δύο διαφορετικά μηνύματα να δώσουν την ίδια σύνοψη. Η μεγάλη αυτή ευαισθησία στα δεδομένα εισόδου αποτελεί μια από τις πολυτιμότερες ιδιότητες της συνάρτησης σύνοψης καθώς παρέχει υπηρεσία ακεραιότητας μηνυμάτων**[44]**. Μια αποδεκτή και ευρέως γνωστή συνάρτηση σύνοψης είναι η SHA-1.

Η συνάρτηση κατακερματισμού δεν κρατάτε μυστική, αλλά η διαφύλαξη της μυστικότητας και ακεραιότητας του μηνύματος έγκειται στο ότι η συνάρτηση κατακερματισμού είναι μονόδρομη και έτσι είναι πολύ δύσκολο να εκτελεστεί προς τα πίσω σε ένα μήνυμα και να βρεθεί το αρχικό

κείμενο(plaintext). Ο αλγόριθμος που χρησιμοποιείται για να παραχθεί η σύνοψη βασίζεται στην ίδια διαδικασία με τον αλγόριθμο RSA. Δηλαδή στον πολλαπλασιασμό δύο μεγάλων πρώτων αριθμών. Επομένως η αντίστροφη κατεύθυνση δηλαδή η παραγοντοποίηση της εξόδου της συνάρτησης για να ανακτηθούν οι δύο αρχικοί πρώτοι αριθμοί είναι εξαιρετικά δύσκολη[3] **[1][8]**. Ο παραλήπτης δεν προσπαθεί να αντιστρέψει τη διαδικασία , αλλά αντ' αυτού τρέχει την ίδια συνάρτηση και συγκρίνει τα δύο αποτελέσματα. Για αυτό και αναφέρονται συχνά ως μονόδρομές συναρτήσεις σύνοψης (one way hash functions).

3.7. Σύγκριση Μεθόδων Κρυπτογράφησης

Σε αυτό το σημείο μπορούμε να συγκρίνουμε τις δυο μεθόδους κρυπτογράφησης συμμετρική και ασύμμετρη, εφόσον εξετάσαμε το τρόπο λειτουργία τους, τους αλγόριθμους που χρησιμοποιούν και τις επιθέσεις που αυτοί έχουν δεχτεί. Όπως είδαμε, κατά τη συμμετρική κρυπτογραφία απαιτείται η ύπαρξη ενός μυστικού κλειδιού το οποίο πρέπει να μεταβιβαστεί στους χρήστες που θέλουν να επικοινωνήσουν με ασφαλή τρόπο. Το πλεονεκτήμα της κρυπτογραφίας δημοσίου κλειδιού είναι ότι το ζεύγος κλειδιών που θα χρησιμοποιηθεί μπορεί να παραχθεί από τους ίδιους τους χρήστες χωρίς να χρειάζεται το ιδιωτικό κλειδί να διανεμηθεί (άρα παραμένει μυστικό στη κατοχή του χρήστη) αλλά μόνο το δημόσιο καθώς αυτό χρησιμοποιείται στη κρυπτογράφηση. Επομένως είναι ευκολότερο να υλοποιηθεί γιατί δεν χρειάζεται η μετάδοση των μυστικών κλειδιών μέσω ενός ασφαλούς δικτύου. Ωστόσο, η υπολογιστική ισχύς που απαιτείται για την ασύμμετρη κρυπτογραφία είναι πολύ μεγαλύτερη από αυτή που χρειάζεται για κρυπτογραφία συμμετρικού κλειδιού. Έτσι για μεταφορά μεγάλων ποσοτήτων δεδομένων προτιμούνται συνήθως οι μέθοδοι συμμετρικής κρυπτογράφησης. Στην πραγματικότητα, η ασφάλεια οποιουδήποτε σχήματος κρυπτογράφησης εξαρτάται από δύο βασικά σημεία που είναι το μήκος του κλειδιού και η υπολογιστική εργασία που περιλαμβάνεται στο σπάσιμο ενός κρυπτογραφήματος. Δεν υπάρχει τίποτα είτε για τη συμμετρική είτε για την ασύμμετρη κρυπτογράφηση που να κάνει τη μία ανώτερη από την άλλη από άποψη αντοχής στην κρυπτανάλυση. Συμπερασματικά, καμία από τις δύο μέθοδοι κρυπτογράφησης έχουν την ίδια σπουδαιότητα και δεν προβλέπεται η ασύμμετρη να αντικαταστήσει τη συμμετρική κρυπτογράφηση.

[3] Στη βιβλιογραφία η διαδικασία αυτή παρομοιάζεται με ένα ποτήρι που έχει σπάσει και έγινε μικρά κομμάτια.Η κατάσταση είναι πολύ δύσκολα αντιστρέψιμη **[1]**

4 *Κεφάλαιο*

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Οι ψηφιακές υπογραφές είναι παρόμοιες με τις αντίστοιχες χειρόγραφες υπογραφές σε έντυπα έγγραφα. Προσφέρουν σημαντικά πλεονεκτήματα έναντι των χειρόγραφων διότι υλοποιούνται με χρήση ασφαλών κρυπτογραφικών αλγορίθμων, έτσι είναι πολύ δυσκολότερο να πλαστογραφηθούν σε σχέση με τις χειρόγραφες. Επίσης, το φυσικό πρόσωπο που υπογράφει ψηφιακά το έγγραφο δεν μπορεί να ισχυριστεί ότι δεν υπέγραψε το μήνυμα με την προυπόθεση ότι το ιδιωτικό του κλεδί δεν υπεκλάπη (Μη-αποποίηση). Παραδείγματα χρήσης είναι τα μηνύματα ηλεκτρονικού ταχυδρομείου, έγγραφα, μηνύματα που στέλνονται στο Διαδίκτυο κλπ. Στην Ελλάδα το 1999 με ειδική πρόβλεψη του νόμου Ν.2672 προτείνεται η αντικατάσταση του όρου "ηλεκτρονική" με τον όρο "ψηφιακή υπογραφή" και δίνεται ο ορισμός της: *"Η ψηφιακής μορφής υπογραφή σε δεδομένα ή λογικά συνεχιζόμενη με αυτά, που χρησιμοποιείται από τον υπογράφοντα ως ένδειξη υπογραφής του περιεχομένου των δεδομένων αυτών, εφόσον η εν λόγω υπογραφή α) συνδέεται μονοσήμαντα με τον υπογράφοντα, β) ταυτοποιεί τον υπογράφοντα, γ) δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον έλεγχό του και δ) συνδέεται με τα δεδομένα στα οποία αναφέρεται κατά τρόπο ώστε να μπορεί να αποκαλυφθεί οποιαδήποτε αλλοίωση των εν λόγω δεδομένων*". Παρόλα αυτά δεν εξομοιώνεται νομικά ακόμη η ψηφιακή υπογραφή με την χειρόγραφη. Το **Προεδρικό Διάταγμα 150/2001 [«Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για**

ηλεκτρονικές υπογραφές» (ΦΕΚ Α΄125/25.6.2001)] καθόρισε το πλαίσιο εκείνο μέσα στο οποίο μία ψηφιακή υπογραφή αναγνωρίζεται νομικά ως χειρόγραφη.

4.1. Ορισμός και Λειτουργία

Ψηφιακή υπογραφή είναι μία μοναδική κρυπτογραφημένη σύνοψη που χρησιμοποιείται για την απόδειξη της γνησιότητας ενός ψηφιακού μηνύματος ή εγγράφου. Με τη χρήση της ο παραλήπτης είναι βέβαιος ότι το μήνυμα που παραλαμβάνει ανήκει στον αποστολέα (αυθεντικοποίηση), χωρίς αλλοιώσεις (ακεραιότητα) και παρέχει υπηρεσίες μη αποποίησης αποστολή ενός μηνύματος**[8]**.

Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού. Ο κάθε χρήστης θα πρέπει να διαθέτει ένα ζεύγος κλειδιών (δημόσιο, ιδιωτικό) τα οποία έχουν μεταξύ τους κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ψηφιακής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα**[2].**

Στη συνέχεια περιγράφεται ο τρόπος λειτουργίας της ψηφιακής υπογραφής. Υποθέτουμε ότι ο χρήστης Β επιθυμεί να αποστείλει ένα μήνυμα στον χρήστη Α. Τότε, ο Β κρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί. Όταν ο Α παραλάβει το κρυπτογραφημένο μήνυμα, το αποκρυπτογραφεί με το δημόσιο κλειδί του Β. Εξασφαλίζει με αυτό τον τρόπο ότι το αρχικό μήνυμα έχει κρυπτογραφηθεί από τον Β. Δεδομένου ότι ο αποστολέας διατηρεί ασφαλές το ιδιωτικό του κλειδί τότε ο παραλήπτης που χρησιμοποιεί το αντίστοιχο δημόσιο κλειδί του Β για να αποκρυπτογραφήσει το μήνυμα, πιστοποιεί την ταυτότητα του αποστολέα. Έτσι, όλο το κρυπτογραφημένο κείμενο αποτελεί μία ψηφιακή υπογραφή (digital signature) καθώς κανένας δεν μπορεί να δημιουργήσει κρυπτογραφημένο κείμενο το οποίο να αποκρυπτογραφείται με το δημόσιο κλειδί του Β.

Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (one way hash) της οποίας η λειτουργία περιγράφηκε στο Κεφάλαιο 3. Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτως του μεγέθους του, παράγεται η σύνοψη του, η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος και είναι μοναδική για κάθε μήνυμα**[1]**. Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, είναι υπολογιστικά

αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί. Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης (ακεραιότητα μηνύματος). Η ψηφιακή υπογραφή, στην ουσία είναι η κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα, σύνοψη. Επίσης, εξαιτίας του γεγονότος ότι οι ψηφιακές υπογραφές δεν περιλαμβάνουν αυτόματα την ημερομηνία ότι το μήνυμα υπογράφηκε μπορεί να έχει τις σοβαρές αρνητικές συνέπειες διότι ότι κάποιος θα μπορούσε να πάρει ένα παλιό μήνυμα και να το υπογράψει σε έναν πιό πρόσφατο χρόνο. Για την αποφυγή αυτού μπορεί να χρησιμοποιηθεί η εμπιστευμένη χρονική σφράγιση στις ψηφιακές υπογραφές. Η εμπιστευμένη χρονική σφράγιση (time-stamping) είναι ένα αποτελεσματικό εργαλείο που θα αποτρέψει αυτόν τον τύπο ψηφιακής κατάχρησης υπογραφών **[12]**.

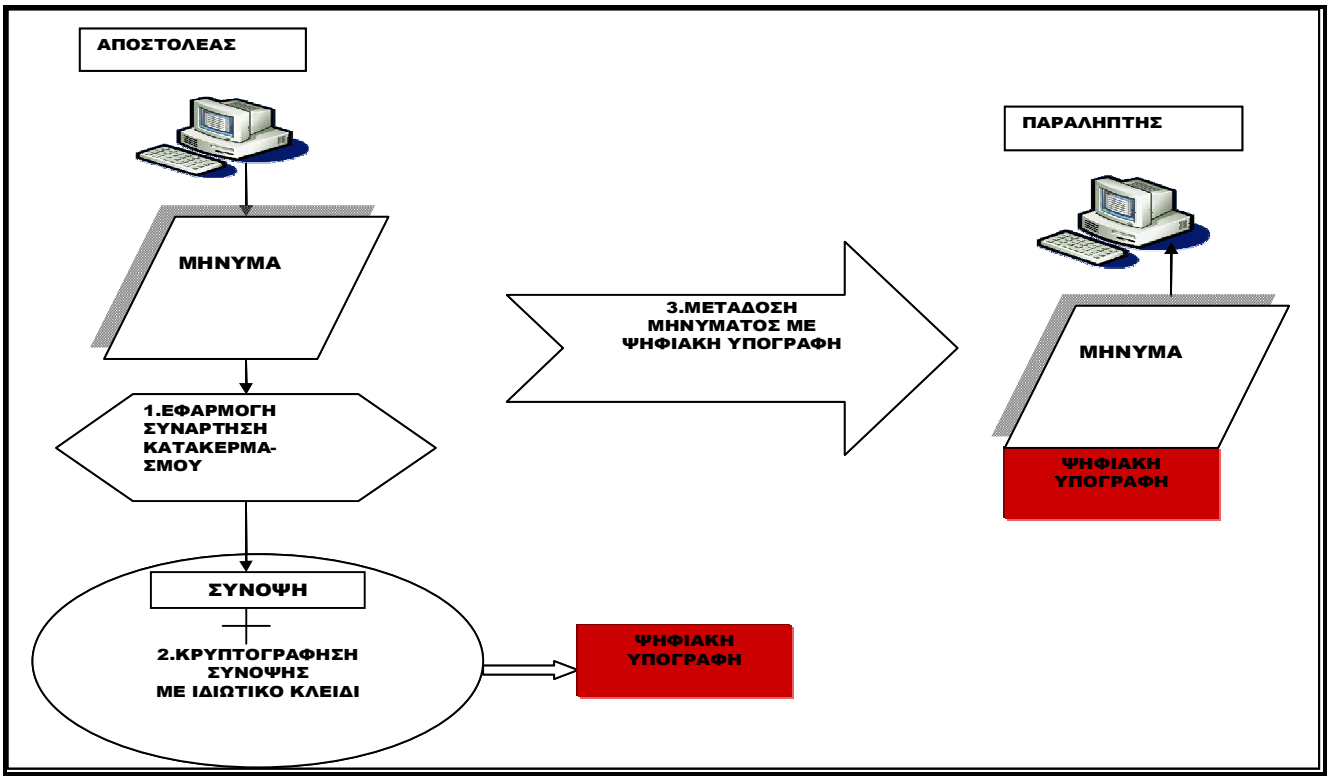
Τέλος, αξίζει να σημειωθεί, ότι για να τεθούν σε εφαρμογή τα παραπάνω και να εκμεταλλευτούμε τα οφέλη που απορρέουν από τη χρήση της ψηφιακής υπογραφής θα πρέπει να ληφθούν υπόψιν ορισμένοι παράγοντες. Πρώτον, θα πρέπει να είμαστε σίγουροι ότι η ψηφιακή υπογραφή έχει εκδοθεί νόμιμα στο όνομα κάποιου χρήστη και ότι αυτός ο χρήστης έδωσε τα πραγματικά του στοιχεία όταν ζήτησε να εκδοθεί η ψηφιακή υπογραφή του. Δημιουργείται η ανάγκη ύπαρξης ενός αξιόπιστου οργανισμού ο οποίος θα πιστοποιεί την ταυτότητα του χρήστη, το οποίο ζήτημα θα αναλυθεί εκτενώς στο επόμενο κεφάλαιο. Δεύτερον, μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. να χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

4.2. Δημιουργία και Επαλήθευση ψηφιακής υπογραφής

Η χρήση της ψηφιακής υπογραφής περιλαμβάνει δύο στάδια: τη δημιουργία/μετάδοση και την επαλήθευσή της. Ακολουθεί μια περιγραφή με τις διαδικασίες που πρέπει να ακολουθήσουν οι χρήστες της ψηφιακής υπογραφής.

Δημιουργία ψηφιακής υπογραφής:

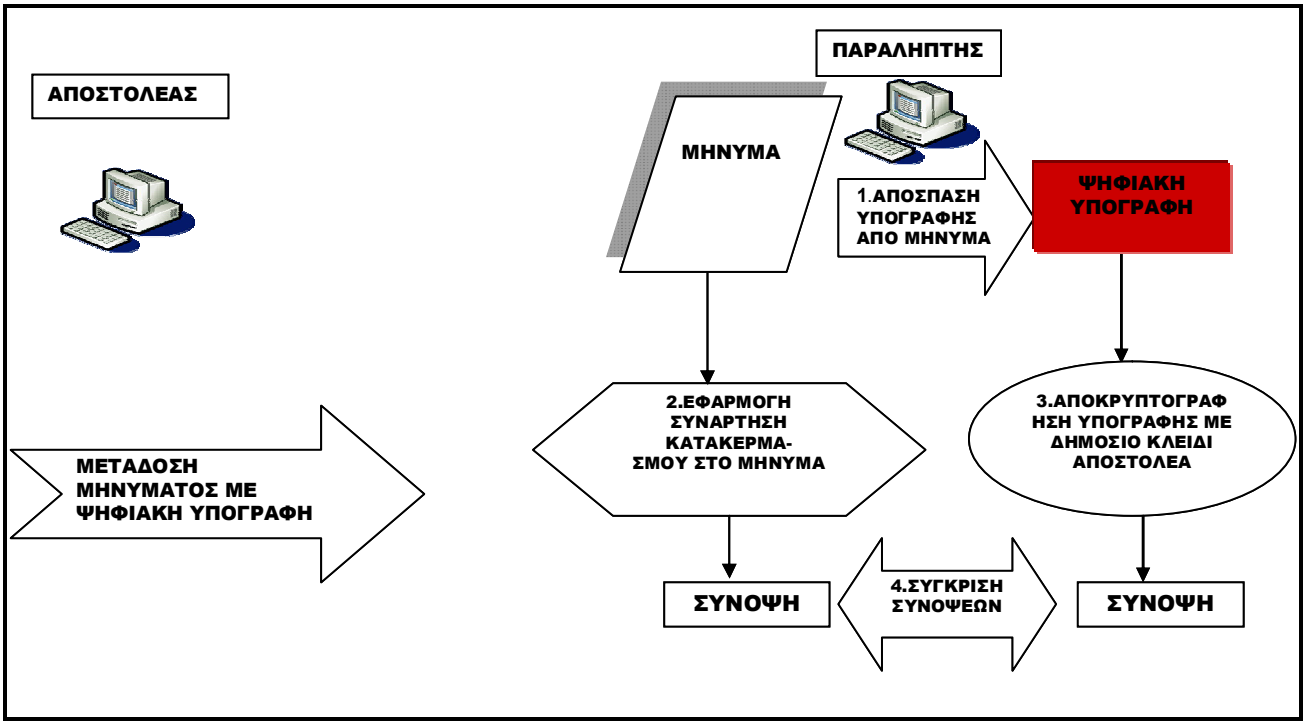
Αρχικά ο αποστολέας δημιουργεί το μήνυμα που επιθυμεί να αποστείλει. Μετά παράγει τη σύνοψη του μηνύματος (message digest) εφαρμόζοντας έναν αλγόριθμο κατακερματισμού ή μια μονόδρομη συνάρτηση σύνοψης (one way hash). Στη συνέχεια, έχοντας στη κατοχή του ένα ζεύγος κλειδιών το οποίο παράχθηκε με τη χρήση ενός αλγόριθμου ασύμμετρου κρυπτοσυστήματος, κρυπτογραφεί τη σύνοψη με το ιδιωτικό του κλειδί. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Τέλος, προσθέτει την κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) στο μήνυμα, το οποίο αποστέλλεται υπογεγγραμμένο στον παραλήπτη μέσω του δικτύου



Εικόνα 5:Απεικόνιση δημιουργίας ψηφιακής υπογραφής

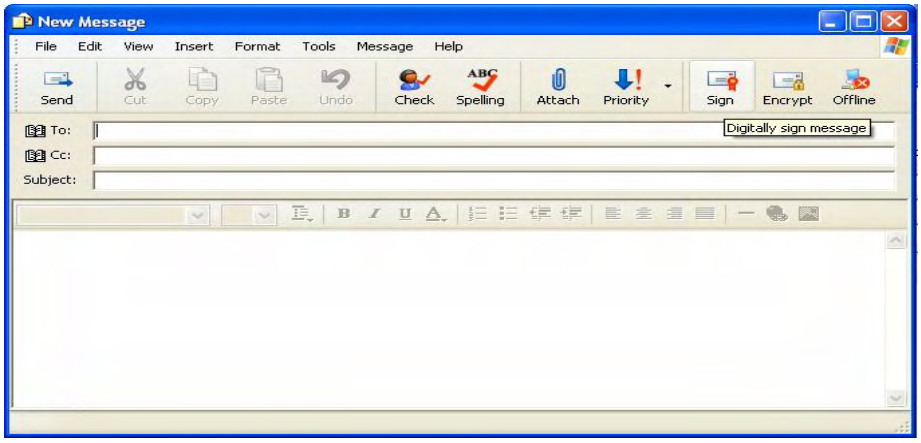
Επαλήθευση ψηφιακής υπογραφής:

Με τη λήψη του μηνύματος ο παραλήπτης απομονώνει τη ψηφιακή υπογραφή. Στη συνέχεια την αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα (με την προϋπόθεση ότι το δημόσιο κλειδί του είναι διαθέσιμο σε όλους, συσχετίζεται με το ιδιωτικό κλειδί και ανήκει σε αυτόν που υπέγραψε ψηφιακά το μήνυμα). Παράλληλα, παράγει τη σύνοψη του μηνύματος εφαρμόζοντας τον ίδιο αλγόριθμο κατακερματισμού ή μονόδρομη συνάρτηση σύνοψης (one way hash) που χρησιμοποίησε ο αποστολέας. Τέλος συγκρίνει τις δύο συνόψεις για να εξετάσει αν είναι ίδιες. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παραχθεί θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί. Αν είναι ίδιες οι συνόψεις, ο παραλήπτης επιβεβαιώνει την αυθεντικότητα του αποστολέα αλλά και την ακεραιότητα του μηνύματος που έλαβε.



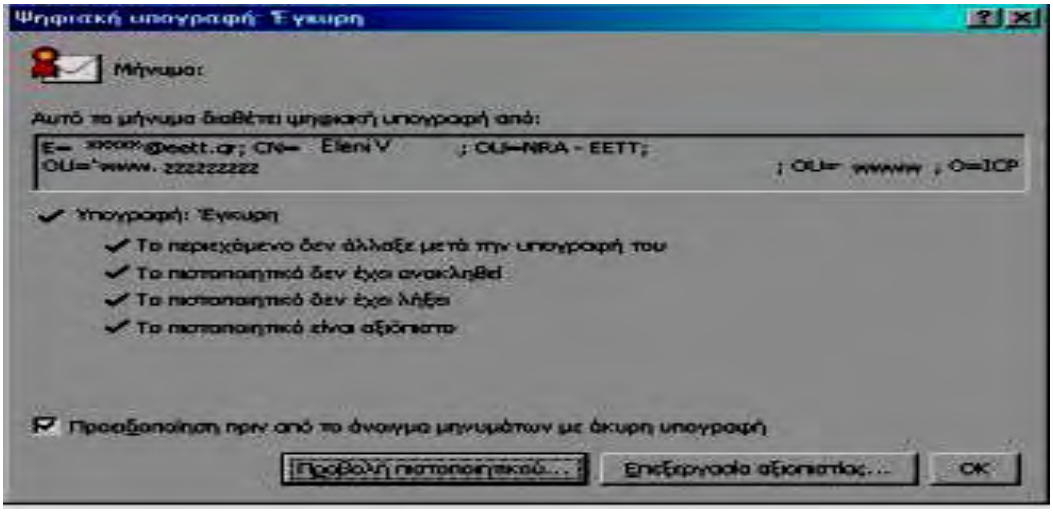
Εικόνα 6:Απεικόνιση επαλήθευσης Ψηφιακής Υπογραφής

Κάθε πρόγραμμα διαχείρισης ηλεκτρονικού ταχυδρομείου δίνει τη δυνατότητα υπογραφής και κρυπτογράφησης μηνυμάτων. Μετά τη δημιουργία του μηνύματος με τη χρήση του κατάλληλου λογισμικού η ψηφιακή υπογραφή συμπεριλαμβάνεται αυτόματα στο μήνυμα. Οι επιλογές του ηλεκτρονικού ταχυδρομείου για να υπογραφεί (Sign) και να κρυπτογραφηθεί (Encrypt) ένα μήνυμα φαίνονται παρακάτω στην **Εικόνα 7 .**Για την κρυπτογράφηση ενός μηνύματος απαιτείται να έχει ο χρήστης το πιστοποιητικό του παραλήπτη αποθηκευμένο στον υπολογιστή για τη χρησιμοποίηση του δημόσιου κλειδί του κατά την αποστολή. Ενεργοποιώντας την επιλογή υπογραφής των μηνυμάτων είναι δυνατή η αποστολή υπογεγραμμένου μηνύματος. Προκειμένου ένας χρήστης να αποστείλλει ένα μήνυμα υπογεγγραμμένο ψηφιακά, θα πρέπει αρχικά να δημιουργήσει ένα μήνυμα το οποίο θα αποθηκεύσει στο ηλεκτρονικό ταχυδρομείο του.



Εικόνα 7: Ένδειξη Sign για υπογραφή μηνύματος

Κατά τη λήψη ενός μηνύματος υπογεγραμμένου ψηφιακά, τα προγράμματα διαχείρισης ηλεκτρονικού ταχυδρομείου μπορούν να αναγνωρίσουν ότι υπάρχει ψηφιακή υπογραφή στο μήνυμα και εμφανίζουν στον χρήστη την ένδειξη υπογεγγραμμένο (signed by:). Έπειτα ο αποδέκτης του μηνύματος μπορεί επαληθεύσει ψηφιακά το υπογεγγραμμένο μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα. Το δημόσιο κλειδί του αποστολέα βρίσκεται στο ψηφιακό πιστοποιητικό του. Έτσι ο παραλήπτης πρέπει να αναζητήσει το πιστοποιητικό του και να το αποθηκεύσει στον υπολογιστή του. Με αυτό τον τρόπο μπορεί να ελέγχει την εγκυρότητα της ψηφιακής υπογραφής ανατρέχοντας στην υπηρεσία που εξέδωσε το πιστοποιητικό ψηφιακό πιστοποιητικό του αποστολέα για να επιβεβαιώσει την εγκυρότητα του πιστοποιητικού. Εάν το πιστοποιητικό είναι αξιόπιστο και δεν έχει ανακληθεί ή λήξει τότε θεωρείται και η υπογραφή έγκυρη. Τότε εξασφαλίζεται και η πιστοποίηση της ταυτότητας του αποστολέα, η ακεραιότητα του περιεχομένου του μηνύματος καθώς και το ότι ο αποστολέας δεν μπορεί να αποποιηθεί την αποστολή. Η **Εικόνα 8** δείχνει τον έλεγχο της εγκυρότητας της ψηφιακής υπογραφής που έχει το μήνυμα.



Εικόνα 8:Ένδειξη ψηφιακής υπογραφής με πιστοποιητικό (http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html)

Σε περίπτωση που για το υπογεγραμμένο μήνυμα, δεν μπορεί να επαληθευτεί το πιστοποιητικό του αποστολέα, εμφανίζεται η ένδειξη (invalid signature) η οποία φαίνεται στη **Εικόνα 9**. Η αιτίες μπορεί να είναι ότι ο παραλήπτης δεν εμπιστεύεται άρα και δεν έχει αποδεχτεί την Αρχή Πιστοποίησης που εξέδωσε το πιστοποιητικό του αποστολέα, ή ότι το πιστοποιητικό του έχει λήξει ή έχει ανακληθεί.

Εικόνα 9: Ένδειξη μη έγκυρη ψηφιακή υπογραφή

4.3. Πρότυπα Ψηφιακών Υπογραφών

Οι ψηφιακές υπογραφές είναι πολύ σημαντικές στην απόδειξη της ταυτότητας του αποστολέα και του χρήστη. *Για αυτό η Αμερικανική (U.S) κυβέρνηση αποφάσισε να καθιερώσει τα πρότυπα σχετικά με τις λειτουργίες και την αποδεκτή χρήση τους. Το 1991, το Εθνικό Ινστιτούτο Τυποποίησης και Τεχνολογίας (NIST) πρότεινε τα ομοσπονδιακά πρότυπα αποκαλούμενα Πρότυπα Ψηφιακής Υπογραφής (Digital Signature Standard-DSS). Η Αμερικανική Ομοσπονδιακή κυβέρνηση απαιτεί τα τμήματα της να χρησιμοποιούν τους αλγόριθμους DSA, RSA, SHA και τον αλγόριθμο Ελλειπτικής Καμπύλης (ECDSA).***[S. Harris, (2008), 8, 725]**

Στο DSS περιγράφει τους αλγόριθμους Digital Signature Algorithm (DSA) και RSA και καλούνται πλέον ως οι πιο διαδεδομένοι χρησιμοποιούμενοι αλγόριθμοι ψηφιακών υπογραφών. Ο DSA καθίσταται στους αλγόριθμους ασύμμετρης κρυπτογραφίας και χρησιμοποιεί κατά την υλοποίηση του διακριτούς λογάριθμους στη δυσκολία των οποίων βασίζεται και αντοχή του έναντι των επιθέσων. Ωστόσο η χρήση του αλγορίθμου DSA περιορίζεται στις ψηφιακές υπογραφές ενώ ο αλγόριθμος RSA (που αναλύθηκε στο Κεφάλαιο 3) χρησιμοποιείται, εκτός των ψηφιακών υπογραφών, στη κρυπτογράφηση και την εξασφάλιση της ασφαλούς διανομής των κλειδιών της συμμετρικής κρυπτογραφίας. Τέλος, η συνάρτηση σύνοψης SHA-1 όπως είδαμε στο Κεφάλαιο 3 διασφαλίζει την ακεραιότητα (integrity) του μηνύματος **[1] [12]**.

5 *Κεφάλαιο*

ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Όπως μελετήσαμε στο Κεφάλαιο 3, για την αποτελεσματική λειτουργία του ασύμμετρου κρυπτοσυστήματος απαιτείται το ιδιωτικό κλειδί να διατηρείται μυστικό και το δημόσιο κλειδί να είναι γνωστό σε όσους δυνητικά ενδιαφέρονται. Έτσι, οποιοσδήποτε μπορεί να αποστείλει το δημόσιο κλειδί του σε έναν ή περισσότερους χρήστες. Ωστόσο, η διανομή αυτή των δημόσιων κλειδιών προς όλους αποκαλύπτει μία σημαντική αδυναμία διασφάλισης της εμπιστευτικότητας αλλά και της αυθεντικοποίησης του αποστολέα. Μια πιθανή επίθεση, κατά την επικοινωνία σε ένα περιβάλλον όπου ανταλλάσσονται ελεύθερα τα δημόσια κλειδιά, είναι ένας χρήστης να διανείμει το δημόσιο κλειδί του με το όνομα και την ταυτότητα κάποιου άλλου χρήστη (προσποίηση). Σε αυτή τη περίπτωση τα κρυπτογραφημένα μηνύματα δεν θα φτάνουν στο πραγματικό προορισμό τους αλλά θα διαβάζονται από το χρήστη που προσποιείται τον πραγματικό προορισμό. Επίσης, ο επιτιθέμενος θα έχει τη δυνατότητα να υπογράφει και να αυθεντικοποιείται στέλνοντας μηνύματα προσποιούμενος κάποιον άλλο χρήστη. Επομένως, προκύπτει η ύπαρξη ενός ψηφιακού πιστοποιητικού το οποίο θα καθιστά έγκυρη την αντιστοίχιση ενός χρήστη με το δημόσιο κλειδί του, ώστε ο παραλήπτης να πιστοποιεί την ταυτότητα του προσώπου με τον οποίο πραγματοποιεί μια συναλλαγή.

5.1. Ορισμός

Ψηφιακό Πιστοποιητικό είναι ένα ηλεκτρονικό έγγραφο το οποίο περιέχει πληροφορίες για τον κάτοχο του, τον εκδότη του πιστοποιητικού και τις πληροφορίες που αφορούν το περιορισμό της χρήσης του. Οι πληροφορίες αυτές συμπεριλαμβάνονται με το δημόσιο κλειδί ενός προσώπου και βοηθούν τους υπόλοιπους χρήστες να ελέγχουν ότι το κλειδί του ισχύει και είναι γνήσιο. Η εγκυρότητα των στοιχείων που αναγράφονται στο πιστοποιητικό επικυρώνεται από μια **Έμπιστη Τρίτη Οντότητα (Trusted Third Party-TTP)**, η οποία πιστοποιεί την αντιστοιχία μιας (ή περισσότερων) ιδιότητας μιας φυσικής οντότητας στο δημόσιο κλειδί που της ανήκει, υπογράφοντας ψηφιακά το πιστοποιητικό. Επομένως, ένα ψηφιακό πιστοποιητικό επιτρέπει σε κάποιον να συνδυάσει την ψηφιακή υπογραφή με ένα δημόσιο κλειδί και κάτι που τον χαρακτηρίζει ως οντότητα. Με άλλα λόγια, πρόκειται για ένα μηχανισμό ασφαλείας για τα δημόσια κλειδιά και για αυτό αποκαλείται και ως πιστοποιητικό δημόσιου κλειδιού**[47]**.

Η Έμπιστη Τρίτη Οντότητα είναι μια οντότητα που εμπιστεύονται όλοι οι χρήστες στην παροχή υπηρεσιών για ασφαλέστερη επικοινωνία. Παρεμβαίνει αλλά δε συμμετέχει στην επικοινωνία των χρηστών. Ο ρόλος της Έμπιστης Τρίτης Οντότητας είναι να πιστοποιήσει ότι το δημόσιο κλειδί του κάτοχου ενός πιστοποιητικού αντιστοιχεί στο ιδιωτικό του κλειδί και συχνά αναφέρεται ως Πάροχος Υπηρεσιών Πιστοποίησης(Certification Service Provider-CSP). Αυτό σημαίνει ότι το ιδιωτικό κλειδί που ταιριάζει με το δημόσιο κλειδί στο πιστοποιητικό μπορεί να χρησιμοποιηθεί για συγκεκριμένους λόγους όπως οι ψηφιακές υπογραφές, το μη αποποίηση και κρυπτογράφηση μηνυμάτων.

5.2. Λειτουργία Ψηφιακού Πιστοποιητικού

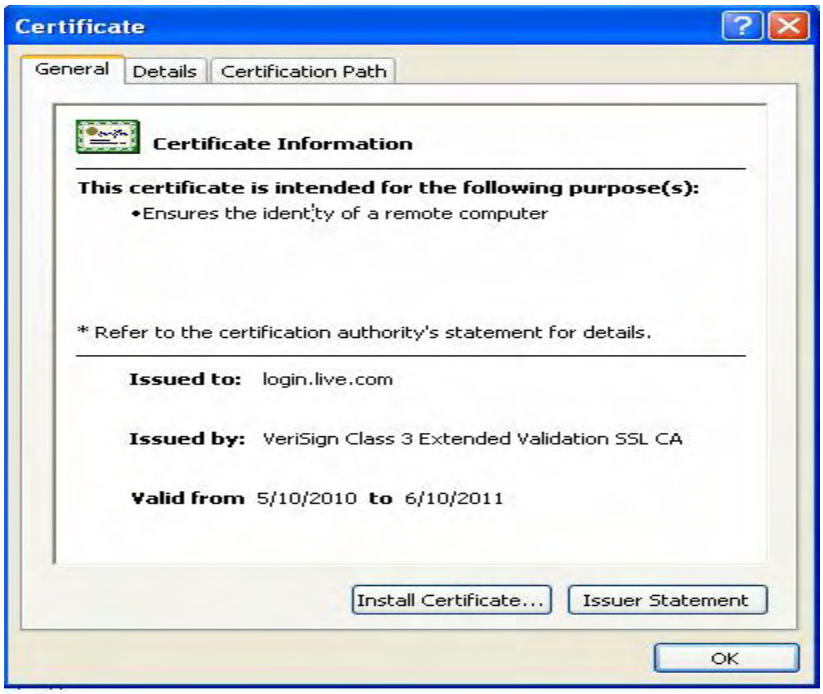
Ένα ψηφιακό πιστοποιητικό μπορεί να εκδοθεί για να πιστοποιήσει ένα φυσικό πρόσωπο ή έναν εξυπηρετητή ή μια άλλη υπηρεσία πιστοποίησης. Το ψηφιακό πιστοποιητικό πιστοποιεί την ταυτότητα του κατόχου του και δίνει τη δυνατότητα σε όσους ενδιαφέρονται να ελέγξουν την εγκυρότητα της.

Για την πραγματοποίηση μιας επικοινωνίας μέσω ηλεκτρονικού ταχυδρομείου μπορούν να χρησιμοποιηθούν τα ψηφιακά πιστοποιητικά. Με την υπογραφή ενός μηνύματος μέσω πιστοποιητικού, αποδεικνύεται στον παραλήπτη η ταυτότητα του αποστολέα (αυθεντικοποίηση και μη-αποποίηση), καθώς και ότι το περιεχόμενο του μηνύματος δεν έχει αλλοιωθεί από κάποιον τρίτο (ακεραιότητα) κατά τη μετάβαση του. Η χρήση της υπογραφής μέσω πιστοποιητικού σε συνδυασμό με τη κρυπτογράφηση του μηνύματος εξασφαλίζει και την εμπιστευτικότητα της πληροφορίας.

Μια άλλη χρήση των ψηφιακών πιστοποιητικών είναι η πλοήγηση σε ασφαλείς δικτυακούς τόπους/ιστοσελίδες. Για να χαρακτηριστούν ασφαλείς κάποιες ιστοσελίδες χρησιμοποιούν ψηφιακά

πιστοποιητικά εξυπηρετητών τα οποία πιστοποιούν τη ταυτότητα του διαχειριστή-κατόχου της ιστοσελίδας. Επίσης, με ενεργοποίηση του πρωτοκόλλου SSL και με τεχνολογίες κρυπτογράφησης εξασφαλίζουν την εμπιστευτικότητα των μεταδιδόμενων πληροφοριών. Έτσι ώστε σε περίπτωση μεταβίβασης στοιχείων από τους χρήστες προς τους ιστότοπους να μην αποκαλύπτονται σε τρίτους. Οι ενδείξεις που ενημερώνουν τον χρήστη για την ύπαρξη ψηφιακού πιστοποιητικού και χρήση ασφαλούς πρωτοκόλλου επικοινωνίας είναι πρώτον η εμφάνιση στη διεύθυνση της ιστοσελίδας **https** αντί για **http** και δεύτερον η εμφάνιση ενός εικονιδίου κλειδωμένης κλειδαριάς.

Στη παρακάτω **Εικόνα 10** παρουσιάζεται ένα απλό παράδειγμα πιστοποιητικού που εξέδωσε η VeriSign**[9]** για μια υπηρεσία όπου πραματοποιείται η εγγραφή ενός χρήστη με την αποστολή των στοιχείων του. Ο σκοπός του πιστοποιητικού αυτού είναι να βεβαιώσει την ταυτότητα της υπηρεσίας έτσι ώστε οι χρήστες να μπορούν να την εμπιστευτούν. Επιπλέον, αναγράφεται και η διάρκεια ισχύος του πιστοποιητικού για την ενημέρωση του χρήστη για την εγκυρότητα του. Στην επιλογή Details εμφανίζονται τα περιεχόμενα του πιστοποιητικά τα οποία αναλύονται στην αμέσως επόμενη ενότητα.



Εικόνα 10:Προβολή Πιστοποιητικού (Επιλογή General)

Ο χρήστης που επιθυμεί να αποκτήσει ψηφιακό πιστοποιητικό παρουσιάζει το δημόσιο κλειδί του στον Πάροχο Υπηρεσιών Πιστοποίησης με έναν αξιόπιστο τρόπο. Ο Πάροχος είναι αρμόδιος να παράγει, να αποθηκεύει και να διανέμει, το υπογεγγραμμένο με το δημόσιο κλειδί του, το πιστοποιητικό του χρήστη. Αν οποιοσδήποτε άλλος χρήστης επρόκειτο να πραγματοποιήσει μια συναλλαγή με χρήστη κάτοχο πιστοποιητικού επιβεβαιώνει ότι τα στοιχεία του είναι σωστά διότι εμπιστεύεται τον Πάροχο που τα πιστοποιεί. Σε περίπτωση που ένας χρήστης δεν εμπιστεύεται τον

Πάροχο που εξέδωσε ένα πιστοποιητικό και ο Πάροχος αυτός έχει ήδη πιστοποιηθεί από κάποιον άλλον Πάροχο τότε ο χρήστης μπορεί να εμπιστευτεί τον πρώτο Πάροχο.

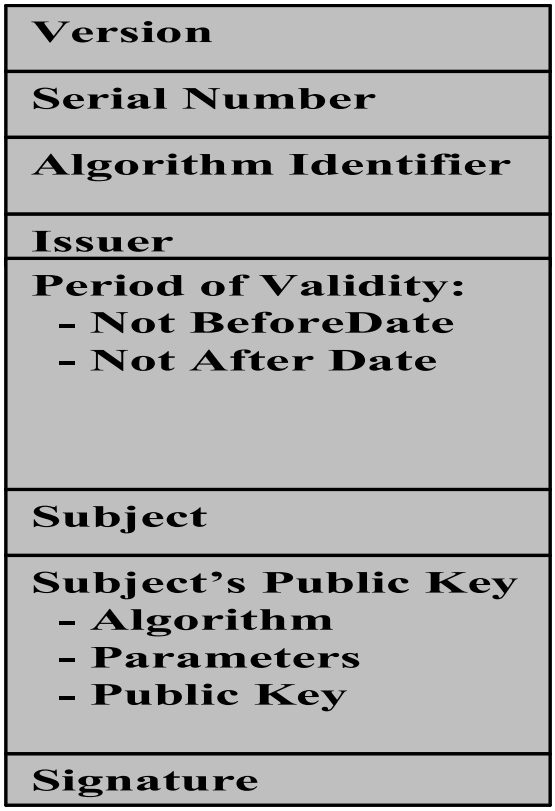
Επιπρόσθετα, η ψηφιακή υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης μπορεί να επαληθεύσει, χρησιμοποιώντας το δημόσιο κλειδί του Παρόχου, για το οποίο (δημόσιο κλειδί) ένας άλλος Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει εκδώσει πιστοποιητικό κ.λπ.

5.3. Μορφή Ψηφιακού Πιστοποιητικού

Ένα ψηφιακό πιστοποιητικό αποτελείται από τα παρακάτω **Βασικά Μέρη:** τα **Αναγνωριστικά Χαρακτηριστικά** του πιστοποιητικού**,**την **Περίοδος Ισχύος** του πιστοποιητικού**,** τα **Στοιχεία του Εκδότη,** τα **Στοιχεία του Χρήστη** που πιστοποιείται**,** το **Δημόσιο κλειδί** του χρήστη,τις **Επεκτάσεις,** όπου αναφέρονται κυρίως οι επιτρεπόμενες χρήσεις των κλειδιών του χρήστη, και την **Υπογραφή του Εκδότη[1]**. Οι πληροφορίες που περιέχονται σε όλη τη δομή του πιστοποιητικού υπογράφονται ψηφιακά από τον Πάροχο Υπηρεσιών Πιστοποίησης με σκοπό να βεβαιώσει ότι οι έχουν πιστοποιηθεί από αυτόν και είναι έγκυρες. Η ψηφιακή υπογραφή δεν βεβαιώνει στην αυθεντικότητα του πιστοποιητικού αλλά μόνο ότι οι υπογεγραμμένες πληροφορίες ταυτότητας πηγαίνουν είναι συνδεδεμένες με το δημόσιο κλειδί.

5.3.1. Πρότυπο Μορφοποίησης Ψηφιακού Πιστοποιητικού(X.509)

Η μορφή και τα δεδομένα που θα εμπεριέχονται σε ένα ψηφιακό πιστοποιητικό διαμορφώνονται με βάση κάποιο πρότυπο. Το πιο διαδεδομένο πρότυπο μορφοποίησης πιστοποιητικού είναι το **ISO/ITU-T X.509**. Το ευρύτερα γνωστό και χρησιμοποιούμενο είναι η τρίτη έκδοση του ITU (IETF) X.509v3 ενώ οι προηγούμενες εκδόσεις είναι το X.509v1 και το X.509v2. Σύμφωνα με το πρότυπο, υπάρχουν συνολικά δέκα πεδία που συμπληρώνονται σε ένα ψηφιακό πιστοποιητικό από τα οποία τα έξι είναι υποχρεωτικά και τα τέσσερα προαιρετικά. Τα υποχρεωτικά πεδία είναι: αύξων αριθμός (**Serial Number**), το προσδιοριστικό αλγορίθμου υπογραφών πιστοποιητικών (**Algorithm Identifier**), το όνομα εκδοτών πιστοποιητικών (**Issuer**), η περίοδος ισχύος πιστοποιητικών (**Period of Validity**),το όνομα υποκειμένου (**Subject**) όπου υποκείμενο είναι ο χρήστης που πιστοποιείται και που ελέγχει το αντίστοιχο ιδιωτικό κλειδί και το δημόσιο κλειδί (**Subject's Public Key**) μαζί με τον αλγόριθμο και τις παραμέτρους του που χρησιμοποιήθηκε για τη παραγωγή του. Τα τέσσερα προαιρετικά πεδία είναι: αριθμός έκδοσης, δύο μοναδικά προσδιοριστικά, και οι επεκτάσεις. Αυτά τα προαιρετικά πεδία εμφανίζονται μόνο στην έκδοση 2 και 3**[11]**. Στην **Εικόνα 11** φαίνεται η μορφή των δεδομένων που αναφέρονται σε ένα πιστοποιητικό με τα υποχρεωτικά πεδία σύμφωνα με το πρότυπο X.509.



Εικόνα 11:Μορφή δεδομένων πρότυπου X.509

Το σύνολο των πεδία που μπορει να υπάρχουν σε ένα πιστοποιητικό καθώς και τι συμπεριλαμβάνει κάθε πεδίο είναι τα εξής:

- **Έκδοση (Version).** Το πεδίο έκδοσης περιγράφει τη σύνταξη του πιστοποιητικού. Όταν το πεδίο έκδοσης παραλείπεται, το πιστοποιητικό ανάφέρεται στην αρχική έκδοση 1. Η έκδοση 1 δεν περιλαμβάνει στα πιστοποιητικά τα μοναδικά προσδιοριστικά ή τις επεκτάσεις. Όταν το πιστοποιητικό περιλαμβάνει τα μοναδικά προσδιοριστικά αλλά όχι τις επεκτάσεις, το πεδίο έκδοσης δείχνει την έκδοση 2. Όταν το πιστοποιητικό περιλαμβάνει τις επεκτάσεις, όπως σχεδόν όλα τα σύγχρονα πιστοποιητικά, το πεδίο έκδοσης δείχνει την έκδοση 3.
- **Αύξων αριθμός (Serial number).** Ο αύξων αριθμός είναι ένας ακέραιος αριθμός που ορίζεται από τον εκδότη πιστοποιητικών σε κάθε ένα πιστοποιητικό. Ο αύξων αριθμός πρέπει να είναι μοναδικός για κάθε πιστοποιητικό που παράγεται από έναν εκδότη.Ο συνδυασμός του ονόματος και του αύξοντος αριθμού εκδότη μπορεί να προσδιορίζει μοναδικά οποιοδήποτε πιστοποιητικό.
- **Υπογραφή (Signature).** Το πεδίο υπογραφών προσδιορίζει ποιος ψηφιακός αλγόριθμος υπογραφών (π.χ., DSA με sha-1 ή RSA) χρησιμοποιήθηκε για το πιστοποιητικό.
- **Εκδότης (Issuer).** Το πεδίο αυτό περιέχει το Διακεκριμένο X.500 όνομα του Πάροχου Υπηρεσιών Πιστοποίησης που παρήγαγε το πιστοποιητικό.
- **Ισχύς (Validity).** Το πεδίο ισχύος δηλώνει τις ημερομηνίες κατά τις οποίες το πιστοποιητικό είναι έγκυρο με τη μορφή Από-Εώς.

- **Υποκείμενο (Subject).** Υποκείμενο χαρακτηρίζεται ο χρήστης κάτοχος του ιδιωτικού κλειδιού που το αντίστοιχο δημόσιο κλειδί βρίσκεται σε αυτό το πιστοποιητικό.Το πεδίο αυτό περιέχει το Διακεκριμένο Όνομα του κατόχου Υποκειμένου.

- **Πληροφορίες για το Δημόσιο κλειδί του υποκειμένου (Subject public key information).** Το πεδίο αυτό περιέχει τις δημόσιες παράμετροι και το προσδιοριστικό του αλγορίθμου. Το δημόσιο κλειδί σε αυτό το πεδίο μαζί με τις παραμέτρους αλγορίθμου, χρησιμοποιείται για να ελέγξει τις ψηφιακές υπογραφές. Εάν το Υποκείμενο πιστοποιητικών είναι ένας Πάροχος, το δημόσιο κλειδί του χρησιμοποιείται για να ελέγχθεί η ψηφιακή υπογραφή του σε ένα πιστοποιητικό.

- **Τύπος Υποκειμένου (Subject type).** Αυτό το πεδίο δείχνει εάν το υποκείμενο είναι κάποιος Πάροχος ,ένα φυσικό πρόσωπο ή ένας εξυπηρετητής.

- **Ονόματα και πληροφορίες ταυτότητας (Names and identity information)**. Αυτό το πεδίο βοηθά στην επιβεβαίωση των ενδιαφερόμενων ότι η αντιστοίχιση του δημόσιου κλειδιού έγινε στο νόμιμο πρόσωπο. π.χ., είναι «alice@ucg.gr» και «C=GR, O=GR university, CN=Alice Adams»

- **Προσδιοριστικό εκδότη και υποκειμένου (Issuer unique ID** and **subject unique ID).** Αυτά τα πεδία περιέχουν τα προσδιοριστικά, και εμφανίζονται μόνο στα πιστοποιητικά των στην εκδόσεων 2 ή 3.

- **Επεκτάσεις (Extensions).** Αυτό το προαιρετικό πεδίο εμφανίζεται μόνο στην έκδοση 3 πιστοποιητικών. Εάν αυτό το πεδίο περιέχει μια ή περισσότερες επεκτάσεις πιστοποιητικών. Οι κοινές επεκτάσεις πιστοποιητικών έχουν καθοριστεί από το ISO **[26]** και το ANSI για να απαντήσουν στις ερωτήσεις που δεν ικανοποιούν από τους γνωστούς τομείς. Οι επεκτάσεις επιτρέπουν στην υπηρεσία πιστοποίησης να περιλάβουν τις πληροφορίες που δεν υποστηρίζονται από τα βασικά πεδία στα πιστοποιητικά.

- **Ιδιότητες Κλειδιού (Key attributes).** Αυτό το πεδίο διευκρινίζει τις επιτρεπόμενες χρήσεις των δημόσιων κλειδιών δηλαδή εάν έχει την ιδιότητα να χρησιμοποιηθεί για να ελέγξει μια ψηφιακή υπογραφή, για κρυπτογράφηση κτλ.

- **Πληροφορίες Πολιτικής Πιστοποίησης (Certification Policy information).** Αυτό το πεδίο βοηθά τους χρήστες να καθορίσουν εάν το πιστοποιητικό ενός άλλου χρήστη είναι έμπιστογια τις συναλλάγες που πραγματοποιεί και άλλους κανόνες που αφορούν την οργάνωση της υπηρεσία ςπου εξέδωσε το πιστοποιητικό.

5.4. Κατηγοριοποίηση Πιστοποιητικών

Τα ψηφιακά πιστοποιητικά διαδρίνονται από τον τύπο του υποκειμένου (φυσικό πρόσωπο, εξυπηρετητής, υπηρεσία) στο οποίο εκδίδονται και τις χρήσεις για τις οποίες προορίζονται.Έτσι τα πιστοποιητικά κατηγοριοποιούνται ως εξής:

1. Απλό Προσωπικό Πιστοποιητικό (Simple Personal Certificate)

Το Απλό Προσωπικό Πιστοποιητικό είναι ένα πιστοποιητικό ταυτοποίησης του κατόχου του. Κατασκευάζεται και αποθηκεύεται ασφαλώς από τον Πάροχο Υπηρεσιών Πιστοποίησης μαζί με τα ζεύγος κλειδιών που σχετίζονται με το πιστοποιητικό. Το ιδιωτικό κλειδί που αντιστοιχεί σε πιστοποιητικό τέτοιου τύπου δεν αποκαλύπτεται σε τρίτους και φυλάσσεται ασφαλώς από τον χρήστη ο οποίος μπορεί να το μεταφέρει σε επιλεγμένο αποθηκευτικό μέσο τηρώντας τις βασικές απαιτήσεις ασφάλειας (χρήση κωδικού ασφαλείας). Οι προτεινόμενες χρήσεις του απλού προσωπικού πιστοποιητικού είναι:η Ψηφιακή Υπογραφή, η Κρυπτογράφηση και το Ασφαλές ηλεκτρονικό ταχυδρομείο.

2. Αναγνωρισμένο Προσωπικό Πιστοποιητικό (Qualified Personal Certificate).

Το Αναγνωρισμένο Προσωπικό Πιστοποιητικό είναι ένα πιστοποιητικό ταυτοποίησης του κατόχου του όμως διαφοροποιείται από το Απλό Προσωπικό Πιστοποιητικό για δύο λόγους.Πρώτον (Σύμφωνα με την **Οδηγία 99/93/ΕΚ** που ενσωματώθηκε στο ελληνικό δίκαιο με το **ΠΔ 150/2001**) για την εξασφάλιση του απαιτούμενο επιπέδου ασφάλειας τα ιδιωτικά κλειδιά (‘δεδομένα δημιουργίας υπογραφής’) θα πρέπει αποθηκεύονται προστατευμένα σε ασφαλές μέσα (έξυπνες κάρτες). Δεύτερον τα κλειδιά που αντιστοιχούν στον χρήστη δημιουργούνται είτε από τον ίδιο τον χρήστη είτε από τον Πάροχο με τον τελευταίο να εγγυάται για την προστασία τους. Οι προτεινόμενες χρήσεις του απλού προσωπικού πιστοποιητικού είναι:η ψηφιακή υπογραφή, η κρυπτογράφηση και το ασφαλές ηλεκτρονικό ταχυδρομείο.

3. Πιστοποιητικό για Εξυπηρετητές (Server Certificate)

Το πιστοποιητικό αυτό εκδίδεται για ταυτοποίηση του εξυπηρετητή μιας ιστοσελίδας έτσι ώστε να θεωρείται έμπιστη από τους επισκέπτες της. Ωστόσο, το πιστοποιητικό εκδίδεται στο όνομα του διαχειριστή της συσκευής. Οι προτεινόμενες χρήσεις του είναι η κρυπτογραφημένη επικοινωνία εξυπηρετητή-πελάτη με χρήση πρωτοκόλλου SSL, η αυθεντικοποίηση εξυπηρέτη και η ανταλλαγή κλειδιών.

4. Πιστοποιητικό για υφιστάμενες Υπηρεσίες Πιστοποίησης(Subordinate Service Certificate)

Πιστοποιητικά εκδίδονται επίσης και για υφιστάμενες υπηρεσίες πιστοποίησης οι οποίες με τη σειρά τους εκδίδουν πιστοποιητικά για τελικούς χρήστες. Οι υπηρεσίες πιστοποίησης που έχουν

πιστοποιηθεί έχουν την υποχρέωση να συμμορφώνονται με την κανόνες και τους όρους που έχει θέσει α αρχική υπηρεσία που την έχει πιστοποιήσει όσον αφορά τις υπηρεσίες που προσφέρουν. Με αυτό τον τρόπο δημιουργείται μία ιεραρχική σχέση πιστοποίηση με διαφορετικές αρμοδιότητες ενώ ο τελικός χρήστης αρκεί να εμπιστεύεται μόνο την Κεντρική Υπηρεσία Πιστοποίησης. Οι χρήσεις των πιστοποητικών αυτών είναι: η υπογραφή των πιστοποιητικών και το ασφαλές ηλεκτρονικό ταχυδρομείο.

6 *Κεφάλαιο*

ΑΣΦΑΛΕΣ ΠΡΩΤΟΚΟΛΛΟ ΕΠΙΚΟΙΝΩΝΙΑΣ (SSL)

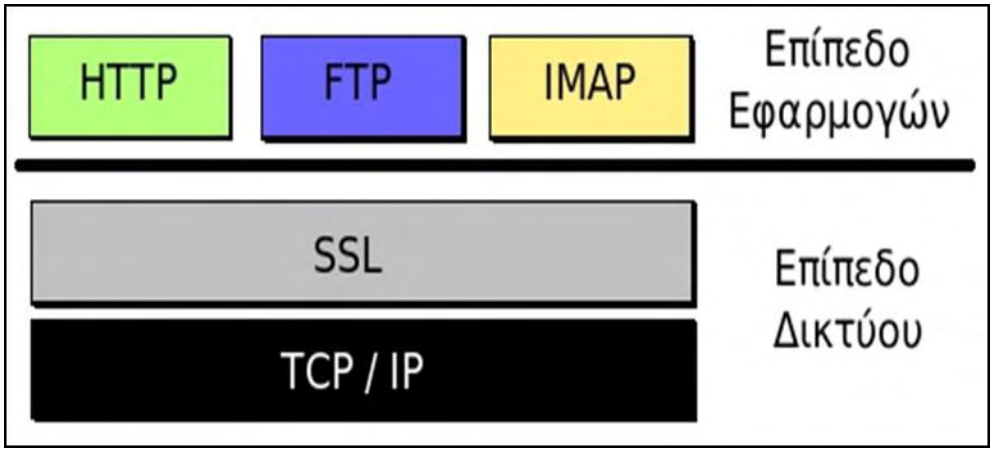
Το **πρωτόκολλο SSL (Secure Sockets Layer)** σχεδιάστηκε από την εταιρεία Netscape για να παρέχει να παρέχει κρυπτογραφική ασφάλεια κατά την μετάδοση προσωπικών ή ευαίσθητων δεδομένων στο διαδίκτυο. Η πρώτη έκδοση v.1.0 χρησιμοποιήθηκε για τις εσωτερικές ανάγκες της Netscape. Με την δεύτερη έκδοση v.2.0 το πρωτόκολλο SSL ενσωματώθηκε στις εκδόσεις v.1.0 και v.2.0 του Netscape Navigator**[2]**. Ωστόσο, λόγω των πολλών περιορισμών που έθετε η έκδοση v.2.0. αναβαθμίστηκε σε SSL v.3.0 Η έκδοση 3.0 του πρωτοκόλλου αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security). Το Internet draft που προσδιορίζει τη τελευταία έκδοση v.3.0 δημοσιεύτηκε το 1996**[45]**.

Η αρχιτεκτονική τοποθέτηση του SSL είναι πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP (email) που φαίνονται στην **Εικόνα 12**. Το SSL στρωματοποιείται ανάμεσα στην εφαρμογή HTTP και στο επίπεδο δικτύου TCP/IP, ενεργώντας σαν ένα ξεχωριστό πρωτόκολλο ασφαλείας.Το κύριο πλεονέκτημα του SSL είναι ότι λειτουργεί για κάθε είδους εφαρμογή που βρίσκεται στο επίπεδο εφαρμογών.Το SSL λαμβάνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε. Ουσιαστικά η λειτουργία του SSL είναι η δημιουργία μιας ασφαλούς σύνδεσης μεταξύ δύο συσκευών μέσω του διαδικτύου χρησιμοποιώντας μεθόδους κρυπτογράφησης. Οι κρυπτογραφικοί αλγόριθμοι που υποστηρίζονται από το

πρωτόκολλο είναι οι εξής: DES-Data Encryption Standard, Triple-DES, DSA - Digital Signature Algorithm, KEA - Key Exchange Algorithm, MD5 - Message Digest, RC2/RC4, RSA, SHA-1 - Secure Hash Algorithm.

- **IP (Internet Protocol):** Το πρωτόκολλο που είναι υπεύθυνο για την δρομολόγηση των μηνυμάτων διαμέσου των δικτύων από την πηγή στον προορισμό.
- **Το TCP (Transmission Control Protocol):** Στηρίζεται στις υπηρεσίες του IP και βεβαιώνει ότι η επικοινωνία είναι αξιόπιστη.
- **HTTP (Hypertext Transfer Protocol):** Κατανοεί τις λεπτομέρειες της διεπαφής ανάμεσα στους φυλλομετρητές Ιστού και τους εξυπηρετητές.

.



Εικόνα 12:Θέση λειτουργίας Πρωτοκόλλου SSL (http://el.wikipedia.org/wiki/SSL)

6.1. Χαρακτηριστικά SSL

Το πρωτόκολλο SSL εμπεριέχει δύο υπό-πρωτόκολλα:

- **Το Πρωτόκολλο Καταγραφής SSL (SSL record protocol):** Καθορίζει τη μορφή με την οποία αναμεταδίδονται τα δεδομένα κάνοντας χρήση του κατακερματισμού και της κρυπτογράφησης. Παρέχει αυθεντικοποίηση, εμπιστευτικότητα και ακεραιότητα.
- **Το Πρωτόκολλο Χειραψίας SSL (SSL Handshake protocol):** Παρέχει υπηρεσίες αυθεντικοποίησης και ανταλλαγής κλειδιών. Σκοπός του είναι να καθιερώσει όλες τις παραμέτρους που θα χρησιμοποιηθούν για την ασφάλεια, όπως τα πρωτόκολλα και τις μεθόδους κρυπτογράφησης, και στη συνέχεια χρησιμοποιεί το πρωτόκολλο καταγραφής για την πραγματοποίηση ανταλλαγής μιας σειράς μηνυμάτων μεταξύ του εξυπηρετητή και του εξυπηρετούμενο.

Το SSL ικανοποιεί τις ακόλουθες απαιτήσεις ασφάλειας:

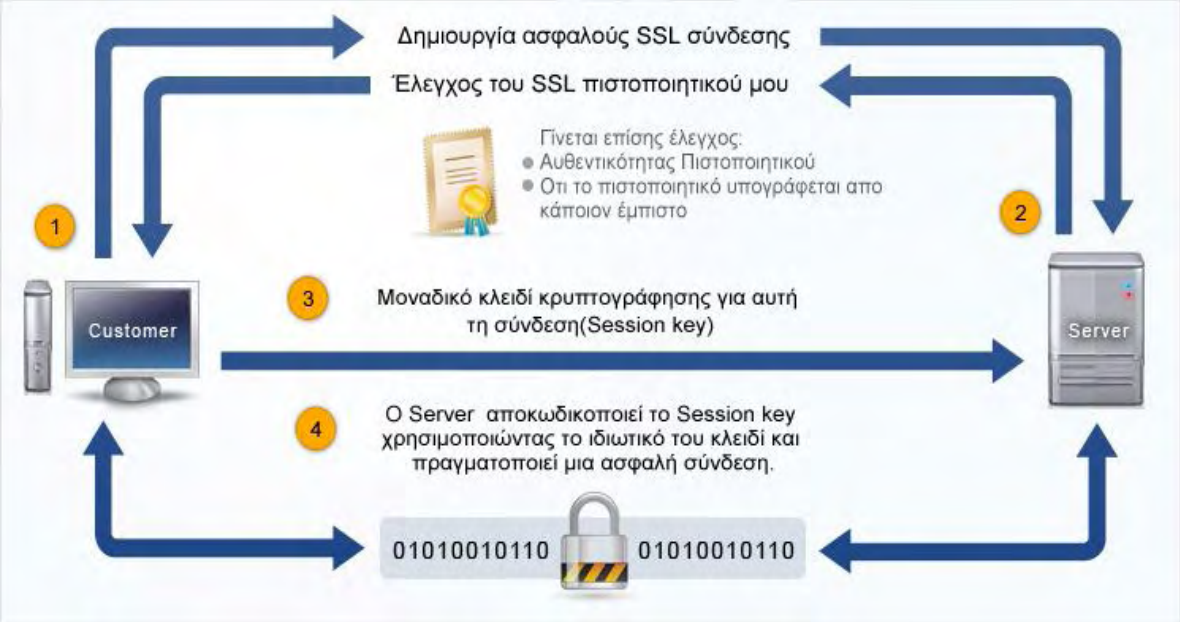
- Αυθεντικοποίηση των δύο άκρων της σύνδεσης με τη χρήση ασύμμετρης κρυπτογράφησης.
- Εμπιστευτικότητα των μεταδιδόμενων πληροφοριών εφόσον κατά το πρωτόκολλο χειραψίας καθορίστηκε ένα κλειδί συνόδου (session key).
- Έλεγχος της ακεραιότητας των μεταδιδόμενων πληροφοριών.

6.2. Τρόπος Λειτουργίας SSL

Οι ιστοσελίδες που είναι κάτοχοι ψηφιακών πιστοποιητικών εξυπηρετητών χρησιμοποιούν το πρωτόκολλο ασφαλείας SSL για να προσφέρει στους ηλεκτρονικούς επισκέπτες της κρυπτογραφημένη συνομιλία για την ενίσχυση της εμπιστοσύνης του επισκέπτη προς αυτήν. Ο τρόπος που λειτουργεί το πρωτόκολλο SSL περιγράφεται ακολούθως και απεικονίζεται στην **Εικόνα 13.**

1. Αρχικά ο χρήστης (εξυπηρετούμενος) στέλνει από τον υπολογιστή του αίτημα στο εξυπηρέτη της ιστοσελίδας για τη δημιουργία ασφαλούς σύνδεσης προκειμένου να πραγματοποιηθεί κρυπτογραφημένη SSL επικοινωνία.
2. Ο εξυπηρετητής στέλνει το ψηφιακό του πιστοποιητικό στον εξυπηρετούμενο για τη αυθεντικοποίηση της ιστοσελίδας το οποίο περιέχει το δημόσιο κλειδί του.Η αυθεντικότητα του εξυπηρέτη εξασφαλίζεται από την Έμπιστη Τρίτη Οντότητα που υπογράφει το πιστοποιητικό του.
3. Ο υπολογιστής του εξυπηρετούμενου, χρησιμοποιεί το δημόσιο κλειδί για να κρυπτογραφήσει με αυτό το κλειδί συνόδου(session key). Το κλειδί συνόδου θα χρησιμοποιηθεί μόνο για τη συγκεκριμένη σύνδεση.
4. Ο εξυπηρέτης χρησιμοποιεί το ιδιωτικό του κλειδί προκειμένου να αποκρυπτογραφήσει το κλειδί συνόδου και να πραγματοποιήσει μια ασφαλής σύνδεση.

Με αυτό τον τρόπο, στη συνέχεια όλα τα δεδομένα που θα μεταδοθούν σε αυτή τη σύνδεση θα κρυπτογραφούνται και θα αποκρυπτογραφούνται με το κοινό μυστικό κλειδί (κλειδί συνόδου) που μοιράστηκε ο εξυπηρετητής με τον εξυπηρετούμενο.Επομένως εδώ συναντήσαμε έναν συνδυασμό ορισμένων μεθόδων που αναλύθηκαν παραπάνω. Η χρήση ψηφιακών πιστοποιητικών για τη μεταβίβαση του δημόσιου κλειδιού, η χρήση κρυπτογραφίας δημόσιου κλειδιού για τη μεταβίβαση του κλειδιού συνόδου και τέλος η χρήση συμμετρικής κρυπτογραφίας για τη κρυπτογράφηση και αποκρυπτογράφηση των μεταδιδόμενων δεδομένων.



Εικόνα 13:Τρόπος λειτουργίας Πρωτοκόλλου SSL
(http://www.tophost.gr/files/images/HOW-SSL-WORKS.jpg)

Στη περίπτωση αυτή που περιγράφηκε παραπάνω αυθεντικοποιήθηκε μόνο ο εξυπηρετητής. Κάποιοι εξυπηρετητές ωστόσο για τη πραγματοποίηση μιας συναλλαγής προυποθέτουν και την αυθεντικοποίηση του χρήστη. Σε αυτή τη περίπτωση θα πρέπει ο εξυπηρετούμενος να είναι κάτοχος ψηφιακού πιστοποιητικού έτσι ώστε να επιβεβαιώνεται η ταυτότητα του.

6.3. Πλεονεκτήματα Μειονεκτήματα Χρήσης SSL

Συμπερασματικά, η χρήση του πρωτοκόλλου SSL εξασφαλίζει την εγκαθίδρυση ασφαλών συνδέσεων μεταξύ εξυπηρέτη και εξυπηρετούμενου. Παρέχει αυθεντικοποίηση χρήστων και μηνυμάτων και υπηρεσίες εμπιστευτικότητας και ακεραιότητας. Το SSL θεωρείται από τα πιο διαδεδομένα πρωτόκολλα ασφαλείας καθώς παρέχει ασφάλεια έναντι πολλών επιθέσεων.Ωστόσο, από την άλλη μεριά αυξάνει το υπολογιστικό κόστος και χρόνο διότι χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Η καθυστέρηση οφείλεται κυρίως στην αρχική διαδικασία χειραψίας όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου. Με αποτέλεσμα να καθυστερείται η μετάδοση των κρυπτογραφημένων δεδομένων που ανταλλάσσονται μεταξύ των μερών που επικοινωνούν. Επομένως ,προτείνεται η χρήση του πρωτοκόλλου SSL για συναλλαγές που πρόκειται να μεταβιβαστούν ευαίσθητες πληροφορίες.

7 *Κεφάλαιο*

ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Στις καθημερινές συμβατικές συναλλαγές η βεβαίωση της ταυτότητας των συμβαλλόμενων μερών γίνεται εύκολα με την παρουσία κάποιου επίσημου εγγράφου, τη σύγκριση των υπογραφών ή την χρήση των πιστωτικών καρτών. Στόχος των σύγχρονων τεχνολογιών ασφάλειας είναι η πραγματοποίηση συναλλάγων σε ανοικτά δίκτυα όπου οι χρήστες, οι πόροι και οι συμμετέχοντες μπορούν να είναι σε απομακρυσμένες θέσεις και σε διαφορετικούς χρόνους. Ωστόσο, θα πρέπει ταυτόχρονα να εξασφαλίζεται η προστασία των πληροφοριών που διακινούνται από αλλοίωση ή αποκάλυψη σε τρίτους αλλά και το γεγονός ότι οι συναλλασσόμενοι δεν μπορούν να αποποιηθούν την εκτέλεση κάποιας ενέργειας. Δύο συμβαλλόμενα μέρη για να χρησιμοποιήσουν την κρυπτογραφία δημόσιου κλειδιού προκειμένου να επιτύχουν τις υπηρεσίες ασφάλειάς τους, πρέπει να είναι σε θέση να λάβουν τα δημόσια κλειδιά ο ένας του άλλου και να επικυρώσουν την ταυτότητα του άλλου συμβαλλόμενου μέρους. Επομένως, πρέπει να στηριχθούν σε έναν εμπιστευμένο τρίτο για να διανείμουν τα δημόσια κλειδιά και να επικυρώσουν την ταυτότητα του συμβαλλόμενου μέρους που συνδέεται με το αντίστοιχο βασικό ζευγάρι. Η προσέγγιση που ικανοποιεί αυτές τις απαιτήσεις ασφάλειας είναι η Υποδομή Δημόσιου Κλειδιού (ΥΔΚ). Μία Υποδομή Δημόσιου Κλειδιού διευκολύνει τη δημιουργία μιας ηλεκτρονικής συναλλαγής καθώς προσδιορίζει τα πρόσωπα που συμβάλλουν και τις διαδικασίες που απαιτούνται για την πραγματοποίηση μιας συναλλαγής.

Μια ΥΔΚ μπορεί περιλαμβάνει έναν ή περισσότερους Πάροχους Υπηρεσιών Πιστοποίησης και στοχεύει στην οργάνωση ενός ολοκληρωμένου περιβάλλοντος διαχείρισης πιστοποιητικών, με όρους τεχνικής επάρκειας και νομικής διασφάλισης κατά τη λειτουργία**[S. Harris**, **(2008)]**.

7.1. Ορισμός

Η IETF –Internet Engineering Task Force ορίζει την Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)ως το σύνολο που απαρτίζεται από το λογισμικό ,το υλικό, τους ανθρώπους, τις πολιτικές και τις διαδικασίες που απαιτούνται για τη δημιουργία, τη διαχείριση,την αποθήκευση, τη διανομή και την ανάκληση ψηφιακών πιστοποιητικών που περιέχουν τα δημόσια κλειδιά.

Η Υποδομή Δημόσιου Κλειδιού χαρακτηρίζεται ως ένα πλαίσιο αυθεντικοποίησης του ISO που χρησιμοποιεί τη κρυπτογραφία δημόσιου κλειδιού και το πρότυπο X.509**[S.Harris**, **(2008)]**. Αποτελείται από πολλά διαφορετικά μέρη: αρχές πιστοποίησης, αρχές εγγραφής, ψηφιακά πιστοποιητικά, κλειδιά, και χρήστες τα οποία ενσωματώνει σε ένα ασφαλές αρχιτεκτονικό σχήμα. Χρησιμοποιεί αλγόριθμους και μεθόδους της ασύμμετρης κρυπτογραφίας που αποτελούν απλά ένα μέρος μιας Υποδομής Δημόσιου Κλειδιού. Στο πλαίσιο μιας Υποδομή Δημόσιου Κλειδιού συνδυάζονται όλες οι απαιτούμενες τεχνολογίες, υπηρεσίες και τα λογισμικά ώστε να δημιουργούνται, να διανέμονται και να διατηρούνται τα πιστοποιητικά και τα κλειδιά κρυπτογράφησης, με σκοπό την επίτευξη κρυπτογραφημένης επικοινωνίας και την επικύρωση των χρηστών που συμμετέχουν**[39]**.

7.2. Συστατικά Μέρη Υποδομής Δημόσιου Κλειδιού

Τα πιο σημαντικά μέρη που συνιστούν την Υποδομή Δημόσιου Κλειδιού συνοψίζονται παρακάτω:

- **Αρχές Πιστοποίησης-ΑΠ (Certification Authority - CA):** Μία Αρχή Πιστοποίησης αποτελεί έναν αξιόπιστο φορέα που εκδίδει τα πιστοποιητικά για τους χρήστες, υπολογιστές και υπηρεσίες. Μία Υποδομή Δημόσιου Κλειδιού μπορεί να διαθέτει περισσότερες από μια ΑΠ και να καθορίσει τη σχέση εμπιστοσύνης που θα έχουν μεταξύ τους..
- **Αρχές Εγγραφής-ΑΕ (Registration Authority - RA):** Η Αρχή Εγγραφής εκτελεί τις διαδικασίες εγγραφής του χρήστη που αιτείται το ψηφιακό πιστοποιητικό. Επίσης, καθήκον της είναι να επιβεβαιώνει την ταυτότητα ενός ατόμου και κινεί τη διαδικασία πιστοποίησης για κάποιον χρήστη. Η ΑΕ δεν μπορεί να εκδώσει τα πιστοποιητικά, αλλά μπορεί να ενεργήσει ως 'μεσίτης' μεταξύ του χρήστη και της ΑΠ**[11]**. Δηλαδή, όταν οι χρήστες χρειάζονται τα νέα πιστοποιητικά,

υποβάλλουν τα αιτήματα στην ΑΕ, και εκείνη επαληθεύει όλες τις απαραίτητες πληροφορίες πριν επιτρέψει ένα αίτημα να πάει στη ΑΠ. Μπορούν να υπάρξουν περισσότερες από μια Αρχή Εγγραφής.

- **Υποκείμενα ή Εγγραφόμενους (Subjects or Subscribers):** Υποκείμενα ή Εγγραφόμενοι σε μία Αρχή Πιστοποίησης είναι όσοι αιτούνται και αποκτούν ψηφιακό πιστοποιητικό υπογεγραμμένο από την Αρχή Πιστοποίησης. Φυσικά πρόσωπα ή εξυπηρετητές καλούνται και ως συνδρομητές.
- **Βασιζόμενα μέρη (Relying Parties - RP):** Τα μέρη που βασίζονται στις αρχές πιστοποίησης ή απλά χρήστες των υπηρεσιών πιστοποίησης είναι οποιεσδήποτε οντότητες οι οποίες χρησιμοποιούν και εμπιστεύονται για τις συναλλαγές τους τα αποδεικτικά πιστοποίησης (ψηφιακά πιστοποιητικά, ψηφιακές υπογραφές, κ.λπ.) άλλων οντοτήτων.
- **Πιστοποιητικά (Certificates):** Το πιστοποιητικό είναι το βασικό στοιχείο της ΥΔΚ και αναγράφει το δημόσιο κλειδί του χρήστη το οποίο μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση και υπογραφή των δεδομένων πριν μεταδοθούν μέσω του δικτύου. Το ψηφιακό πιστοποιητικό περιέχει επίσης πληροφορίες όπως η επιτρεπόμενες χρήσεις πιστοποιητικού, αύξων αριθμός, υπογραφή, εκδότης, και την περίοδο ισχύος. Κάθε πιστοποιητικό έχει προκαθορισμένο χρόνο ισχύος, με σκοπό τον περιορισμό της πιθανότητας παραβίασης της ασφάλειας.
- **Αποθήκη Πιστοποιητικών και Υπηρεσίες Καταλόγου (Repositories & Directories):** Μετά την έκδοση των πιστοποιητικών από την Αρχή Πιστοποίησης, θα πρέπει να μεταφέρονται σε αποθήκες (repositories) για τη αποτελεσματική διαχείριση τους. Επίσης, για την ορθή ενημέρωση των υπολοίπων χρηστών της υποδομής για την έκδοση ενός πιστοποιητικού αποθήκευση των πιστοποιητικών γίνεται σε καταλόγους και η πρόσβαση στις υπηρεσίες καταλόγων μπορεί να γίνει χρήση του πρωτοκόλλου Lightweight Directory Access Protocol (LDAP).
- **Λίστες ανάκλησης πιστοποιητικών – ΛΑΠ (Certificate Revocations Lists - CRL):** Τα πιστοποιητικά μπορούν να ανακληθούν για κάποιους λόγους, παραδείγματος χάριν, εάν το ιδιωτικό κλειδί του ιδιοκτήτη έχει χαθεί ή οι υπάρχουν αλλαγές στις πληροφορίες του κατόχου του πιστοποιητικού. Οι ΛΑΠ είναι κατάλογοι πιστοποιητικών που έχουν ανακληθεί για κάποιο λόγο από την Αρχή Πιστοποίησης ηοποία πρέπει επίσης να και να επεξεργαστεί τις λίστες ανάκλησης πιστοποιητικών. Κάθε ΛΑΠ υπογράφεται από την ίδια την Αρχή που εξέδωσε τα πιστοποιητικά για να αποδείξει τη γνησιότητα της. Η ΛΑΠ αναφέρει επίσης τη χρονική στιγμή ανάκλησης των πιστοποιητικών
- **Αλγόριθμοι και μέθοδοι:** είναι οι μέθοδοι και αλγόριθμοι που χρησιμοποιούνται για τη δημιουργία ζεύγους κλειδιών, τη κρυπτογράφηση και το κατακερματισμό κατά τη δημιουργία

ψηφιακής υπογραφής ώστε να παρέχουν στοιχεία εμπιστευτικότητας και ακεραιότητας και την επικύρωση της ταυτότητας του αποστολέα.

- **Πολιτική Πιστοποίησης (Certification Policy - CP):**Το σύνολο των κανόνων λειτουργίας, όρων χρήσης καθώς και τις υποχρεώσεις που θέτει η Αρχή Πιστοποίησης.

- **Δήλωση Διαδικασιών Πιστοποίησης (Certification Practice Statement-CPS):** Περιλαμβάνει το σύνολο των διαδικασιών και λειτουργιών που πραγματοποιούνται για τη σωστή διαχείριση των πιστοποιητικών.

7.3. Λειτουργία Υποδομής Δημόσιου Κλειδιού

Η υπηρεσία ΥΔΚ διαρθρώνεται και λειτουργεί ενδεικτικά ως εξής: Όταν ένας χρήστης (οντότητα) επιθυμεί να αποκτήσει ψηφιακό πιστοποιητικό, αρχικά υποχρεούται να μελετήσει τη Πολιτική Πιστοποίησης (ΠΠ) της Υποδομής Δημόσιου Κλειδιού και να συμφωνήσει με τους όρους που θέτει και κυρίως να είναι βέβαιος ότι το πιστοποιητικό που αιτείται αν ενδείκνυται για το σκοπό που το επιθυμεί.

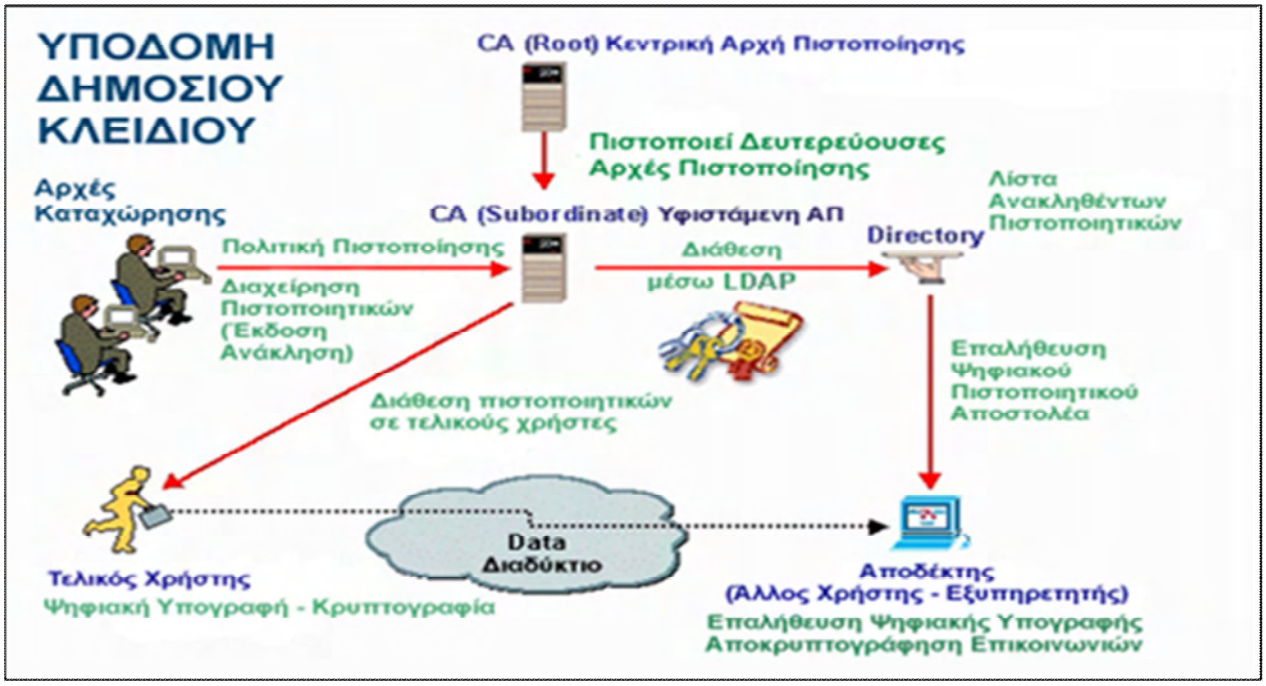
Στη συνέχεια απευθύνεται στην Αρχή Εγγραφής (ΑΕ) η οποία αναλαμβάνει τη διεκπεραίωση των αιτημάτων για έκδοση πιστοποιητικών, για τους χρήστες που τα δικαιούνται, και την επιβεβαίωση της ταυτότητας του χρήστη με όσα φυσικά πιστοποιητικά απαιτείται ανάλογα με το τύπο του πιστοποιητικού. Η Αρχή Εγγραφής και ο χρήστης ανταλλάσσουν τις απαιτούμενες πληροφορίες για να γίνει η εξακρίβωση της ταυτότητας του χρήστη (οντότητα). Έπειτα, η ΑΕ αποφασίζει εάν αποδέχεται ή απορρίπτει την αίτηση. Εάν την αποδεχτεί τότε η αίτηση θα σταλεί ηλεκτρονικά στην Αρχή Πιστοποίησης. Ταυτόχρονα η Αρχή Εγγραφής αναλαμβάνει τα καθήκοντα για το μέρος που αφορά τα υπολογιστικά συστήματα (εφαρμογές, βάσεις δεδομένων κ.λπ.). Ο αριθμός των Αρχών Εγγραφής που θα υπάρχουν και ποιες θα είναι αυτές θα προκύπτει από τη μελέτη εφαρμογής της Υποδομής Δημόσιου Κλειδιού.

Η Αρχή Πιστοποίησης (ΑΠ) δημιουργεί το ψηφιακό πιστοποιητικό δημόσιου κλειδιού του χρήστη και τον ενημερώνει πότε και πώς μπορεί να το αποκτήσει. Όταν η ΑΠ υπογράφει το πιστοποιητικό, δεσμεύει την ταυτότητα του χρήστη (οντότητα) στο δημόσιο κλειδί, και εγγυάται για την αυθεντικότητα του. Είναι η Έμπιστη Τρίτη Οντότητα(ή Πάροχος Υπηρεσιών Πιστοποίησης) που επιτρέπει την επικοινωνία οντοτήτων που δεν έχουν συναντηθεί ποτέ να επικυρώσουν η μία στην άλλη την ταυτότητα τους και να επικοινωνήσουν με μια ασφαλή μέθοδο**[4]**. Το ζεύγος κλειδιών του χρήστη που πιστοποιούνται δημιουργούνται είτε από τον ίδιο είτε από την Αρχή

Πιστοποίησης. Σε περίπτωση που παραχθούν από τον ίδιο επιβεβαιώνεται η αντιστοιχία του ιδιωτικού κλειδιού με το δημόσιο. Όταν ο χρήστης αποκτήσει το πιστοποιητικό στο τέλος της διαδικασίας τα κλειδιά του και το ψηφιακό πιστοποιητικό θα αποθηκεύονται στην έξυπνη κάρτα ή σε οποιοδήποτε άλλο ισοδύναμο επιλεγμένο μέσο αποθήκευσης που θα διαθέτει.

Επομένως, μετά την έκδοση του πιστοποιητικού από μια Αρχή Πιστοποίησης και την ασφαλή μεταβίβαση του στον χρήστη (οντότητα), η ΑΠ έχει και ορισμένες επιπρόσθετες υπηρεσίες που πρέπει να προσφέρει. Οι οποίες είναι: αποθήκευση και δημοσίευση των πιστοποιητικών. Η ΥΔΚ αναλαμβάνει να παρέχει την υπηρεσία αποθήκευσης των δημοσίων κλειδιών των χρηστών σε μορφή πιστοποιητικού το οποίο θα περιλαμβάνει και άλλες πληροφορίες του χρήστη (οντότητα) σε έναν εξυπηρετητή LDAP έτσι ώστε να παρέχει σε όλους τους χρήστες την δυνατότητα αναζήτησης του πιστοποιητικού ενός άλλου χρήστη. Δηλαδή, κάθε φορά που ένας χρήστης του δικτύου λαμβάνει ένα υπογεγραμμένο μήνυμα ή έχει πρόσβαση σε μια πιστοποιημένη ιστοσελίδα ή επιθυμεί να επιβεβαιώσει τη ταυτότητα μιας Υφιστάμενης Αρχής Πιστοποίησης να μπορεί να ενημερώνεται μέσω της αναζήτησης από την αρχή πιστοποίησης που εξέδωσε το πιστοποιητικό για να βεβαιώσει τη γνησιότητα, την εγκυρότητα και την τρέχουσα ισχύ των στοιχείων του άλλου μέρους της επικοινωνίας. Επιπρόσθετα, η ΥΔΚ αναλαμβάνει την ανανέωση ή επανέκδοση πιστοποιητικών για την αντικατάσταση πιστοποιητικών τα οποία έχουν λήξει, ή όταν τα στοιχεία τα οποία φέρει το πιστοποιητικό έχουν τροποποιηθεί**[4]**.

Τέλος, παρέχει υπηρεσία ανάκλησης πιστοποιητικών η ΑΠ είναι υπεύθυνη για την ανάκληση πιστοποιητικών για λόγους που κρίνει η ΑΠ ότι δεν είναι πλέον έγκυρα. Για την ενημέρωση των χρηστών της για τα ανακληθέντα πιστοποιητικά η ΥΔΚ δημοσιεύει Λίστες Ανάκλησης Πιστοποιητικών (ΛΑΠ). Στην **Εικόνα 14** φαίνονται οι βασικές συνιστώσες μιας Υποδομής Δημόσιου Κλειδιού και οι λειτουργίες τους.



Εικόνα 14:Περιγραφή λειτουργίας Υποδομής Δημόσιου Κλειδιού (pki.auth.gr)

7.4. Παροχές Υποδομής Δημόσιου Κλειδιού

Οι απαιτήσεις ασφάλειας που ικανοποιούνται από μία Υποδομή δημόσιου κλειδιού είναι οι εξής: **Εμπιστευτικότητα (Confidentiality), Ακεραιότητα (Integrity), Μη Αποποίηση (Non-Repudiation)**, **Αυθεντικοποίηση εξυπηρετητή/πελάτη (server/client authentication)/ (Authentication)**, **Ηλεκτρονικές υπογραφές (Electronic signatures).**

7.4.1. Εμπιστευτικότητα

Ένα σχέδιο ΥΔΚ υπάρχει ώστε να παρέχει τη δυνατότητα και τα μέσα σε έναν χρήστη να μεταδώσει πληροφορίες κατά τρόπο ιδιωτικό, χωρίς οποιαδήποτε προσωπική ή ευαίσθητη πληροφορία του να γίνεται διαθέσιμη δημόσια. Όταν κάποιο στοιχείο διαβιβάζεται σε ολόκληρο το Διαδίκτυο είναι επιτακτική ανάγκη να διατηρείται κρυπτογραφημένο και ιδιωτικό. Κάτι τέτοιο δεν αποτελεί μόνο ανάγκη για τις επιχειρήσεις που διαβιβάζουν στοιχεία όπως τα οικονομικές αρχεία, αλλά τίθεται πλέον ζήτημα και από νομικής πλευράς. Το πρώτο βήμα σε ένα επιτυχές σχέδιο ΥΔΚ είναι να ληφθούν δύο κλειδιά, ένα δημόσιο και ένα ιδιωτικό κλειδί. Αναγκαία προϋπόθεση είναι η φύλαξη του ιδιωτικού κλειδιού από τον χρήστη και να μη το μοιραστεί με οποιονδήποτε άλλον. Μια ψηφιακή υπογραφή περιλαμβάνεται στο ψηφιακό πιστοποιητικό και με την προσθήκη της υπογραφής στα μηνύματα ηλεκτρονικού ταχυδρομείου, ο παραλήπτης μπορεί να είναι σίγουρος ότι οι ιδιωτικές πληροφορίες λαμβανόμενες εστάλησαν πράγματι από τον αποστολέα. Ωστόσο όπως αναλύσαμε στο Κεφάλαιο Ψηφιακά Πιστοποιητικά αυτή δεν είναι αρκετή για να εξασφαλίσει ότι

κρατιούνται οι πληροφορίες ασφαλείς σύμφωνα με τους νόμους περί ιδιωτικότητας. Ο αμέσως καλύτερος τρόπος να εξασφαλιστεί η ιδιωτικότητα του ατόμου είναι να χρησιμοποιηθεί ένα σχέδιο ΥΔΚ**[3]**.

7.4.2. Αυθεντικοποίηση

Κατά την μελέτη ενός σχεδίου Υποδομής Δημόσιου Κλειδιού φαίνεται ότι η βάση είναι η αυθεντικοποίηση. Οι ηλεκτρονικές συναλλαγές απαιτούν ασφαλή ανταλλαγή πληροφοριών ανάμεσα σε δύο μέρη, δηλαδή μηχανισμούς επαλήθευσης ταυτότητας (authentication) των συμβαλλομένων μερών και μη αποποίηση ευθύνης από κανένα από αυτά τα μέρη. Τέτοιες υπηρεσίες παρέχονται από την υποδομή δημοσίου κλειδιού μέσω της δημιουργίας και διαχείρισης ζευγών κρυπτογραφικών κλειδιών, βάσει των οποίων εκδίδονται και τα ψηφιακά πιστοποιητικά. Τα κλειδιά και τα πιστοποιητικά που εκδίδονται και διακινούνται στα πλαίσια της υποδομής χρησιμοποιούνται για τη διασφάλιση της επικοινωνίας μέσω υπηρεσιών κρυπτογράφησης και ψηφιακής υπογραφής.

Όταν κάποιος ενδιαφερόμενος υποβάλλει αίτηση για ένα ζεύγος κλειδιών, πρέπει πρώτα να προσκομίσει αποδείξεις που θα επικυρώνει το ποιος είναι στην Αρχή Πιστοποίησης. Η Αρχή Πιστοποίησης συνεργάζεται με την Αρχή Εγγραφής και η τελευταία θα χρησιμοποιήσει διάφορες στρατηγικές, εργαλεία, και μεθόδους για να αποδείξουν ότι ο συνδρομητής είναι αυτός που ισχυρίζεται. Είναι καθήκον της ΑΕ να επικυρώσει τα φυσικά πιστοποιητικά του συνδρομητή, πριν διανέμει την αίτηση στην ΑΠ. Μόλις, η ΑΠ εκδώσει ένα ψηφιακό πιστοποιητικό ο συνδρομητής θα λάβει το ιδιωτικό και δημόσιο κλειδί του. Χωρίς την κατάλληλη επικύρωση όμως που παρέχεται από την Αρχή Εγγραφής και που δίνεται στην Αρχή Πιστοποίησης, το ψηφιακό πιστοποιητικό δεν θα εκδιδόταν. Μόλις λάβει ένας συνδρομητής τα κλειδιά και το ψηφιακό πιστοποιητικό του, μπορεί να αρχίσει τα αποστέλλει κρυπτογραφημένα μηνύματα. Εάν δεν διαθέτει έγκυρο ιδιωτικό ή δημόσιο κλειδί (π.χ. το ψηφιακό πιστοποιητικό του ανακλήθηκε) δεν θα είναι σε θέση να κρυπτογραφήσει ή να αποκρυπτογραφήσει οποιαδήποτε μηνύματα. Ή αντίστοιχα όταν κάποιος λαμβάνει ένα κρυπτογραφημένο μήνυμα, πρέπει να έχει ένα έγκυρο ιδιωτικό ή δημόσιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Αυτό δείχνει ότι το ένα σύστημα κρυπτογραφίας αλλά και η επιτυχής εφαρμογή ενός σχεδίου ΥΔΚ εξαρτάται από την αυθεντικοποίηση. Στην πραγματικότητα,θα μπορούσαμε να πούμε ότι η αυθεντικοποίηση είναι το κλειδί για μια επιτυχημένη ΥΔΚ**[12]**.

7.4.3. Ακεραιότητα

Με τον όρο ακεραιότητα εννοείται τη μετάδοση στοιχείων μέσα από ένα δίκτυο χωρίς να

υποστούν αλλοίωση, δηλαδή να φτάνουν στον προορισμό τους ολόκληρα και πλήρη. Η διατήρηση της ακεραιότητας των στοιχείων αποτελεί έναν από τους σημαντικότερους στόχους μιας ΥΔΚ. Μια ΥΔΚ παρέχει τα μέσα για τη κρυπτογράφηση ενός μηνύματος, την αποστολή του σε ολόκληρο το Διαδίκτυο, έχοντας έναν δέκτη που το αποκρυπτογραφεί για να το διαβάσει. Εάν αυτό το μήνυμα μεταβληθεί οπουδήποτε κατά τη διαδικασία αυτή, το σύστημα έχει αποτύχει και το περιεχόμενο του μηνύματος δεν θεωρείται άξιο εμπιστοσύνης. Τα στοιχεία που περιέχονται σε ένα μήνυμα μπορούν να αλλοιωθούν με πολλούς διαφορετικούς τρόπους. Εκτός από τις κακόβουλες επιθέσεις που μπορούν να δεχθούν, όπως είναι τα ζωύφια λογισμικού, οι ιοί και τα κακόβουλα υπάρχουν και άλλοι παράγοντες που μπορούν να συμβάλουν στην αλλοίωση της ακεραιότητα στοιχείων όπως είναι ή περίπτωση λάθους ή αποτυχίας των υπολογιστών ή και η περίπτωση των φυσικών καταστροφών. Μια ΥΔΚ πρέπει να εξασφαλίσει ότι το στοιχείο προστατεύεται από το λεπτό που κρυπτογραφείται και προστατεύεται από τις επιθέσεις. Η πιο κοινή μέθοδος που χρησιμοποιείται για να αποτρέψει την αλλοίωση της ακεραιότητας των στοιχείων είναι μέσω της ψηφιακής υπογραφής η οποία είναι ένα σημαντικό εργαλείο που χρησιμοποιείται για να εξασφαλίσει ότι τα μηνύματα είναι σωστά και έχουν διαβιβαστεί ακέραια κάνοντας χρήση κάποιου κατακερματισμού (hashing). Αυτό είναι ένα σημαντικό βήμα σε ένα σχέδιο ΥΔΚ και δεν πρέπει να λείψει. Επίσης είναι επιτακτικό να κρατούνται με συνέπεια πάντα τα ασφαλή αντίγραφα των στοιχείων και να διατηρούνται οι υπολογιστές κατάλληλα διατηρημένοι και απαλλαγμένοι από κακόβουλο λογισμικό. Η χρησιμοποίηση όλων αυτών των εργαλείων ασφαλείας είναι ζωτικής σημασίας καθώς συμβάλλει στην επιτυχία η αποτυχία ενός σχεδίου Υποδομής Δημόσιου Κλειδιού και της εξασφάλισης ότι τα στοιχεία παραμένουν ολόκληρα και πλήρες.

7.5. Πρότυπες Αρχιτεκτονικές

Σε μια Υποδομή Δημόσιου Κλειδιού μπορεί να λειτουργούν περισσότερε από μια αρχές Πιστοποίησης. Η αρχιτεκτονική που θα ακολουθήσει μια υποδομή διαφοροποιείται ανάλογα με τον αριθμό των αρχών πιστοποίησης που εμπλέκονται, τις σχέσεις εμπιστοσύνης που υπάρχουν μεταξύ δυο αρχών πιστοποίησης καθώς και το σημείο που τοποθετούν την εμπιστοσύνη τους οι χρήστες. Η εμπιστοσύνη σε ένα πιστοποιητικό βασίζεται στο πόσο έμπιστη είναι η αρχή πιστοποίησης που το εξέδωσε. Οι πρότυπες αρχιτεκτονικές Υποδομής Δημόσιου Κλειδιού είναι οι εξής:

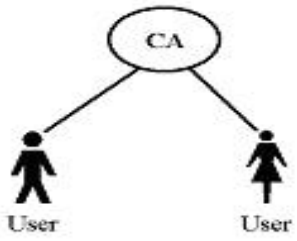
- **Απλή αρχιτεκτονική (Single architecture)**
- **Ιεραρχική αρχιτεκτονική (Hierarchical architecture)**
- **Mesh αρχιτεκτονικήή αρχιτεκτονική Δικτύου**

- **Bridge αρχιτεκτονικήή αρχιτεκτονική Γέφυρα**

Ωστόσο, πριν την εφαρμογή ενός σχεδίου Υποδομής Δημόσιου Κλειδιού, θα πρέπει να ληφθούν υπόψιν συγκεκριμένες ανάγκες και απαιτήσεις προκειμένου να επιλεχθεί ποια αρχιτεκτονική ΥΔΚ είναι πιο κατάλληλη. Αρχικά το κόστος υλοποίησης αποτελεί περιορισμό στην επιλογή ενός μοντέλου ΥΔΚ, δεδομένου ότι χρειάζεται ο κατάλληλος εξοπλισμός για να φιλοξενήσει κάθε αρχή πιστοποίησης. Μια απλή αρχιτεκτονική απαιτεί μόνο ένα μηχάνημα για να φιλοξενήσει την ΑΠ, ενώ σε μια ιεραρχική ή Mesh αρχιτεκτονική ανακύπτει η ανάγκη για διάφορα εργαλεία (με τον κατάλληλο λογισμικό, άδειες, κ.λπ.) για την υποστήριξη αυτών των σχημάτων. Έπειτα, ο αριθμός των ατόμων που θα απασχοληθούν σε μια υποδομή αποτελεί ένα άλλο περιορισμό στην επιλογή ενός μοντέλου ΥΔΚ και θα κριθεί ανάλογα με το μέγεθος της οργάνωσης και τη ποσότητα των πιστοποιητικών που θα διεκπαιρεώνει. Τέλος, η δομή του οργανισμού διαδραματίζει σημαντικό ρόλο στην επιλογή της κατάλληλης αρχιτεκτονικής. Οι μικρότεροι οργανισμοί είναι προτιμότερο να επιλέγουν την εφαρμογή μιας ενιαίας αρχιτεκτονικής καθώς είναι πιο εύκολο να υποστηρίξει μια πιο περιορισμένη ομάδα χρηστών. Όσον αφορά μεγαλύτερους οργανισμούς η επιλογή αρχιτεκτονικής θα εξαρτηθεί από το τη συχνότητα που γίνεται η ανταλλαγή πληροφοριών καθώς με την ιεραρχική αρχιτεκτονική αυξάνεται το φορτίο επεξεργασίας στα μονοπάτια πιστοποίησης. Ωστόσο οι αρχιτεκτονικές Mesh και Bridge παρουσιάζουν αρκετά σύνθετη δομή και για αυτό απαιτείται προσεκτικός σχεδιασμός και σωστή οργάνωση.

7.5.1. Απλή Αρχιτεκτονική

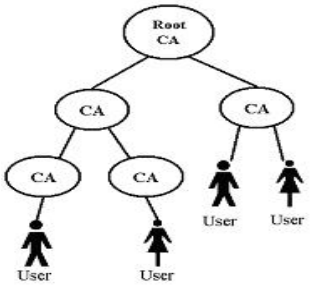
Μια απλή αρχιτεκτονική είναι το πιο βασικό μοντέλο Υποδομής Δημόσιου Κλειδιού και περιέχει μόνο μια Αρχή Πιστοποίησης. Όλοι οι χρήστες της τοποθετούν την εμπιστοσύνη τους σε αυτή την Αρχή. Αυτή η αρχή πιστοποίησης είναι υπεύθυνη για την διαχείριση όλων των χρηστών που ζητούν πιστοποιητικό και θα είναι η μοναδική αρχή έκδοσης και ο μοναδικός τρόπος να πιστοποιείται η εγκυρότητα ενός πιστοποιητικού.Δεδομένου ότι υπάρχει μόνο μία ΑΠ κάθε διαδρομή πιστοποίησης θα ξεκινήσει με το δημόσιο κλειδί αυτής. Δηλαδή κάθε πιστοποιητικό που εκδίδεται για τους χρήστες θα υπογράφεται ψηφιακά από αυτήν και αντίστοιχα οι χρήστες μπορούν να επαληθεύσουν την υπογραφή της με το δημόσιο κλεδί της.



Εικόνα 15:Απλή Αρχιτεκτονική Υποδομής Δημόσιου Κλειδιού

7.5.2. Ιεραρχική Αρχιτεκτονική

Η ιεραρχική αρχιτεκτονική αποτελείται από περισσότερες από μια αρχές πιστοποίησης και είναι κατασκευασμένη με διαφορετικά επίπεδα αρχών πιστοποίησης περιλαμβάνοντας υφιστάμενες αρχές πιστοποίησης σε μορφή δέντρου. Σε αυτήν τη δομή, όλοι οι χρήστες εμπιστεύονται μια κύρια ΑΠ τη "ρίζα" (root CA). Η ρίζα ΑΠ πιστοποιεί μόνο τις υφιστάμενες ΑΠ, ενώ οι υφιστάμενες ΑΠ μπορούν να εκδίδουν πιστοποιητικά για τους χρήστες ή άλλες ΑΠ. Η σχέση εμπιστοσύνης που ορίζεται είναι σε μία μόνο κατεύθυνση. Σε αυτή την αρχιτεκτονική ΥΔΚ, κάθε μονοπάτι πιστοποίησης ξεκινά με το δημόσιο κλειδί της ρίζας ΑΠ, κάθε φορά που κάποιος θέλει να ελέγξει την εγκυρότητα ενός πιστοποιητικού, εξετάζει αν υπάρχει εμπιστοσύνη ανάμεσα στην αρχή πιστοποίησης που εξέδωσε το πιστοποιητικό και την ΑΠ ρίζας.

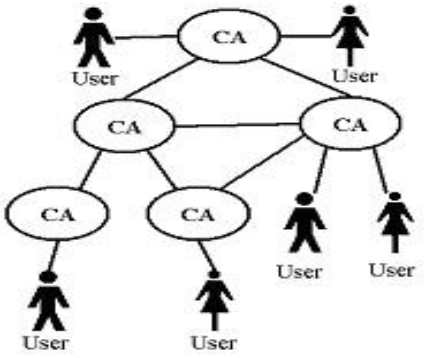


Εικόνα 16:Ιεραρχική Αρχιτεκτονική Υποδομής Δημόσιου Κλειδιού

7.5.3. Mesh Αρχιτεκτονική

Η αρχιτεκτονική mesh ή αλλιώς αρχιτεκτονική δικτύου δεν περιλαμβάνει μόνο μία Αρχή Πιστοποίησης που θεωρείται αξιόπιστη από όλες τις υπόλοιπες αρχές πιστοποίησης της ΥΔΚ όπως γίνεται στις δύο προηγούμενες αρχιτεκτονικές. Οι αρχές πιστοποίησης μπορούν να συνδεθούν με μια **διασταύρωση πιστοποίησης ή δια-πιστοποίηση (Cross-Certification)** με αποτέλεσμα τη δημιουργία ενός ιστού εμπιστοσύνης (web of trust). Σε αυτόν τον ιστό κατασκευάζονται μονοπάτια πιστοποίησης τα οποία συνδέουν μεταξύ τους έμπιστες αρχές πιστοποίησης όπου πραγματοποιείται μια διαδικασία ανταλλαγής πληροφοριών μεταξύ δύο ΑΠ, ώστε να εμπιστεύεται η μια τα κλειδιά της άλλης. Μια ΑΠ μπορεί να δημιουργήσει και να ένα πιστοποιητικό δημόσιου κλειδιού μιας

άλλης ΑΠ. Όλοι οιχρήστες που ανήκουν στην μία εμπιστεύονται όλους τους χρήστες που ανήκουν στην άλλη. Οι τελικοί χρήστες μπορούν να επιλέξουν την εμπιστοσύνη μιας Αρχής Πιστοποίησης στην ΥΔΚ και να αποφασίσουν για την εγκυρότητα ενός πιστοποιητικού ή την απόρριψή του.

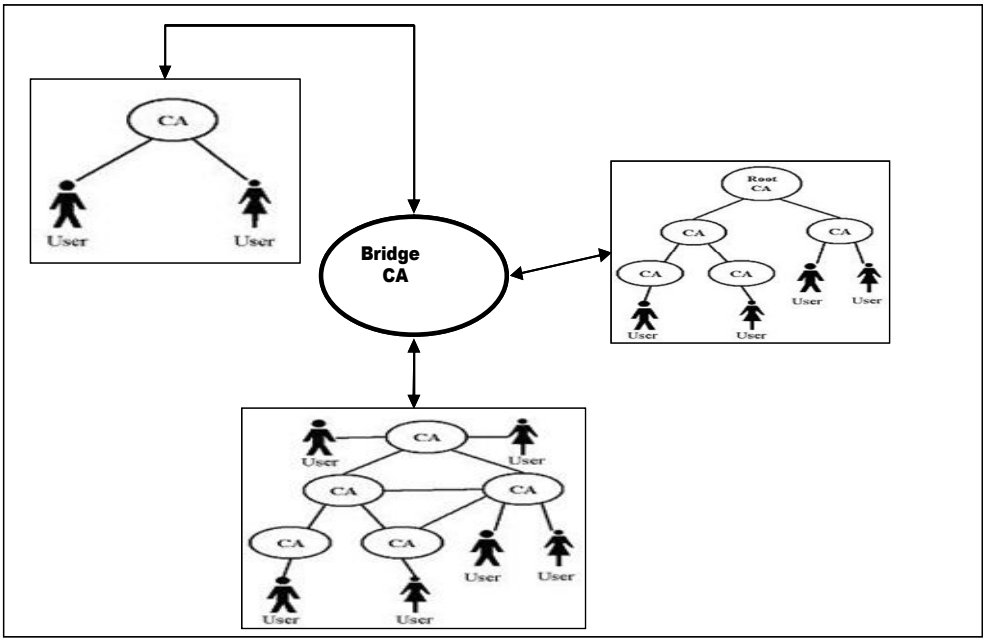


Εικόνα 17:Mesh Αρχιτεκτονική Υποδομής Δημόσιου Κλειδιού

7.5.4. Bridge Αρχιτεκτονική

Οι αρχιτεκτονικές που αναφέρθηκαν παραπάνω μπορεί να μην καλύπτουν τις ανάγκες κάθε οργανισμού ή αυτές οι ανάγκες είναι πιθανό να αλλάζουν στην πορεία του χρόνου και να απαιτούνται αναπροσαρμογές που δεν συμφωνούν με το αρχικό σχήμα. Για την αντιμετώπιση τέτοιων προβλημάτων, έχουν δημιουργηθεί περισσότερο ευέλικτες αρχιτεκτονικές οι οποίες παρουσιάζουν κοινά στοιχεία με παραπάνω από μια από τις βασικές αρχιτεκτονικές που αναφέρθηκαν παραπάνω. Το πιο χαρακτηριστικό παράδειγμα τέτοιας αρχιτεκτονικής είναι αυτό της αρχιτεκτονικής αρχής πιστοποίησης με χρήση γέφυρας (Bridge Certification Authority), το οποίο φαίνεται στην **Εικόνα 18.**

Κεντρικό σημείο της αρχιτεκτονικής αυτής είναι μια ενδιάμεση αρχή πιστοποίησης η οποία δεν εκδίδει απευθείας πιστοποιητικά στους χρήστες, ούτε πιστοποιεί κατωτέρου επιπέδου αρχές πιστοποίησης. Αυτό που κάνει είναι να αποτελεί ενδιάμεσο σημείο το οποίο αναλαμβάνει την εγκαθίδρυση εμπιστοσύνης ανάμεσα σε διαφορετικές και άγνωστες μεταξύ τους αρχές πιστοποίησης. Συνήθως μια αρχιτεκτονική Bridge χρησιμοποιείται για να επιλυθούν προβλήματα που προκύπτουν από ασυμβατότητες στις πολιτικές των αρχών πιστοποίησης, χωρίς να αλλάξουν οι χρήστες της ΥΔΚ το σημείο εμπιστοσύνης που έχουν εξαρχής**[12]**.



Εικόνα 18:Bridge Αρχιτεκτονική Υποδομής Δημόσιου Κλειδιού

8 *Κεφάλαιο*

ΑΡΧΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΚΑΙ ΕΓΓΡΑΦΗΣ

Για να κατορθώσει ένα σχέδιο Υποδομής Δημόσιου Κλειδιού να προσφέρει τις υπηρεσίες που αναφέραμε στο προηγούμενο κεφάλαιο θα πρέπει κάθε συμμετέχον μέρος της να λειτουργεί σωστά και σύμφωνα με τους κανόνες που έχουν τεθεί. Η Αρχή Πιστοποίησης και η Αρχή Εγγραφής αποτελούν τα βασικά συστατικά μέρη ενός Πάροχου Υπηρεσιών Πιστοποίησης. Συμβάλλουν στην ορθή λειτουργία μιας Υποδομής Δημόσιου Κλειδιού και παρέχουν τις κατάλληλες υπηρεσίες για τη διαχείριση των ψηφιακών πιστοποιητικών. Τα καθήκοντα της Αρχής Πιστοποίησης είναι να εκδίδει τα πιστοποιητικά δημόσιου κλειδιού και να βεβαιώσει ότι το δημόσιο κλειδί που έχει ενσωματωθεί πράγματι ανήκει στην συγκεκριμένη οντότητα όπως αναφέρεται στο πιστοποιητικό**.**Οι θέσεις της Αρχής Εγγραφής είναι να εκτελεί τις κατάλληλες διεργασίες όπως να λαμβάνει τα αιτήματα χρήστη, να επιβεβαιώσει τις ταυτότητες τους και να τα εισάγει σε βάση δεδομένων του χρήστη**[47]**.

8.1. Αρχή Πιστοποίησης

Η Αρχή Πιστοποίησης -(ΑΠ) (Authority Certificate-CA) είναι μία Έμπιστη Τρίτη Οντότητα που καθορίζει ότι το ψηφιακό πιστοποιητικό ισχύει και ότι οι πληροφορίες και τα στοιχεία μιας οντότητας είναι έγκυρα. Αποτελεί βασικό συστατικό μιας υποδομής δημόσιου κλειδιού καθώς είναι οι προμηθευτές που εκδίδουν το ψηφιακό πιστοποιητικό και ασχολείται με τη διαχείριση τους για ολόκληρο τον κύκλο ζωής τους. Η αρχή πιστοποιητικών απαρτίζεται από μια συλλογή υλικού

,λογισμικού και προσώπων και χαρακτηρίζεται από το δημόσιο κλειδί που κατέχει. Κάθε πιστοποιητικό που εκδίδει η ΑΠ αναφέρει το όνομά της και το υπογράφει με το ιδιωτικό της κλειδί.

Πρωτίστως, η ΑΠ έχει καθήκον να συντάσσει, σύμφωνα με τα καθορισμένα πρότυπα που έχουν θεσπιστεί, και να συντηρεί τα κείμενα στα οποία θα αναφέρονται η Πολιτική και οι Διαδικασίες Πιστοποίησης που ακολουθεί για την έκδοση και τη διαχείριση των ψηφιακών πιστοποιητικών και τη λειτουργία του συστήματος της. Αυτά τα κείμενα, Πολιτική Πιστοποίησης (ΠΠ) και Δήλωση Διαδικασιών Πιστοποίησης (ΔΔΠ), υποχρεούται να τα δημοσιεύει για την ενημέρωση κάθε δυνητικά ενδιαφερόμενου χρήστη και να συμμορφώνεται πλήρως με τους ρητούς κανόνες που έχουν τεθεί. Επίσης, μια ΑΠ θα πρέπει να δημιουργεί το δικό της πιστοποιητικό, το οποίο το υπογράφει η ίδια με το ιδιωτικό κλειδί της (ή προηγουμένως να έχει πιστοποιηθεί από κάποια άλλη ΑΠ) και να το δημοσιεύει στους χρήστες. Τέλος, θα πρέπει να συμμορφώνεται με το νομικό πλαίσιο του ΠΔ150/01 για τους Παρόχους Υπηρεσιών Πιστοποίησης και να συντηρεί ένα αξιόπιστο σύστημα με επαρκή διαθεσιμότητα.

8.1.1. Παροχές Υπηρεσιών Αρχής Πιστοποίησης

Οι βασικότερες υπηρεσίες που παρέχει η Αρχή Πιστοποίησης στα πλαίσια μιας Υποδομής Δημόσιου Κλειδιού είναι οι εξής: **1.Δημιουργία και Έκδοση Πιστοποιητικών, 2.Διανομή Πιστοποιητικών, 3.Αποθήκευση Πιστοποιητικών σε καταλόγους, 4.Ανάκληση/Ακύρωση Πιστοποιητικών, 5.Δημοσίευση Λιστών Ανακληθέντων Πιστοποιητικών (ΛΑΠ).**

Όταν ένας χρήστης αιτηθεί ένα ψηφιακό πιστοποιητικό η Αρχή Εγγραφής ελέγχει την ταυτότητα και επαληθεύει τις πληροφορίες του πριν να εγκρίνει την έκδοση του ψηφιακού πιστοποιητικού. Έπειτα, η ΑΕ αποστέλλει την αίτηση στην Αρχή Πιστοποίησης με ασφαλή τρόπο προκειμένου να εξασφαλιστεί η εμπιστευτικότητα των στοιχείων. Η Αρχή Πιστοποίησης **δημιουργεί** το πιστοποιητικό, το **εκδίδει** υπογράφοντας το με το ιδιωτικό της κλειδί. Στη συνέχεια, το **διανέμει** στον αιτούντα με επιλεγμένο ασφαλή τρόπο έτσι ώστε να διατηρείται η εμπιστευτικότητα των κλειδιών του.

Επιπρόσθετα η ΑΠ μπορεί να **ανακαλέσει** ή και να **ακυρώσει** ένα πιστοποιητικό σε περίπτωση που κρίνει ότι είναι αναγκαίο, όπως για παράδειγμα σε περίπτωση που παραβιαστεί η εμπιστευτικότητα του ιδιωτικού κλειδιού του χρήστη ή η ΑΠ αντιληφθεί ότι εξέδωσε το πιστοποιητικό σε λάθος χρήστη.

Η ΑΠ θα πρέπει να **αποθηκεύει** τα πιστοποιητικά που εκδίδει και να τα διατηρεί και πέραν της διάρκειας ισχύος τους. Η αποθήκευση των πιστοποιητικών γίνεται στις Αποθήκες Πιστοποιητικών (certificate repositories), ώστε οι χρήστες να έχουν τη δυνατότητα πρόσβασης στις πληροφορίες των πιστοποιητικών μέσω της διαδικασίας αναζήτησης. Η τεχνολογία που

χρησιμοποιείται για τις αποθήκες πιστοποιητικών είναι τα συστήματα καταλόγου (Directory Systems) που είναι συμβατά με το πρωτόκολλο LDAP (Lightweight Directory Access Protocol).

Όταν η ΑΠ εκδίδει ένα πιστοποιητικό, βεβαιώνει ότι ο χρήστης (οντότητα) έχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιλαμβάνεται στο πιστοποιητικό. Εάν η ΑΠ περιλαμβάνει και πρόσθετες πληροφορίες στο πιστοποιητικό, βεβαιώνει ότι οι πληροφορίες αντιστοιχούν στον χρήστη. Αυτές οι πρόσθετες πληροφορίες μπορεί να είναι να είναι τα στοιχεία επαφής (π.χ., μια διεύθυνση ηλεκτρονικού ταχυδρομείου), ή πληροφορίες της πολιτικής πιστοποίησης που ακολουθεί (π.χ., οι τύποι εφαρμογών που μπορούν να εκτελεστούν με αυτό το δημόσιο κλειδί). Μετά την έκδοση του πιστοποιητικού οι πληροφορίες που αναγράφονται πιστοποιούνται από την ΑΠ ότι είναι αυθεντικές και ότι το δημόσιο κλειδί του χρήστη δεν έχει κατοχυρωθεί από κάποιον άλλο. Πληροφορίες προσωπικές ή άλλες που δεν έχουν πιστοποιηθεί δεν αναγράφονται. Οι οντότητες που πρόκειται να επικοινωνήσουν με τον χρήστη εμπιστεύονται τις πληροφορίες αυτές και στη συνέχεια εξάγουν το δημόσιο κλειδί, όντας σίγουρες ότι αντιστοιχεί στον χρήστη, από το πιστοποιητικό για να το χρησιμοποιήσουν για την πραγματοποίηση ασφαλών επικοινωνιών. Για να μπορέσει οποιαδήποτε οντότητα να ελέγξει τις πληροφορίες που χρειάζεται και ότι το πιστοποιητικό είναι σε ισχύ και έγκυρο θα πρέπει η Αρχή Πιστοποίησης μετά την έκδοση των ψηφιακών πιστοποιητικών να τα αποθηκεύει, να τα διατηρεί και να τα **δημοσιεύει**. Στην περίπτωση της ανάκλησης, οι ανακλημένες πληροφορίες πιστοποιητικών αποθηκεύονται και δημοσιεύονται σε μια Λίστα Ανάκλησης Πιστοποιητικών-ΛΑΠ (Certification Revocated List-CRL) έτσι ώστε κάθε χρήστης να μπορεί να ελέγχει εάν ένα πιστοποιητικό είναι σε ισχύ ή ανακλημένο. Η ΑΠ έχει ως υποχρέωση να διατηρεί και να ενημερώνει περιοδικά τη ΛΑΠ.

8.2. Πολλαπλές Αρχές Πιστοποιητικού

Με την ύπαρξη πολλαπλών Αρχών Πιστοποίησης ένα πρόβλημα που μπορεί να προκύψει είναι όταν δύο διαφορετικές οντότητες ή μέρη που χρησιμοποιούν δύο διαφορετικές ΑΠ και εάν δεν έχουν αποδεχτεί τις αντίστοιχες αρχές, τα πιστοποιητικά δεν μπορεί να φαίνονται έγκυρα. Για την αντιμετώπιση του προβλήματος αυτού το δημόσιο κλειδί κάθε ΑΠ θα πρέπει να είναι υπογεγραμμένο από μια ακόμη ΑΠ την οποία εμπιστεύονται και οι δύο, επιτρέποντας έτσι να δημιουργηθεί ένα κατευθυνόμενο γράφημα εμπιστοσύνης. Όταν η οντότητα που λαμβάνει ένα πιστοποιητικό είναι μια Αρχή Πιστοποίησης, τότε και τα πιστοποιητικά που εκδίδει αυτή θεωρούνται αξιόπιστα. Η ΑΠ εκδότης αναφέρει το όνομά της σε κάθε πιστοποιητικό (και ΛΑΠ) που παράγει, και το υπογράφει με το ιδιωτικό της κλειδί. Μόλις καθορίσουν οι χρήστες ότι

εμπιστεύονται μια ΑΠ (άμεσα, ή μέσω ενός μονοπατιού πιστοποίησης) μπορούν να εμπιστευθούν τα πιστοποιητικά που εκδίδονται. Αυτή η διαδικασία ανταλλαγής πληροφοριών ανάμεσα σε δύο Αρχές Πιστοποίησης ώστε να εμπιστεύονται η μια τα κλειδιά της άλλης ονομάζεται **Διαπιστοποίηση** ή διασταύρωση πιστοποίησης (**Cross-certification**). Έτσι όλοι οι χρήστες που ανήκουν στη μια Αρχή Πιστοποίησης εμπιστεύονται όλους τους χρήστες της άλλης Αρχής Πιστοποίησης.

Σε ένα ιεραρχικό μοντέλο εμπιστοσύνης μία Αρχή Πιστοποίησης, η οποία υπογράφει το πιστοποιητικό της ονομάζεται Κεντρική Αρχή Πιστοποίησης. Μία Αρχή Πιστοποίησης της οποίας το πιστοποιητικό έχει υπογραφεί από τη Κεντρική Αρχή Πιστοποίησης ονομάζεται Υφιστάμενη Αρχή Πιστοποίησης. Οι Υφιστάμενες Αρχές Πιστοποίησης υποχρεούνται να συμμορφώνονται και να υιοθετούν πλήρως την Δήλωση Πρακτικών Πιστοποίησης της Κεντρικής Αρχής Πιστοποίησης. Κάθε Υφιστάμενη Αρχή Πιστοποίησης εφόσον η ίδια έχει πιστοποιηθεί από κάποια άλλη ΑΠ που λειτουργεί σε ανώτερο επίπεδο μπορεί να εκδόσει ψηφιακό πιστοποιητικό σε κάποια άλλη υφιστάμενη ΑΠ που βρίσκεται σε κατώτερο επίπεδο από αυτή. Όλες οι πορείες εμπιστοσύνης ξεκινάνε από την Κεντρική ΑΠ. Οι Στηριζόμενες Οντότητες βλέπουν και εμπιστεύονται μέσα από τα πιστοποιητικά την Κεντρική Αρχή Πιστοποίησης. Τέλος μέσα στα καθήκοντα της Υφιστάμενης ΑΠ είναι να προστατεύει το ιδιωτικό της κλειδί που υπογράφει τα πιστοποιητικά που εκδίδει και να ενημερώνει την Κεντρική Αρχή Πιστοποίησης σε περίπτωση απώλειας ή έκθεσης του.

8.3. Αρχή Εγγραφής

Η Αρχή Εγγραφής-ΑΕ (Registration Authority RA) αποτελεί και αυτή μια σημαντική πτυχή της Υποδομής Δημόσιου Κλειδιού. Είναι η οντότητα που επιβεβαιώνει τα στοιχεία της ταυτότητας ενός χρήστη, κινεί τη διαδικασία πιστοποίησης σε συνεργασία με την Αρχή Πιστοποίησης εκ μέρους ενός χρήστη (οντότητα) και εκτελεί τις διοικητικές λειτουργίες του κύκλου της ζωής πιστοποιητικών.

Μια Υποδομή Δημόσιου Κλειδιού στηρίζεται στα διαφορετικά συστατικά της για να λειτουργήσει επιτυχώς. Χρησιμοποιεί την τεχνολογία της κρυπτογράφησης προκειμένου να μεταφερθούν ασφαλώς σε ολόκληρο το διαδίκτυο προσωπικά στοιχεία. Εάν πριν την εφαρμογή των ιδιωτικών και δημόσιων κλειδιών για την κρυπτογράφηση δεν αυθεντικοποιηθούν τα στοιχεία, δεν υπάρχει κανένας τρόπος στη συνέχεια να ελεγχθεί ότι το στοιχείο που μεταφέρεται είναι νόμιμο. Η αυθεντικοποίηση είναι το κλειδί που κάνει μια ΥΔΚ να είναι επιτυχημένη**[1]**. Η ΑΕ αναλαμβάνει να επιβεβαιώσει ότι τα στοιχεία που θα εισαχθούν σε ένα πιστοποιητικό είναι αυθεντικά πριν από την

έκδοση του, επομένως, είναι αυτονόητο πως διαδραματίζει έναν πολύ σημαντικό ρόλο η οργάνωση μιας ποιοτικής Αρχής Εγγραφής.

8.3.1. Παροχές Υπηρεσιών Αρχής Εγγραφής

Οι βασικές υπηρεσίες που παρέχει η ΑΕ συνοπτικά είναι οι εξής:1.**Αποδοχή των αιτήσεων 2.Ελέγχος στοιχείων και αυθεντικοποίηση χρήστη, 3.Αποδοχή/Απόρριψη αίτησης, 4.Εγγραφή χρήστη, 5.Αποστολή στοιχείων και αιτήσεων στην ΑΠ, 6.Έλεγχος συμμόρφωσης χρήστη με Πολιτική πιστοποίησης.**

Όταν κάποιος χρήστης (οντότητα) θελήσει να εκδόσει ένα ψηφιακό πιστοποιητικό θα απευθυνθεί πρώτα στην Αρχή Εγγραφής στην οποία θα παρουσιάσει τα φυσικά πιστοποιητικά ή τα πιστοποιητικά της επιχείρησης /ιστοσελίδας του και εκείνη θα καθορίσει εάν οι πληροφορίες αυτές είναι ή όχι σωστές και αν όντως αντιστοιχούν στην οντότητα που αιτείται το πιστοποιητικό. Χρησιμοποιεί τις κατάλληλες μεθόδους για να ενισχύσει τον έλεγχο της ταυτότητας του υποψήφιου συνδρομητή. Η διαδικασία πιστοποίησης της ταυτότητας ενός χρήστη που αιτείται διαφοροποιείται ανάλογα με την προσέγγιση που θα κάνει ο χρήστης. Η προσέγγιση αυτή μπορεί να είναι, είτε ηλεκτρονικά είτε με φυσική παρουσία ενός χρήστη παρουσιάζοντας κάποιο επίσημο έγγραφο (π.χ ταυτότητα ή μια απλή επικοινωνία). Στην πρώτη περίπτωση μία μέθοδος είναι να ελέγξει την οντότητα μέσω του ηλεκτρονικού της ταχυδρομείου. Αυτή η διαδικασία χρησιμοποιείται και ως επαλήθευση του χρήστη πριν τη παραλαβή ενός πιστοποιητικού από μια ΑΠ. Στη δεύτερη περίπτωση, η ΑΕ ελέγχει και επικυρώνει τα έγγραφα που χρησιμοποιούνται για να αποδείξουν την ταυτότητα του συνδρομητή. Επιβεβαιώνει ότι ο σκοπός/χρήση του πιστοποιητικού και το μέγεθος του κλειδιού μπορούν να ικανοποιηθούν και είναι σύμφωνα με τους όρους που θέτονται στην πολιτική πιστοποίησης της Υποδομής Δημόσιου Κλειδιού. Αυτές οι πληροφορίες, μόλις αποδειχθούν έγκυρες θα αποσταλούν με ασφαλή τρόπο στην ΑΠ έτσι ώστε να εισαχθούν στο ψηφιακό πιστοποιητικό. Σε αντίθετη περίπτωση η ΑΕ απορρίπτει το αίτημα του χρήστη.

Η αρχή εγγραφής δεν υπογράφει το ψηφιακό πιστοποιητικό, αυτό είναι ένα από τα καθήκοντα της Αρχής Πιστοποίησης. Η ΑΕ παράλληλα με την επαλήθευση όλων των πληροφοριών σχετικά με την ταυτότητα του υποψηφίου συνδρομητή αναλαμβάνει και την εγγραφή του χρήστη. Επίσης χειρίζεται ζητήματα, όπως η εγγραφή να κατέχει ένα διακριτικό και σωστά διατυπωμένο όνομα**[12]**.Τέλος, διαχειρίζεται τις όποιες οικονομικές υποχρεώσεις μπορεί να προκύψουν, που μπορεί να εμποδίσουν την εξέλιξη της διαδικασίας έκδοσης.

8.4. Νομικό Πλαίσιο

Στην «Οδηγία 99/93 του Ευρωπαϊκού Κοινοβουλίου» η οποία αναφέρεται στις ηλεκτρονικές υπογραφές, περιγράφεται και ο τρόπος λειτουργίας των Παροχών Υπηρεσιών Πιστοποίησης. Με το ΠΔ 150/2000 (25.6.2000) ενσωματώθηκαν οι απαιτήσεις της Οδηγίας αυτής και στο Ελληνικό Δίκαιο. Η ΕΕΤΤ ρυθμίζει ζητήματα των αναγνωρισμένων πιστοποιητικών και θέτει το θεσμικό πλαίσιο για την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης. Στο ΠΔ 150/2000 η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) με την υπ. αρ. 248/71 Απόφασή της «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής» (ΦΕΚ 603/Β/16-5-2002) ορίστηκε αρμόδιος φορέας για τις παρακάτω αρμοδιότητες**[2][7]**:

- Τη παροχή ‘εθελοντικής διαπίστευσης’, ύστερα από έγγραφη αίτηση του ενδιαφερόμενου Παρόχου Υπηρεσιών Πιστοποίησης, για την επίτευξη ενός βελτιωμένου επίπεδου παροχής υπηρεσιών πιστοποίησης. Με την ‘εθελοντική διαπίστευση’ απονέμονται δικαιώματα αλλά και υποχρεώσεις στον Πάροχο Υπηρεσιών Πιστοποίησης.
- Την εποπτεία και έλεγχο των εγκατεστημένων στην Ελλάδα Παρόχων Υπηρεσιών Πιστοποίησης, καθώς και των φορέων διαπίστευσης και ελέγχου της συμμόρφωσης των διατάξεων δημιουργίας υπογραφής (υλικού ή λογισμικού που χρησιμοποιείται για την εφαρμογές του ιδιωτικού κλειδιού για τη δημιουργία της ηλεκτρονικής υπογραφής).
- Η επιβολή προστίμων σε Παρόχους Υπηρεσιών Πιστοποίησης, που λειτουργούν ως διαπιστευμένοι, χωρίς να είναι καθώς και την ενημέρωση της Ευρωπαϊκής Επιτροπής για τις επωνυμίες και τις διευθύνσεις όλων των διαπιστευμένων εθνικών Παρόχων Υπηρεσιών Πιστοποίησηςκαι αλλαγές αυτών.

9 *Κεφάλαιο*

ΔΙΑΔΙΚΑΣΙΕΣ ΕΓΓΡΑΦΗΣ - ΕΚΔΟΣΗΣ ΚΑΙ ΔΙΑΧΕΡΙΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Στην ενότητα αυτή αποτυπώνονται οι προδιαγραφές και οι διαδικασίες που απαιτούνται για την εγγραφή μιας οντότητας σε μια υπηρεσία πιστοποίησης καθώς και οι υποχρεώσεις κάθε Αρχής προκειμένου να παρέχει τους απαιτούμενους μηχανισμούς ασφάλειας. Κύριο σημείο μίας επιτυχημένης Υποδομής Δημόσιου Κλειδιού είναι η διαχείριση των εκδοθέντων πιστοποιητικών. Την ευθύνη αυτού αναλαμβάνει ο Πάροχος Υπηρεσιών Πιστοποίησης ο οποίος βεβαιώνει την κατάσταση του πιστοποιητικού για όλη τη διάρκεια ισχύος του αλλά και πέραν αυτής. Οι διαδικασίες από τις οποίες μπορεί να περάσει ένα πιστοποιητικό είναι οι ακόλουθες: ανάκληση, ανανέωση, αναζήτηση, ανάκτηση. Όπως αναφέραμε στα παραπάνω κεφάλαια ο Πάροχος Υπηρεσιών Πιστοποίησης διαθέτει έναν χώρο στον οποίο ο ενδιαφερόμενος χρήστης μπορεί να έχει πρόσβαση, στο οποίο αποθηκεύει όλα τα εκδοθέντα πιστοποιητικά.

9.1. Διαδικασίες Εγγραφής

Με τον όρο εγγραφή μιας οντότητας σε μια Υποδομή Δημόσιου Κλειδιού ορίζεται το σύνολο των διαδικασιών μέσω των οποίων η οντότητα αιτείται την απόκτηση ψηφιακού πιστοποιητικού και παρέχει όλα τα στοιχεία που απαιτούνται για την έγκριση της έκδοσης αυτού**[1]**.

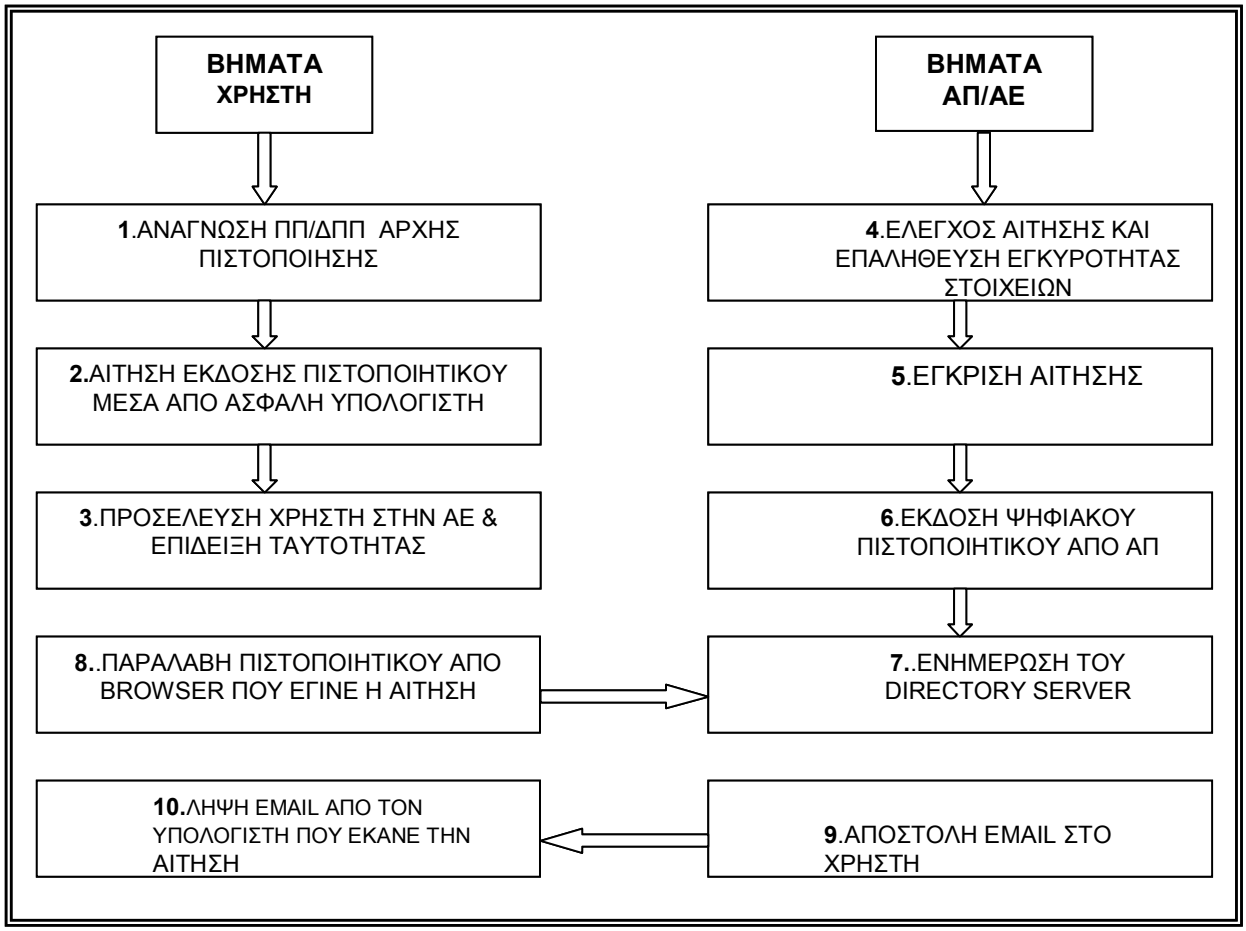
Η οντότητα που επιθυμεί να αποκτήσει ψηφιακό πιστοποιητικό από μια υπηρεσία

πιστοποίησης θα πρέπει αρχικά να ενημερωθεί από τα δημοσιευμένα κείμενα Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης και να κρίνει εάν καλύπτεται από τους κανόνες και όρους που θέτονται. Εφόσον, συμφωνήσει απευθύνεται στην Αρχή Εγγραφής και ξεκινάει την διαδικασία συμπληρώνοντας με τα στοιχεία του τη δομημένη ηλεκτρονική φόρμα αίτησης για έκδοση του ψηφιακού πιστοποιητικού. Η Αρχή Εγγραφής οφείλει να κάνει ενδελεχή έλεγχο της αίτησης για τυχόν λανθασμένα ή παρελλειπόμενα στοιχεία. Εάν τα στοιχεία και ο τύπος του πιστοποιητικού που αιτείται δεν έρχονται σε αντίθεση με τους κανόνες της Πολιτικής Πιστοποίησης η ΑΕ προχωράει στη διαδικασία αυθεντικοποίησης των στοιχείων και της ταυτότητας του αιτούντα. Για την αυθεντικοποίηση απαιτείται η προσκόμιση συγκεκριμένων εγγράφων τα οποία θα λειτουργούν ως αποδεικτικά της ορθότητας και εγκυρότητας των στοιχείων που δηλώθηκαν στην αίτηση και της ταυτοποίησης της οντότητας. Τα έγγραφα που προσκομίζονται καθορίζονται ανάλογα με το επίπεδο ασφάλειας που καλείται να παρέχει η υπηρεσία πιστοποίησης. Η ΑΕ πραγματοποιεί τον κατάλληλο έλεγχο προκειμένου να επαληθεύσει τα στοιχεία που δηλώθηκαν. Στη περίπτωση που ο χρήστης έχει ήδη στη κατοχή του ζεύγος κλειδιών υπογράφει ψηφιακά την αίτηση που αποστέλλει στην ΑΕ για την επιβεβαίωση της αντιστοιχίας του ιδιωτικού του κλειδιού με το δημόσιο επαληθεύοντας την υπογραφή του**[12]**. Εφόσον η ΑΕ ολοκληρώσει την αυθεντικοποίηση η ΑΕ εγκρίνει την αίτηση και καταχωρεί την εγγραφή της οντότητας με τα ακριβή στοιχεία που παρασχέθηκαν. Στη συνέχεια η ΑΕ πραγματοποιεί επικοινωνία με την Αρχή Πιστοποίησης και την ενημερώνει εγκαίρως για την νέα αίτηση. Η ΑΕ μεταβιβάζει την αίτηση μαζί με τα πιστοποιημένα στοιχεία στην Αρχή Πιστοποίησης χρησιμοποιώντας πάντα ασφαλή μέσα επικοινωνίας. Τέλος, η ΑΕ οφείλει να διατηρεί αρχείο με τις αιτήσεις που έλαβε και με τα πιστοποιητικά που προσκομίστηκαν για τη διαδικασία της αυθεντικοποίησης.

9.2. Διαδικασίες Έκδοσης και Παραλαβής

Με τον όρο έκδοση ενός ψηφιακού πιστοποιητικού ορίζεται το σύνολο των διαδικασιών μέσω των οποίων η Αρχή Πιστοποίησης κατασκευάζει το ψηφιακό πιστοποιητικό, το εκδίδει και το παραδίδει έπειτα στον αιτούντα. Η Αρχή Πιστοποίησης με την παραλαβή της εγκεκριμένης αίτησης ξεκινάει τη διαδικασία έκδοσης του πιστοποιητικού. Αρχικά, κατασκευάζει το πιστοποιητικό του οποίου η μορφή είναι σύμφωνη με κάποιο διεθνή αναγνωρισμένο πρότυπο (X.509). Στο πιστοποιητικό που δημιουργεί η ΑΠ περιλαμβάνονται τα ακριβή και επαληθευμένα στοιχεία που έλαβε από την Αρχή Εγγραφής και το δημόσιο κλειδί της οντότητας πιστοποιώντας την αντιστοιχία του με το ιδιωτικό κλειδί. Πληροφορίες που θεωρούνται προσωπικές ή ευαίσθητες που ενδεχομένως να χρησιμοποιήθηκαν με σκοπό την αυθεντικοποίηση του χρήστη δεν περιλαμβάνονται. Έπειτα, η

Αρχή Πιστοποίησης υπογράφει με το ιδιωτικό κλειδί της το πιστοποιητικό για να το επικυρώσει και το εκδίδει για να το παραλάβει ο συνδρομητής. Μετά την έκδοση του πιστοποιητικού η Αρχή πιστοποίησης αποθηκεύει το πιστοποιητικό στους καταλόγους της. Στη συνέχεια ενημερώνει τον δικαιούχο στέλνοντας του ηλεκτρονικό μήνυμα το οποίο περιέχει ένα ασφαλές κωδικό τον οποίο ο χρήστης θα χρησιμοποιήσει για να παραλάβει το πιστοποιητικό του. Η σύνδεση που επικοινωνεί ο χρήστης με την ΑΠ θα πρέπει να είναι κρυπτογραφείται μέσω πρωτοκόλλου ασφαλείας SSL. Η διαδικασία αυτή γίνεται για την αυθεντικοποίηση του παραλήπτη του πιστοποιητικού δηλαδή ότι ο παραλήπτης είναι πράγματι αυτός για τον οποίο εκδόθηκε το πιστοποιητικό. Ο παραλήπτης μόλις λάβει τον μήνυμα θα παραλάβει το πιστοποιητικό του κάνοντας χρήση του κωδικού ασφαλείας. Η διαδικασία παραλαβής θα πρέπει να γίνεται από το ίδιο τερματικό σταθμό, όπου έκανε και την αίτηση για να κάνει άμεσα την αποθήκευση του πιστοποιητικού του στον υπολογιστή του και όχι μεταφορά του έτσι ώστε να διασφαλιστεί η προστασία του πιστοποιητικού. Στην περίπτωση φυσικής παρουσίας του χρήστη για την παραλαβή του πιστοποιητικού η μεταφορά του στον υπολογιστή γίνεται μέσω ασφαλών επιλεγμένων αποθηκευτικών μέσων. Τέλος, η ΑΠ οφείλει να διατηρεί αρχείο με όλες τις διαδικασίες που πραγματοποιήκαν για ένα πιστοποιητικό όπως έγκριση, έκδοση, παραλαβή κτλ



Εικόνα 19:Περιγραφή βημάτων έκδοσης πιστοποιητικού

9.3. Υπηρεσία Διαχείρισης Κλειδιών

Το κρυπτογραφικό σύστημα χρησιμοποιείται για να παρέχει υπηρεσίες ασφάλειας όπως η εμπιστευτικότητα, ακεραιότητα, και επικύρωση. Ωστόσο οι υπηρεσίες αυτές δεν μπορούν να παρασχεθούν εάν η διαχείριση και διανομή των κλειδιών που χρησιμοποιούνται κατά την κρυπτογραφία δεν πραγματοποιείται με ασφαλή τρόπο. Τα κλειδιά δεν πρέπει να τροποποιούνται ,αλλοιώνονται ή να αποκαλύπτονται σε τρίτους. Έτσι εμπιστεύονται κάποια Έμπιστη Τρίτη Οντότητα που εκδίδει διατηρεί και διανέμει τα κλειδιά**[1]**.

Η διαδικασία παραγωγής κλειδιών είναι το πρώτο βήμα μετά την αποδοχή της αίτησης της εγγραφής του χρήστη (οντότητα). Ο χρήστης θα μπορούσε να παράγει ο ίδιος τα κλειδιά του ή να αναθέσει στην υπηρεσία πιστοποίησης την εργασία αυτή. Ωστόσο, το νομικό πλαίσιο της Ευρωπαικής Ένωσης για τις ψηφιακές υπογραφές ορίζει τον Πάροχο Υπηρεσιών Πιστοποίησης ως το μόνο υπεύθυνο για τη παραγωγή και διανομή των κλειδιών που πιστοποιεί. Πριν από την έκδοση των κλειδιών απαιτείται η διαδικασία παραγωγής τυχαίων αριθμών οι οποίοι εισάγονται στον επιλεγμένο αλγόριθμο έτσι ώστε να παραχθούν μη προβλέψιμα κλειδιά.

Η διανομή των κλειδιών που παρήχθησαν πρέπει να πραγματοποιείται μέσα από ασφαλείς διαύλους επικοινωνίας ή με ασφαλείς τρόπους εκτός σύνδεσης (out-of-band),και η μεταφορά τους να γίνεται με εγκεκριμένα αποθηκευτικά μέσα (π.χ ;έξυπνες κάρτες). Επίσης η διανομή των κλειδιών θα πρέπει να γίνεται αποκλειστικά στον κάτοχο του.

Ακόμη είναι απαραίτητη η τήρηση αντιγράφων ασφαλείας των κλειδιών από την Υπηρεσία διαχείρισης κλειδιών. Ο Πάροχος Υπηρεσίων Πιστοποίησης που είναι ο εκδότης των κλειδιών θα πρέπει να παρέχει τους κατάλληλους μηχανισμούς αποθήκευσης των κλειδιών για την ασφαλή διατήρηση τους αλλά και ανάκτηση τους σε περιπτώσεις που απαιτείται. Σημαντικό ρόλο για τη διασφάλιση της εμπιστευτικότητας του κλειδιού είναι οι μέθοδοι αποθήκευσης τους. Η τήρηση των αντιγράφων γίνεται μέσω της αποθήκευσης τους σε ασφαλή αρχεία από την υπηρεσία. Ο αλγόριθμος που θα χρησιμοποιήσει το κλειδί, οι διαμορφώσεις, και οι παράμετροι αποθηκεύονται σε χώρο που πρέπει επίσης να είναι επαρκώς προστατευμένα. Η ανάκτηση ενός δημόσιου κλειδιού γίνεται άμεσα από το πιστοποιητικό μέσω της υπηρεσίας αναζήτησης των καταλόγων που είναι αποθηκευμένο. Ωστόσο η ανάκτηση ενός ιδιωτικού κλειδιού απαιτεί μια διαδικασία πιο σύνθετη. Πρέπει πρώτα ο χρήστης να αιτηθεί στην ΑΕ για ανάκτηση του ιδιωτικού του κλειδιού και έπειτα γίνεται αυθεντικοποίηση της ταυτότητας του προκειμένου να επικυρωθεί η αντιστοιχία του με το δημόσιο κλειδί. Τέλος, οι προαναφερθέντες λειτουργίες της υπηρεσία Διαχείρισης κλειδιών πραγματοποιούνται κατά την κρίση του χρήστη και τη σχέση εμπιστοσύνης του με τον Πάροχο Υπηρεσιών Πιστοποίησης.

9.4. Αναζήτηση Πιστοποιητικού

Για να μπορέσει ένας χρήστης να ενημερωθεί για τα πιστοποιητικά των υπόλοιπων μελών της ΥΔΚ και τα δημόσια κλειδιά που φέρουν θα πρέπει να λειτουργεί μια υπηρεσία αποθήκευσης των πιστοποιητικών που δημιουργούνται. Τα ψηφιακά πιστοποιητικά μετά την έκδοση τους αποθηκεύονται σε καταλόγους που ακολουθούν το πρότυπο X.500. Το πρότυπο X.500 είναι ένα από τα πιο διαδεδομένα πρότυπα για την παροχή υπηρεσιών καταλόγων. Κάθε φορά που δημιουργείται ένα νέο πιστοποιητικό οι κατάλογοι ενημερώνονται και είναι προσβάσιμοι και διαθέσιμοι από όλους τους χρήστες. Έτσι παρέχεται στα μέλη της ΥΔΚ η δυνατότητα να αναζητήσουν πληροφορίες για τα εκδοθέντα πιστοποιητικά Η αναζήτηση πιστοποιητικών πραγματοποιείται για την ενημέρωση του χρήστη για την ισχύ και εγκυρότητα του πιστοποιητικού και ακόμη του παρέχει χρήσιμες πληροφορίες για τους υπόλοιπους χρήστες προκειμένου να επικυρώσει την ταυτότητα τους. Για την παροχή αποδοτικής πρόσβασης των χρηστών στις υπηρεσίες καταλόγων (Directory Services) που ακολουθούν το πρότυπο X.500 γίνεται χρήση του πρωτοκόλλου Lightweight Directory Access Protocol (LDAP) το οποίο έχει ορισθεί από το IETF (RFC 1777) και αρχικά αναπτύχθηκε από το University of Michigan**[2]**. Η αναζήτηση των πιστοποιητικών γίνεται με τη σύνδεση του χρήστη στον ιστότοπο που έχει δημοσιεύσει η ΑΠ τους καταλόγους πιστοποιητικών και λαμβάνει τις πληροφορίες που χρειάζεται συμπληρώνοντας σε μια φόρμα κάποιο στοιχείο του πιστοποιητικού (π.χ.όνομα του κατόχου του, το mail του). Η αναζήτηση του πιστοποιητικού μέσω της ιστοσελίδας της ΑΠ γίνεται για λόγους φιλικότητας προς τον χρήστη, στην ουσία η αναζήτηση των καταλόγων πραγματοποιείται μέσω του πρωτοκόλλου LDAP.

9.5. Ανανέωση Πιστοποιητικού

Τα ψηφιακά πιστοποιητικά έχουν ορισμένη διάρκεια ισχύος την οποία ορίζει η Αρχή Πιστοποίησης που το εξέδωσε. Έτσι με το πέρας της ημερομηνίας το πιστοποιητικό παύει να ισχύει. Τότε μπορεί να πραγματοποιηθεί η ανανέωση του πιστοποιητικού κατόπιν σχετικής αίτησης του χρήστη-συνδρομητή στην ΑΕ. Η αίτηση για ανανέωση του πιστοποιητικού θα πρέπει να γίνεται σε χρονικό διάστημα που ορίζει η ΑΠ στο σχετικό κείμενο της Πολιτικής Πιστοποίησης. Κατά την ανανέωση δεν χρησιμοποιούνται τα ίδια κλειδιά του χρήστη αλλά εκδίδονται νέα ζεύγη και νέο πιστοποιητικό. Ωστόσο, δεν επαναλαμβάνονται οι διαδικασίες εγγραφής του χρήστη εφόσον η ΑΕ διατηρεί αρχείο με καταχωρημένα τα στοιχεία των μελών της ΥΔΚ.

9.6. Ανάκληση Πιστοποιητικού

Στις διαδικασίες διαχείρισης δημόσιων κλειδιών και πιστοποιητικών περιλαμβάνεται και η ανάκληση. Η διαδικασία της ανάκλησης είναι η μετάβαση από μια κατάσταση όπου το πιστοποιητικό ισχύει και δεν έχει λήξει σε μια κατάσταση όπου παύει να είναι ενεργό. Τα ψηφιακά πιστοποιητικά ανακαλούνται είτε απευθείας από την Αρχή Πιστοποίησης είτε κατόπιν αίτησης του συνδρομητή ή κάποιας τρίτης οντότητας όπου αναφέρουν την αιτία για ανάκληση. Τα αιτήματα για ανάκληση πιστοποιητικών, δέχεται και διεκπαιρεώνει η Αρχή Εγγραφής. Η Αρχή Εγγραφής με τη παραλαβή του αιτήματος ανάκλησης πιστοποιητικού οφείλει να αυθεντικοποιήσει τα στοιχεία της αίτησης και να ελέγξει εάν ισχύει ο λόγος ανάκλησης του πιστοποιητικού που ισχυρίστηκε ο αιτών. Οι λόγοι για τους οποίους μια Αρχή Πιστοποίησης μπορεί να ανακαλέσει ένα πιστοποιητικό είναι οι εξής:

- Απώλεια ιδιωτικού κλειδιού της ΑΠ.
- Απώλεια ιδιωτικού κλειδιού του χρήστη.
- Γνωστοποίηση του ιδιωτικού κλειδιού του χρήστη σε κάποια τρίτη οντότητα.
- Υποψία παραβίασης της ιδιωτικότητας του κλειδιού.
- Αλλαγή των στοιχείων που περιέχει το πιστοποιητικό.
- Παραβίαση της συμφωνημένης χρήσης ενός πιστοποιητικού

Για την ορθή επαλήθευση ενός πιστοποιητικού από τους χρήστες απαιτείται η παρουσία ενός αποτελεσματικού μηχανισμού που αφορά την ενημέρωση τους για τα ανακληθέντα πιστοποιητικά. Οι χρήστες θα πρέπει να έχουν τη δυνατότητα να εξετάσουν ανά πάσα στιγμή αν ένα πιστοποιητικό είναι ακόμα σε ισχύ ή έχει ανακληθεί. Επομένως, σε περίπτωση ανάκλησης πιστοποιητικού η Αρχή Πιστοποίησης θα ενεργήσει κατάλληλα ώστε να γνωστοποιήσει στους ενδιαφερόμενους για την κατάσταση του πιστοποιητικού. Κάθε οντότητα πιστοποίησης θα πρέπει να χρησιμοποιεί έναν χώρο αποθήκευσης των ανακληθέντων πιστοποιητικών ο οποίος θα δημοσιεύεται και θα είναι εύκολα προσβάσιμος.

9.6.1. Λίστες Ανάκλησης Πιστοποιητικών

Κάθε Αρχή Πιστοποίησης είναι υπεύθυνη για την δημιουργία και δημοσιοποίηση μιας πλήρης λίστας με τα πιστοποιητικά που έχουν ανακληθεί. Μια από τις πιο διαδεδομένους μεθόδους δημοσίευσης των ανακληθέντων πιστοποιητικών είναι οι Λίστες Ανάκλησης Πιστοποιητικών-ΛΑΠ (Certificate Revocated Lists-CRLs). Η Λίστα Ανάκλησης Πιστοποιητικών είναι ένας κατάλογος πιστοποιητικών και συμπεριλαμβάνεται στο πρότυπο X.509**[42]**. Τα πιστοποιητικά που συμπεριλαμβάνονται στη ΛΑΠ είναι αυτά τα οποία δεν έχουν λήξει αλλά έχουν ανακληθεί και

παύουν να ισχύουν. Η ΑΠ οφείλει να υπογράφει ψηφιακά κάθε ΛΑΠ που δημοσιεύει και να την ενημερώνει περιοδικά ανά χρονικά διαστήματα τα οποία έχει ορίσει στην Δήλωση Διαδικασιών Πιστοποίησης της. Οι χρήστες θα πρέπει να έχουν άμεση και εύκολη πρόσβαση στους καταλόγους πιστοποιητικών στη διεύθυνση που έχει δημοσιεύσει η Αρχή Πιστοποίησης τις ΛΑΠ να τις προμηθεύεται και να ελέγχει τη κατάσταση ενός πιστοποιητικού.

Ωστόσο, λόγω του συνεχούς αυξανόμενου μεγέθους των ΛΑΠ προτάθηκαν οι δ-ΛΑΠ (delta CRL). Η λειτουργία αυτών είναι αρχικά η έκδοση της πρώτης βασικής ΛΑΠ και στη συνέχεια εκδίδονται οι δ-ΛΑΠ οι οποίες περιλαμβάνουν μόνο τις τελευταίες ενημερώσεις. Έτσι ο χρήστης εφόσον αποκτήσει την βασική ΛΑΠ στη συνέχεια προμηθεύεται κάθε φορά τις δ-ΛΑΠ από το σημείο εκείνο και έπειτα που ενημερώθηκε την προηγούμενη φορά**[2]**.

9.6.2. Πρωτόκολλο Κατάστασης Πιστοποιητικών Πραγματικού Χρόνου(OCSP)

Με τη προαναφερθείσα μέθοδο της ΛΑΠ προκύπτουν ορισμένα θέματα σχετικά με τον χρόνο που ενημερώνεται. Στο διάστημα που μεσολαβεί μεταξύ δυο ενημερώσεων είναι πιθανό να ανακληθεί ένα πιστοποιητικό αλλά να χρησιμοποιείται ως έγκυρο με τις αρνητικές συνέπειες που μπορεί να φέρει κάτι τέτοιο. Ένα πράδειγμα είναι αν ένας χρήστης δηλώσει τη κλοπή του ιδιωτικού του κλειδιού η ΑΠ θα ανακαλέσει το πιστοποιητικό του, ωστόσο στο διάστημα μέχρι να ενημερωθεί η ΛΑΠ για το ανακληθέν πιστοποιητικό ένας άλλος χρήστης μπορεί να χρησιμοποιεί το ιδιωτικό κλειδί για κρυπτογραφημένες συναλλαγές και να αυθεντικοποιείται ως τον χρήστη κάτοχο του πιστοποιητικού. Αυτό το πρόβλημα έρχεται να λύσει η χρήση του πρωτοκόλλου (Online Certificate Status Protocol-OCSP). Το πρωτόκολλο OCSP καθορίστηκε στο πρότυπο RFC 2560 δουλεύει πάνω από το HTTP και ενημερώνει τον χρήστη για το αν ένα πιστοποιητικό είναι άκυρο ή έγκυρο σε πραγματικό χρόνο. Ο χρήστης (OCSP Request) στέλνει αίτηση στον εξυπηρετητή με τα πιστοποιητικά που θέλει να ελέγξει την καταστάση τους και ο OCSP (Responder) εφόσον ελέγξει τις απαραίτητες πληροφορίες είτε με επικοινωνία με την ΑΠ είτε με ενημέρωση από τις CRLs στέλνει υπογεγραμμένη απάντηση άμεσα στον χρήστη**[43]**.

10 *Κεφάλαιο*

ΠΡΟΤΥΠΗ ΠΟΛΙΤΙΚΗ ΠΙΣΤΟΠΟΙΗΣΗΣ

10.1. Εισαγωγή

Το παρόν κείμενο περιγράφει την Πολιτική Πιστοποίησης που χρησιμοποιείται από την Αρχή Πιστοποίησης (Α.Π.) της Υ.Δ.Κ. του Πανεπιστημίου Στερεάς Ελλάδας. Η Πολιτική Πιστοποίησης (Π.Π.) διασφαλίζει την έκδοση πιστοποιητικών μετά από έλεγχο στοιχείων ταυτότητας που προσκομίζονται από τον χρήστη στην Αρχή Εγγραφής (ΑΕ) με την φυσική του πρόσβαση. Η παρούσα Πολιτική Πιστοποίησης περιγράφει την έκδοση πιστοποιητικών που εντάσσονται στις εξής κατηγορίες:

- Πιστοποιητικά Χρηστών
- Πιστοποιητικά Εξυπηρετητών

10.1.1. Επισκόπηση

Το παρόν κείμενο περιγράφει την Πολιτική Πιστοποίησης που χρησιμοποιείται από την Αρχή Πιστοποίησης (Α.Π.) της Υ.Δ.Κ. του Πανεπιστημίου Στερεάς Ελλάδας.

Η Πολιτική Πιστοποίησης περιγράφει το σύνολο συγκεκριμένων **κανόνων** το οποίο χρησιμοποιείται για την έκδοση και διαχείριση πιστοποιητικών από την Αρχή Πιστοποίησης. Μία πολιτική πιστοποίησης μπορεί να περιλαμβάνει τις απαιτήσεις για την ταυτοποίηση ενός συνδρομητή προκειμένου να λάβει ένα πιστοποιητικό, τις απαιτήσεις για την λειτουργία της Υ.Δ.Κ, κ.λπ. Επίσης, εξασφαλίζει την εφαρμοσιμότητα ενός πιστοποιητικού στα πλαίσια μιας κοινότητας.

Άρα ο χρήστης που επιθυμεί να λάβει πιστοποιητικό θα πρέπει να αποτιμήσει το σκοπό και τις εφαρμογές που θα το χρησιμοποιήσει.

Μια Δήλωση Διαδικασιών Πιστοποίησης είναι το σύνολο των **διαδικασιών** που υιοθετούνται από μια αρχή πιστοποίησης για την έκδοση, τη διαχείριση, την αναστολή,την ανάκληση, την ανανέωση ή αναζήτηση των ψηφιακών πιστοποιητικών όπως επίσης διαδικασίες λειτουργίας των συστημάτων και νομικά θέματα σύμφωνα με μια συγκεκριμένη πολιτική πιστοποιητικών.

Για την αποτελεσματική και ορθή λειτουργία μιας υποδομής δημόσιου κλειδιού απαιτείται η σύνταξη και δημοσίευση δύο κειμένων: της Πολιτικής Πιστοποίησης Π.Π (Certification Policy-CP) και της Δήλωσης Πρακτικών Πιστοποίησης Δ.Π.Π (Certification Practice Statement-CPS). Ο χρήστης ενός πιστοποιητικού μπορεί να χρησιμοποιήσει την Πολιτική Πιστοποίησης για να αποφασίσει εάν το υπό χρήση πιστοποιητικό καλύπτει της ανάγκες ασφαλείας της εφαρμογής του και συνεπώς αν μπορεί να εμπιστευθεί την εγκυρότητα των στοιχείων που περιέχει.

Όλα τα πιστοποιητικά οφείλουν να περιέχουν αναφορά προς την Πολιτική και τη Δήλωση Διαδικασιών Πιστοποίησης.

10.1.2. Ονομασία και αναγνώριση κειμένου

Το παρόν κείμενο ονομάζεται « Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης Πρότυπης Υποδομής Δημοσίου Κλειδιού» και αποτελεί την τεκμηρίωση και τον κανονισμό λειτουργίας της Υποδομής Δημοσίου Κλειδιού και της Αρχή Πιστοποίησης Πανεπιστημίου Στερεάς Ελλάδας. Σε σύντμηση πρέπει να αναφέρεται ως «ΠΠ- Πανεπιστημίου Στερεάς Ελλάδας».

Σκοπός της Πολιτικής Πιστοποίησης είναι να προσδιορίσει, να καταγράψει και να κοινοποιήσει προς κάθε ενδιαφερόμενο μέρος (π.χ. μέλη της ακαδημαϊκής κοινότητας, εγγραφόμενοι, τρίτα μέρη που βασίζονται στην εγκυρότητα των υπηρεσιών) τις συνθήκες και τις λειτουργικές πρακτικές που εφαρμόζονται ή διέπουν την παροχή των Υπηρεσιών Πιστοποίησης.

Η δομή του παρόντος κειμένου βασίζεται στο πρότυπο IETF RFC-3647 **[32]** με τυχόν ελάχιστες διαφοροποιήσεις οι οποίες κρίθηκαν αναγκαίες.

Ο παγκόσμια μοναδικός Αριθμός Αναγνώρισης (OID) αυτού του εγγράφου

είναι: *χ.χ.χ.χ.χ.χ.χ.χχχχ.α.α.*1.0 όπου:

Τα πρώτα ψηφία *χ* δηλώνουν το παγκόσμια μοναδικό Αριθμός Αναγνώρισης (OID) του παρόντος εγγράφου Πανεπιστημίου Στερεάς Ελλάδας καταχωρημένος από τον οργανισμό ΙΑΝΑ.[4]

Το πρώτο ψηφίο α δηλώνει την Υπηρεσία Πιστοποίησης

[4] Στον παρόν έγγραφο δεν αντιστοιχεί ακόμη (OID) για αυτό και συμβολίζεται με το γράμμα χ.

Το δεύτερο ψηφίο α δηλώνει Δήλωση Διαδικασιών Πιστοποίησης

Το τρίτο και το τέταρτο α είναι ψηφίο του αριθμού έκδοσης (version) της Δήλωσης Διαδικασιών Πιστοποίησης

10.1.3. Συστατικά Υποδομής Δημόσιου Κλειδιού

10.1.3.1. Αρχή Πιστοποίησης

Η Αρχή Πιστοποίησης είναι η οντότητα της Υποδομής Δημόσιου Κλειδιού που εκδίδει τα πιστοποιητικά. Οι Α.Π. διέπονται από εξαιρετικά αυστηρά μέτρα ασφάλειας και δεν δέχονται απευθείας τις αιτήσεις έκδοσης και ανάκλησης πιστοποιητικών από τους συνδρομητές (τελικούς χρήστες). Η Αρχή Εγγραφής δέχεται τις αιτήσεις.

Η Κεντρική Αρχή Πιστοποίησης του Πανεπιστημίου Στερεάς Ελλάδας εκδίδει πιστοποιητικά για το σύνολο των συμμετεχόντων στην Υποδομή Δημόσιου Κλειδιού του Πανεπιστημίου Στερεάς Ελλάδας (πρόσωπα και εξυπηρετητές).

Υπεύθυνο για τη διαχείριση και λειτουργία της Α.Π. του Πανεπιστημίου Στερεάς Ελλάδας με στόχο την πιστοποίηση των χρηστών και των συσκευών του Πανεπιστημίου Στερεάς Ελλάδας είναι το Κέντρο Λειτουργίας Δικτύων του Πανεπιστημίου Στερεάς Ελλάδας

10.1.3.2. Αρχή Εγγραφής

Η Αρχή Εγγραφής είναι οντότητες που είναι αρμόδιες για την πιστοποίηση της ταυτότητας των εγγραφόμενων πριν από την έκδοση του πιστοποιητικού. Οι ΑΕ διαβιβάζουν με ασφαλή τρόπο τις αιτήσεις στην αρμόδια Αρχή Πιστοποίησης. Οι ΑΕ δέχονται τις αιτήσει για την διαχείριση των πιστοποιητικών (έκδοση και ανάκληση).

Το Κέντρο Λειτουργίας Δικτύου Πανεπιστημίου Στερεάς Ελλάδας λειτουργεί ως Αρχή Εγγραφής της Υ.Δ.Κ και εφαρμόζει αυστηρές διαδικασίες πιστοποίησης ταυτότητας των χρηστών της υπηρεσίας πιστοποίησης.

10.1.3.3. Συνδρομητές

Οι τελικοί χρήστες ή συνδρομητές των πιστοποιητικών που εκδίδονται υπό αυτή την Πολιτική Πιστοποίησης είναι το σύνολο των οντοτήτων που υπάγονται στις εξής κατηγορίες:

- Χρήστες και μέλη του Πανεπιστημίου Στερεάς Ελλάδας και των φορέων που συνεργάζονται με αυτό.
- Υπολογιστικά συστήματα που βρίσκονται υπό την διαχείριση χρηστών ή μελών του Πανεπιστημίου Στερεάς Ελλάδας και των φορέων που συνεργάζονται με αυτό.

10.1.3.4. Βασιζόμενα Μέρη/Οντότητες(Relying Parties)

Οι οντότητες που βασίζονται στις παρεχόμενες υπηρεσίες πιστοποίησης ή αλλιώς τα μέρη που βασίζονται στην υπηρεσία (Relying Parties) μπορεί να είναι οποιεσδήποτε οντότητες, εντός ή εκτός της ελληνικής ακαδημαϊκής κοινότητας, οι οποίες χρησιμοποιούν κατ' οποιονδήποτε τρόπο τα τεκμήρια πιστοποίησης (ψηφιακά πιστοποιητικά, ψηφιακές υπογραφές,κλπ) και επαφίενται στις πληροφορίες που περιέχουν.

Για την ακρίβεια, οι οντότητες που εμπιστεύονται την Υπηρεσία Πιστοποίησης είναι τα φυσικά πρόσωπα που, αφού ενημερωθούν και συμφωνήσουν με τους όρους και τις προϋποθέσεις χρήσης του πιστοποιητικού που βρίσκονται στο παρόν κείμενο και αφού ελέγξουν και επαληθεύσουν την εγκυρότητα ενός πιστοποιητικού που έχει εκδοθεί από την Υπηρεσία Πιστοποίησης του Πανεπιστημίου Στερεάς Ελλάδας σύμφωνα με τα παραπάνω, αποφασίζουν τα ίδια αν θα βασισθούν ή όχι στα περιεχόμενα του πιστοποιητικού και κατά συνέπεια να προβούν σε συγκεκριμένες ενέργειες ή να αποκτήσουν τη δικαιολογημένη πεποίθηση για ένα γεγονός.Για την επαλήθευση της εγκυρότητας ενός πιστοποιητικού, ο χρήστης θαπρέπει να ελέγξει ότι:

- Βρίσκεται εντός της περιόδου ισχύος του, δηλαδή έχει ξεκινήσει και δεν έχει λήξει η ισχύς του,
- . Είναι έγκυρα υπογεγραμμένο από έμπιστη Αρχή Πιστοποίησης,
- Δεν έχει ανακληθεί για οποιοδήποτε λόγο,
- Τα στοιχεία ταυτότητας του υποκειμένου που περιέχει ταιριάζουν με τα στοιχεία που παραθέτει ο υπογράφων,
- Η χρήση για την οποία υποβάλλεται το πιστοποιητικό συμφωνεί με την χρήση για την οποία έχει εκδοθεί από την ΑΠ.
- Ακολουθούνται οι όροι και οι συνθήκες που περιγράφονται στο παρόν κείμενο.

10.1.3.5. Άλλοι Συμμετέχοντες

Δεν ορίζεται.

10.1.4. Χρήση Πιστοποιητικού

10.1.4.1. Κατάλληλες Χρήσεις Πιστοποιητικού

Τα πιστοποιητικά που εκδίδονται υπό την παρούσα Πολιτική Πιστοποίησης χρησιμοποιούνται μόνο για:

- ακαδημαϊκούς ή εκπαιδευτικούς σκοπούς

- στα πλαίσια της λειτουργίας του Πανεπιστημίου Στερεάς Ελλάδας για ενέργειες που δεν εμπεριέχουν οικονομικές συναλλαγές
- Στα πλαίσια λειτουργίας του Πανεπιστημίου Στερεάς Ελλάδας, για διαχειριστικούς σκοπούς

α) Στην υπογραφή ενός ηλεκτρονικού εγγράφου από ένα φυσικό πρόσωπο με τη χρήση του ψηφιακού πιστοποιητικού του και κατά προτίμηση με τη χρήση δημιουργίας σύνοψης υπογραφής ώστε να εξασφαλίζονται τουλάχιστο τα παρακάτω χαρακτηριστικά: 1) η αυθεντικότητα της προέλευσης (authenticity), 2) η ακεραιότητα του υπογεγραμμένου κειμένου (integrity) δηλαδή ότι το περιεχόμενό του δεν έχει τροποποιηθεί από τη στιγμή της υπογραφής του, και 3) η δέσμευση του υπογράφοντα ως προς το περιεχόμενο του εγγράφου και η μη άρνηση της υπογραφής του (non-repudiation).

β) Στην υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου, για την εξασφάλιση της αυθεντικότητας της διεύθυνσης ηλεκτρονικού ταχυδρομείου του αποστολέα και για όλες τις ιδιότητες που περιγράφηκαν στο Κεφάλαιο 4.

γ) Στην απόδειξη της ταυτότητας (Authentication) ενός φυσικού προσώπου κατά την επικοινωνία τους με άλλες οντότητες, εξασφαλίζοντας επιπλέον χαρακτηριστικά ασφάλειας, ισχυρότερα από αυτά που παρέχει η κλασική μέθοδος πρόσβασης με συνθηματικό χρήστη.

δ) Στην κρυπτογράφηση εγγράφων και μηνυμάτων με την χρήση του δημοσίου κλειδιού κάποιας οντότητας, εξασφαλίζοντας ότι μόνο ο επιδιωκόμενος παραλήπτης και κάτοχος του αντίστοιχου ιδιωτικού κλειδιού μπορεί να αποκρυπτογραφήσει και να διαβάσει το έγγραφο ή το μήνυμα.

στ) Στην υλοποίηση ασφαλών δικτυακών πρωτοκόλλων, όπως τα SSL,secure DNS, IPSec κλπ.

Όλες οι χρήσεις των πιστοποιητικών θα πρέπει να έχουν απαιτούμενο επίπεδο ασφάλειας ίσο ή χαμηλότερο από αυτό της διαδικασίας έκδοσης των πιστοποιητικών.

10.1.4.2. Απαγορευμένες Χρήσεις Πιστοποιητικού

Τα πιστοποιητικά δεν επιτρέπεται να χρησιμοποιηθούν για εμπορικές συναλλαγές ή για συναλλαγές που αφορούν μεταφορά χρημάτων όπως επίσης και για συναλλαγές που εμπεριέχουν νομικές δεσμεύσεις.

10.1.5. Διαχειριστής Πολιτικής

10.1.5.1. Οργάνωση που διαχειρίζεται το έγγραφο

Το Κέντρο Λειτουργίας Δικτύου του Πανεπιστημίου Στερεάς Ελλάδας

10.1.5.2. Πρόσωπο επικοινωνίας

Το Κέντρο Λειτουργίας Δικτύου του Πανεπιστημίου Στερεάς Ελλάδας

10.1.5.3. Πρόσωπο που κρίνει την συμμόρφωση Δ.Δ.Π.

Το Κέντρο Λειτουργίας Δικτύου του Πανεπιστημίου Στερεάς Ελλάδας

10.1.5.4. Διαδικασίες έγκρισης Πάροχου Υπηρεσιών Πιστοποίησης

Δεν ορίζεται.

10.1.6. Ορισμοί και ακρωνύμια

Στον παρακάτω Πίνακα 11.1 αναφέρονται τα ακρωνύμια, οι όροι,οι συντομεύσεις και οι αντίστοιχοι αγγλικοί όροι αυτών που συναντάμε στο παρόν Κεφάλαιο 11 Πρότυπη Πολιτική Πιστοποίησης:

Αναγνωριστικό Αντικειμένου ΑΑ
Object Identifier OID
Αρχή Εγγραφής ΑΕ
Registration Authority RA
Αρχή Πιστοποίησης ΑΠ
Certification Authority CA
Δήλωση Διαδικασιών Πιστοποίησης ΔΔΠ
Δημόσιο Κλειδί Public Key
Διακεκριμένο Όνομα ΔΟ
Distinguished Name DN
Έμπιστη Τρίτη Οντότητα ΕΤΟ
Trusted Third Party TTP
Ιδιωτικό Κλειδί Private Key
Κοινό Όνομα ΚΟ
CommonName CN
Λίστα Ανάκλησης Πιστοποιητικών ΛΑΠ
Certificate Revocation List CRL
Όνομα Οργανισμού Ο
OrganizationName O

Οργανωτική Μονάδα ΟΜ
Organizational Unit OU
Όνομα Χώρας Χ
CountryName C
Πιστοποιητικό Certificate
Πολιτική Πιστοποίησης ΠΠ
Certification Policy CP
Υποδομή Δημοσίου Κλειδιού ΥΔΚ
Public Key Infrastructure PKI
Ψηφιακά Πιστοποιητικά για Αρχή Πιστοποίησης Certification Authority Digital Certificates
Ψηφιακά Πιστοποιητικά για Εξυπηρετητές Server Digital Certificates
Ψηφιακά Πιστοποιητικά Ταυτότητας Personal Identity Digital Certificates
Ψηφιακά Πιστοποιητικά για Υπογραφή Αντικειμένων Object-Signing Digital Certificates
Συνδρομητής Subscriber
Οντότητα που βασίζεται στην υπηρεσία Relying Party
Αποθήκη Δεδομένων Data Repository
Αυθεντικοποίηση Authentication
Secure Socket Layer SSL

Πίνακας 1:Όροι-Ακρωνύμια-Συντομεύσεις Πρότυπης Πολιτική Πιστοποίησης

10.2. Υποχρεώσεις Δημοσίευσης και Αποθήκευσης

10.2.1. Αποθήκες

Η Υ.Δ.Κ Πανεπιστημίου Στερεάς Ελλάδας διαθέτει κεντρική αποθήκη δεδομένων κάνοντας χρήση καταλόγων, όπου δημοσιεύονται τα κείμενα πολιτικής πιστοποίησης και διαδικασιών πιστοποίησης, το πιστοποιητικό της Αρχής Πιστοποίησης και τελικά πιστοποιητικά συνδρομητών/εξυπηρετητών.

10.2.2. Δημοσίευση πληροφοριών ψηφιακών πιστοποιητικών

Η ΑΠ τηρεί αποθήκη διαθέσιμη μέσω του διαδικτύου στην οποία δημοσιεύει το Ψηφιακό Πιστοποιητικό της Αρχής Πιστοποίησης (τύπου Χ.509), τα Ψηφιακά Πιστοποιητικά που εκδίδονται

σύμφωνα με τη Δήλωση Διαδικασιών Πιστοποίησης, την τρέχουσα Λίστα Ανάκλησης Πιστοποιητικών-ΛΑΠ, τα κείμενο της Πολιτικής και Διαδικασιών Πιστοποίησης .

Η ΑΠ εκτελεί όλες τις ενέργειες για την αδιάλειπτη, όσο είναι εφικτό, διαθεσιμότητα της αποθήκης της. Η ηλεκτρονική διεύθυνση της αποθήκης της Υποδομής Δημοσίου Κλειδιού Πανεπιστημίου Στερεάς Ελλάδας είναι: (http://www.dib.ucg.gr/)

Επιπλέον, είναι δυνατή η αποθήκευση και αναζήτηση πιστοποιητικών και Λ.Α.Π στην υπηρεσία καταλόγου του Πανεπιστημίου Στερεάς Ελλάδας

10.2.3. Συχνότητα δημοσίευσης

Τα πιστοποιητικά που εκδίδονται από την ΑΠ θα δημοσιοποιούνται άμεσα, μετά την έκδοση άλλα και παραλαβή τους από τον εγγραφόμενο. Η ΛΑΠ θα εκδίδεται τουλάχιστον κάθε εξήντα (60) ημέρες. Η Λ.Α.Π ενημερώνεται σύμφωνα με τη παράγραφο 10.4.9.7.

10.2.4. Έλεγχος πρόσβασης στις αποθήκες

Η πρόσβαση στο τμήμα της αποθήκης που περιέχει τα πιστοποιητικά που έχουν εκδοθεί είναι δημόσια και γίνεται μόνο με τη μορφή αναζήτησης. Η αναζήτηση γίνεται είτε με το σειριακό αριθμό (serial number) του πιστοποιητικού, οπότε προβάλλεται μια εγγραφή, είτε με το Διακεκριμένου Ονόματος (ΔΟ) του αντικειμένου του πιστοποιητικού, οπότε είναι πιθανό να επιστραφεί λίστα πιστοποιητικών.

10.3. Ταυτοποίηση και Αυθεντικοποίηση Ταυτότητας

10.3.1.1. Ονομασία

Τα ονόματα που χρησιμοποιούνται για την έκδοση των πιστοποιητικών εξαρτώνται από την κατηγορία του πιστοποιητικού και προτείνεται να ακολουθούν το πρότυπο Διακεκριμένου Ονόματος Χ.501 ως μοναδικό χαρακτηριστικό όνομα μίας οντότητας-τελικός συνδρομητής.

10.3.1.2. Τύπος Ονομασίας

10.3.1.2.1. Πιστοποιητικά χρήστη

Τα πιστοποιητικά χρήστη θα περιλαμβάνουν:

- τη συντομογραφία της χώρας στην οποία ανήκει ο χρήστης στο χαρακτηριστικό ‘C’. (π.χ. C=GR)

- τη τοποθεσία της χώρας στην οποία ανήκει στο χαρακτηριστικό 'ST' (π.χ ST=Lamia)
- την ονομασία του Πανεπιστημίου Στερεάς Ελλάδας στο χαρακτηριστικό 'O' (π.χ. O=University of Lamia)
- τη συντομογραφία της χώρας στην οποία ανήκει το Πανεπιστήμιο Στερεάς Ελλάδας στο χαρακτηριστικό 'OU' (π.χ. OU=GR)
- την απόδοση σύμφωνα με τον καθορισμένο τύπο ονομάτων του πλήρους ονόματος του συνδρομητή ακριβώς όπως αναγράφεται στα έγγραφα που αποδεικνύουν την ταυτότητα του (π.χ. ταυτότητα, δελτίο ταυτότητας φοιτητή) στο χαρακτηριστικό Common Name-'CN'
- τη διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη στο χαρακτηριστικό 'emailAddress'.

Επίσης συνιστάται να αναγράφεται και το όνομα της ομάδα του Πανεπιστημίου Στερεάς Ελλάδας (π.χ. φοιτητής, μέλος ΔΕΠ) στην οποία ανήκει ο συνδρομητής.

10.3.1.2.2. Πιστοποιητικά Εξυπηρετητή

Τα πιστοποιητικά εξυπηρετητών θα περιλαμβάνουν:

- το πλήρες όνομα του εξυπηρετητή κατά την υπηρεσία ονοματολογίας (Fully Qualified Domain Name – FQDN, Domain Name System DNS)
- την ονομασία του Πανεπιστημίου Στερεάς Ελλάδας στο χαρακτηριστικό 'O'.
- τη συντομογραφία της χώρας που ανήκει το Πανεπιστήμιο Στερεάς Ελλάδας στο χαρακτηριστικό 'OU'.

10.3.1.2.3. Πιστοποιητικά της Αρχής Πιστοποίησης

Το πιστοποιητικό της Α.Π. θα περιλαμβάνει

- τη συντομογραφία της χώρας στην οποία ανήκει στο χαρακτηριστικό 'C'
- την τη τοποθεσία της χώρας στην οποία ανήκει στο χαρακτηριστικό 'ST' (π.χ ST=Lamia)
- το όνομα της ΑΠ. του Πανεπιστημίου Στερεάς Ελλάδας που περιέχει λεκτική απόδοση του όρου ΑρχήΠιστοποίησης (Certification Authority) στο χαρακτηριστικό 'CN'

- την ονομασία του Πανεπιστημίου Στερεάς Ελλάδας στο χαρακτηριστικό 'O'
- τη συντομογραφία της χώρας στην οποία ανήκει στο χαρακτηριστικό 'OU'
- τη διεύθυνση ηλεκτρονικού ταχυδρομείου του διαχειριστικού φορέα στο 'emailAddress'.

10.3.1.3. Υποχρέωση τα ονόματα να έχουν συγκεκριμένο νόημα

Τα ονόματα που περιλαμβάνονται στα πιστοποιητικά χρηστών θα πρέπει να έχουν άμεση σχέση με τον συνδρομητή/κάτοχο του πιστοποιητικού και να τον χαρακτηρίζουν.

10.3.1.4. Δυνατότητα διατήρησης ανωνυμίας ή χρήση ψευδώνυμου του συνδρομητή

Δεν ορίζεται.

10.3.1.5. Κανόνες σύνταξης ονομασίας

Μια ονομασία συντάσσεται ορθά όπως ορίζεται στην ενότητα 10.3.1.και ονομάζεται Διακεκριμένο Όνομα (ΔΟ).

10.3.1.6. Μοναδικότητα Ονομασίας

Τα ονόματα συντάσσονται ανάλογα με την κατηγορία του πιστοποιητικού. Το Διακεκριμένο Όνομα (ΔΟ) των συνδρομητών προτείνεται να είναι μοναδικό για την Α.Π. που εκδίδει το πιστοποιητικό.

10.3.1.7. Διαδικασία επίλυσης διαφορών σχετικά με την κυριότητα Ονόματος και εμπορικών σημάτων.

Δεν ορίζεται.

10.3.2. Αρχική Επαλήθευση ταυτότητας

10.3.2.1. Μέθοδοι απόδειξης κατοχής ιδιωτικού κλειδιού

Η Αρχή Εγγραφής είναι η αρμόδια αρχή που πρέπει να επαληθεύσει ότι ο χρήστης που αιτείται ένα πιστοποιητικό κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιλαμβάνεται στο προς έκδοση πιστοποιητικό. Αυτό επιτυγχάνεται με την εξής διαδικασία :

- Πιστοποιείται η ταυτότητα του συνδρομητή.

- Υποβάλλεται αίτηση για έκδοση πιστοποιητικού η οποία περιέχει το δημόσιο κλειδί του συνδρομητή και έχει υπογραφεί με το ιδιωτικό κλειδί του συνδρομητή.
- Ελέγχει την αντιστοιχία των κλειδιών επικυρώνοντας την υπογραφή με το δημόσιο κλειδί του χρήστη.

10.3.2.2. Αυθεντικοποίηση ταυτότητας οργανισμού

Η Αρχή Εγγραφής προτείνεται να επιβεβαιώνει το όνομα του οργανισμού που αναγράφεται στο πιστοποιητικό. Ο οργανισμός υποβάλλει εγγράφως αποδεικτικό της σχέσης του με το Πανεπιστημίου Στερεάς Ελλάδας

10.3.2.3. Αυθεντικοποίηση ταυτότητας φυσικού προσώπου

10.3.2.3.1. Αυθεντικοποίηση χρήστη

Η Αρχή Εγγραφής θα πιστοποιεί το όνομα του χρήστη που αναγράφεται στο πιστοποιητικό με φυσική παρουσία του προσώπου και προσκόμιση επίσημου εγγράφου που περιέχει φωτογραφία του χρήστη(π.χ. αστυνομική ταυτότητα, διαβατήριο, δίπλωμα οδήγησης, φοιτητική ταυτότητα, ΟΧΙ ΠΑΣΟ) και το οποίο θεωρείται αξιόπιστο. Όλα τα πιστοποιητικά φυσικών προσώπων που εκδίδονται θα πρέπει να ελέγχονται για ταυτοπροσωπία.

Εάν η ΑΕ έχει ήδη εκτελέσει διαδικασία φυσικής ταυτοποίησης του χρήστη στο παρελθόν (π.χ. για την εκχώρηση κωδικού πρόσβασης ή λογαριασμού e-mail) τότε δεν είναι απαραίτητη η επανάληψη της διαδικασίας, αλλά θεωρείται αρκετή μία απλή επιβεβαίωση της αίτησης μέσω της πιστοποιημένης διεύθυνσης ηλεκτρονικής αλληλογραφίας του αιτούντος.

10.3.2.3.2. Αυθεντικοποίηση εξυπηρετητή

Η Αρχή Εγγραφής πιστοποιεί την εξουσιοδότηση του αιτούντος για τη λειτουργία του εξυπηρετητή και τη συμμόρφωση του με την Πολιτική Πιστοποίησης. Η ταυτότητα του αιτούντος πιστοποιείται σύμφωνα με τις διαδικασίες της παραγράφου 10.3.2.Ο συνδρομητής συμπληρώνει την αίτηση για έκδοση πιστοποιητικού σε ιστοσελίδα όπου πρέπει να πιστοποιηθεί η ταυτότητά του παρουσιάζοντας το προσωπικό πιστοποιητικό του.

10.3.3. Μη-ελεγχόμενες πληροφορίες συνδρομητή

Οι πληροφορίες που δεν ελέγχονται δεν συμπεριλαμβάνονται στις πληροφορίες που φέρει το ψηφιακό πιστοποιητικό του χρήστη.

10.3.4. Αυθεντικοποίηση Αρχής Πιστοποίησης

Δεν ορίζεται.

10.3.5. Κριτήρια για διαλειτουργικότητα

Δεν ορίζεται.

10.3.6. Πιστοποίηση και Αυθεντικοποίηση για επανάληψη αίτησης χρήστη

Η ΑΠ ΔΕΝ εκδίδει νέο πιστοποιητικό με το ίδιο κλειδί.

10.3.6.1. Επαλήθευση ταυτότητας για συνηθισμένη αίτηση έκδοσης νέου κλειδιού-πιστοποιητικού

Ο χρήστης μπορεί να κάνει νέα αίτηση για έκδοση νέου κλειδιού-πιστοποιητικού δέκα (10) μέρες πριν την λήξη του ισχύοντος πιστοποιητικού, ακολουθώντας την διαδικασία που περιγράφεται στην παράγραφο 10.3.2.

10.3.6.2. Αυθεντικοποίηση ταυτότητας για αίτηση έκδοσης νέου κλειδιού-πιστοποιητικού μετά από ανάκληση .

Μετά από ανάκληση ο χρήστης μπορεί να κάνει νέα αίτηση για έκδοση νέου κλειδιού-πιστοποιητικού και να επαναλάβει τη διαδικασία που περιγράφεται στην παράγραφο 10.3.2.

10.3.7. Αυθεντικοποίηση ταυτότητας για αιτήματα ανάκλησης

Η ΑΕ πιστοποιεί την ταυτότητας του συνδρομητή για την αποδοχή ενός αιτήματος ανάκλησης πιστοποιητικού. Η ΑΕ αποδέχεται τις αιτήσεις ανάκλησης πιστοποιητικού που έχουν υπογραφεί ψηφιακά από έγκυρα πιστοποιητικά που δεν έχουν ανακληθεί ή λήξει πριν την ολοκλήρωση της αίτησης ανάκλησης.

Επίσης, προτείνεται η ΑΠ να χρησιμοποιεί επιπρόσθετες μεθόδους πιστοποίησης όπως η χρήση ειδικού μυστικού κωδικού για την ανάκληση του πιστοποιητικού που έχει δοθεί στον συνδρομητή κατά την παραλαβή του πιστοποιητικού του.

10.4. Απαιτήσεις λειτουργίας, κύκλος ζωής πιστοποιητικών

10.4.1. Αιτήσεις για πιστοποιητικά

10.4.1.1. Ποιος δικαιούται να καταθέσει αίτημα για έκδοση πιστοποιητικού

Αιτήσεις για έκδοση πιστοποιητικού δικαιούνται να καταθέσουν μόνο οι συνδρομητές που περιγράφονται στην παράγραφο 10.1.3.3.

10.4.1.2. Διαδικασία κατάθεσης αιτήματος για έκδοση πιστοποιητικού και ευθύνες

Το Διακεκριμένο Όνομα του πιστοποιητικού του αιτούντος πρέπει να είναι σύμφωνο με όσα αναφέρονται στην παράγραφο 10.3.2. Η πιστοποίηση της ταυτότητας του χρήστη πρέπει να έχει γίνει σύμφωνα με όσα ορίζονται στο κεφάλαιο 10.3.

Ο συνδρομητής υποβάλει τη ηλεκτρονική αίτηση για έκδοση του πιστοποιητικού στην ιστοσελίδα της Αρχής Πιστοποίησης http://www.dib.ucg.gr/.

10.4.2. Επεξεργασία των αιτήσεων πιστοποιητικών

10.4.2.1. Διαδικασίες πιστοποίησης και αυθεντικοποίησης συνδρομητή

Η επεξεργασία των αιτήσεων γίνεται με βάση όσων αναφέρονται στην παράγραφο 10.3.2. Όλα τα αιτήματα ελέγχονται ως προς την εγκυρότητά τους και ελέγχεται η απόδειξη ταυτότητας των συνδρομητών καθώς και η ύπαρξη ή όχι σχέσης τους με το Πανεπιστημίου Στερεάς Ελλάδας.

10.4.2.2. Έγκριση ή απόρριψη αιτήσεων πιστοποιητικών

Μετά από όλους τους ελέγχους ταυτότητας του αιτούμενου χρήστη, ελέγχεται και το περιεχόμενο της ψηφιακής αίτησης πιστοποιητικού. Σε περίπτωση που ο αιτούμενος δεν δικαιούται ψηφιακό πιστοποιητικό ή η ψηφιακή αίτηση δεν έχει συμπληρωθεί σωστά, η αίτηση απορρίπτεται. Διαφορετικά η αίτηση εγκρίνεται.

10.4.2.3. Χρόνος επεξεργασίας των αιτήσεων πιστοποιητικών

Τα αιτήματα πιστοποιητικών εξυπηρετούνται σε διάστημα το πολύ δέκα πέντε (15) εργάσιμων ημερών, εκτός από τις περιπτώσεις ανωτέρας βίας.

10.4.3. Έκδοση πιστοποιητικών

10.4.3.1. Διαδικασίες Αρχών Πιστοποίησης κατά την έκδοση πιστοποιητικών

Τα πιστοποιητικά εκδίδονται μετά την ασφαλή μεταφορά των αιτήσεων από την Αρχή Εγγραφής στην ΑΠ. Η Α.Π. πρέπει να ενημερώνει το συνδρομητή για την έκδοση του πιστοποιητικού του. Στην περίπτωση που απορρίψει την έκδοση του πιστοποιητικού του συνδρομητή οφείλει να ενημερώνει τον συνδρομητή για την απόρριψη της αίτησης αλλά και για τους λόγους απόρριψης της αίτησης του.

10.4.3.2. Ενημέρωση του συνδρομητή από την ΑΠ σχετικά με την έκδοση του πιστοποιητικού

Η ΑΠ ενημερώνει το συνδρομητή για την έκδοση ή απόρριψη έκδοσης του πιστοποιητικού με αποστολή μηνύματος μέσω ηλεκτρονικού ταχυδρομείου. Στο ίδιο μήνυμα και εφόσον η αίτηση έχει γίνει αποδεκτή, ζητείται από το συνδρομητή η αποδοχή και παραλαβή του πιστοποιητικού από συγκεκριμένη ιστοσελίδα της ΑΠ.

10.4.4. Αποδοχή των πιστοποιητικών

10.4.4.1. Συμπεριφορά που αποτελεί την παραλαβή πιστοποιητικών

Η παραλαβή των πιστοποιητικών θα γίνεται μέσω της ασφαλής ιστοσελίδας της ΑΠ και αποκλειστικά από τον χρήστη που αιτήθηκε την έκδοση του πιστοποιητικού.Επίσης προτείνεται η παραλαβή του πιστοποιητικού να πραγματοποιείται από τον ίδιο υπολογιστή που έγινε η αίτηση αλλά και που θα αποθηκευτεί το πιστοποιητικό προκειμένου να αποφευχθεί η μεταφορά του πιστοποιητικού για λόγους ασφαλείας.

10.4.4.2. Δημοσίευση πιστοποιητικών από τις ΑΠ

Οι ΑΠ δημοσιεύουν τα πιστοποιητικά μόνο εφόσον έχει γίνει παραλαβή τους από τους δικαιούχους σύμφωνα με την παράγραφο 10.4.4.1.

10.4.4.3. Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικών

Δεν προβλέπεται ενημέρωση άλλων οντοτήτων για τα νέα πιστοποιητικά.

10.4.5. Ζεύγος κλειδιών και χρήσεις των πιστοποιητικών

10.4.5.1. Χρήσεις των κλειδιών και πιστοποιητικών από τους συνδρομητές

Οι συνδρομητές της ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας επιτρέπεται να χρησιμοποιούν τα ιδιωτικά κλειδιά και τα πιστοποιητικά τους σε χρήσεις που περιγράφονται στην παράγραφο 10.6.1.7.

10.4.5.2. Χρήσεις των κλειδιών και πιστοποιητικών τα βασιζόμενα μέρη (Relying parties)

Τα μέρη που βασίζονται στην υπηρεσία μπορούν να χρησιμοποιούν τα δημόσια κλειδιά και τα πιστοποιητικά των συνδρομητών της Υποδομής Δημοσίου Κλειδιού Πανεπιστημίου Στερεάς Ελλάδας ακολουθώντας τα όσα αναγράφονται στην παράγραφο 10.1.3.4.

Οι λειτουργίες που μπορούν να εκτελέσουν είναι:

- Επαλήθευση ψηφιακά υπογεγραμμένων μηνυμάτων Ηλεκτρονικού Ταχυδρομείου.
- Κρυπτογράφηση μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- Επαλήθευση ψηφιακά υπογεγραμμένων κειμένων/κώδικα εφαρμογών
- Κρυπτογράφηση αρχείων και δεδομένων καθώς και καναλιών επικοινωνίας
- Έλεγχος ταυτότητας (authentication)
- Έλεγχος δικαιώματος πρόσβασης (authorization)

10.4.6. Ανανέωση πιστοποιητικών

10.4.6.1. Συνθήκες κατά τις οποίες μπορεί να γίνει ανανέωση πιστοποιητικών

Ισχύει ότι αναφέρεται στη παράγραφο 10.3.3

10.4.6.2. Ποιος μπορεί να καταθέσει αίτημα ανανέωσης πιστοποιητικού

Δεν ορίζεται.

10.4.6.3. Διαδικασίες των ΑΚ, ΑΠ για επεξεργασία αιτημάτων ανανέωσης

Δεν ορίζεται.

10.4.6.4. Ενημέρωση συνδρομητών για τα ανανεωμένα πιστοποιητικά

Δεν ορίζεται.

10.4.6.5. Αποδοχή ανανεωμένων πιστοποιητικών

Δεν ορίζεται.

10.4.6.6. Δημοσίευση ανανεωμένων πιστοποιητικών

Δεν ορίζεται.

10.4.6.7. Ενημέρωση άλλων οντοτήτων για την ανανέωση πιστοποιητικών

Δεν ορίζεται.

10.4.7. Επανέκδοση κλειδιών

10.4.7.1. Συνθήκες επανέκδοσης κλειδιών

Επανέκδοση κλειδιών πιστοποιητικών επιτρέπονται όταν πλησιάζει η λήξη ισχύοντος πιστοποιητικού ή όταν έχει ανακληθεί πιστοποιητικό και πρέπει να εκδοθεί νέο.

10.4.7.2. Ποιος μπορεί πραγματοποιήσει αίτημα επανέκδοσης κλειδιών Πιστοποιητικών

Αίτημα επανέκδοσης κλειδιών-πιστοποιητικών δικαιούται να κάνει οι συνδρομητές-κάτοχοι πιστοποιητικών των οποίων το πιστοποιητικό ή το κλειδί τους έχει λήξει ή ανακληθεί.

10.4.7.3. Διαδικασίες των ΑΕ και ΑΠ για αιτήματα επανέκδοσης κλειδιών

Ακολουθείται η διαδικασία που προβλέπεται για έκδοση νέων πιστοποιητικών όπως περιγράφεται στην παράγραφο 10.4.3. Οι δικαιούχοι συνδρομητές, λαμβάνουν μήνυμα ηλεκτρονικού ταχυδρομείου από την Αρχή Εγγραφής δεκαπέντε (15) μέρες πριν τη λήξη του πιστοποιητικού τους και ενημερώνονται για την επικείμενη λήξη του.

10.4.7.4. Ενημέρωση συνδρομητών για τα πιστοποιητικά όπου πραγματοποιήθηκε επανέκδοση κλειδιού

Ακολουθείται η ίδια διαδικασία με την έκδοση νέων πιστοποιητικών όπως περιγράφεται στην παράγραφο 10.4.3.2.

10.4.7.5. Αποδοχή πιστοποιητικών στα οποία επανεκδόθηκε κλειδί

Ισχύει ότι αναφέρεται στη παράγραφο 10.4.4.1.

10.4.7.6. Δημοσίευση πιστοποιητικών στα οποία επανεκδόθηκε κλειδί

Το πιστοποιητικό με το νέο κλειδί δημοσιεύεται, σύμφωνα με τις διαδικασίες της αποθήκης όπως περιγράφονται στην παράγραφο 10.4.4.2.

10.4.7.7. Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικών με νέο κλειδί

Δεν προβλέπεται ενημέρωση άλλων οντοτήτων για τα πιστοποιητικά στα οποία το κλειδί επανεκδόθηκε.

10.4.8. Μεταβολή Πιστοποιητικών

10.4.8.1. Συνθήκες κατά τις οποίες μπορεί να γίνει μεταβολή

πιστοποιητικών

Δεν επιτρέπεται η μεταβολή στοιχείων στα πιστοποιητικά. Σε περίπτωση που έχει γίνει λάθος κατά την έκδοση του πιστοποιητικού (ορθογραφικό ή άλλο), το πιστοποιητικό ανακαλείται και ακολουθείται η διαδικασία έκδοσης νέου πιστοποιητικού, όπως περιγράφεται στην παράγραφο 10.4.3.

10.4.8.2. Πώς μπορεί να γίνει αίτημα μεταβολής πιστοποιητικών

Δεν επιτρέπεται η μεταβολή στοιχείων στα πιστοποιητικά.

10.4.8.3. Διαδικασίες των ΑΚ, ΑΠ για αιτήματα μεταβολής πιστοποιητικών

Δεν επιτρέπεται η μεταβολή στοιχείων στα πιστοποιητικά.

10.4.8.4. Ενημέρωση συνδρομητών για τα πιστοποιητικά που μεταβλήθηκαν

Δεν επιτρέπεται η μεταβολή στοιχείων στα πιστοποιητικά.

10.4.8.5. Αποδοχή πιστοποιητικών που μεταβλήθηκαν

Δεν επιτρέπεται η μεταβολή στοιχείων στα πιστοποιητικά.

10.4.8.6. Δημοσίευση πιστοποιητικών που μεταβλήθηκαν

Δεν επιτρέπεται η μεταβολή στοιχείων στα πιστοποιητικά.

10.4.8.7. Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικών που μεταβλήθηκαν

Δεν επιτρέπεται η μεταβολή στοιχείων στα πιστοποιητικά.

10.4.9. Αναστολή και ανάκληση πιστοποιητικών

10.4.9.1. Συνθήκες ανάκλησης

Το πιστοποιητικό ανακαλείται υπό τις εξής συνθήκες:

- Τα στοιχεία που περιέχει το πιστοποιητικό έχουν αλλάξει στοιχεία ή διαπιστωθεί ότι είναι λανθασμένα.
- Το ιδιωτικό κλειδί εκτεθεί ή χαθεί
- Μη έγκαιρη παραλαβή του πιστοποιητικού από τον συνδρομητή
- Η χρήση του πιστοποιητικού δεν είναι σύμφωνη με τη δήλωση διαδικασιών πιστοποίησης/πολιτική πιστοποίησης.

- Διακοπή σχέσης συνδρομητή με το Πανεπιστήμιο Στερεάς Ελλάδος (π.χ αποφοίτηση)

10.4.9.2. Ποιος μπορεί να αιτηθεί ανάκληση

Το πιστοποιητικό ανακαλείται είτε από τον ίδιο τον συνδρομητή είτε από άλλη οντότητα η οποία μπορεί να αποδείξει την έκθεση του ιδιωτικού κλειδιού ή την χρήση του πιστοποιητικού εκτός των όσων δηλώνονται στη πολιτική/διαδικασίες πιστοποίησης. Επίσης, η Γραμματεία του Πανεπιστημίου Στερεάς Ελλάδος αιτείται ανάκληση για τα άτομα που χάνουν την ιδιότητα υπό την οποία πιστοποιήθηκαν.

10.4.9.3. Διαδικασία αιτήματος ανάκλησης

Το πιστοποιητικό ανακαλείται είτε από τον ίδιο τον συνδρομητή είτε από άλλη οντότητα η οποία μπορεί να αποδείξει την έκθεση του ιδιωτικού κλειδιού ή την χρήση του πιστοποιητικού εκτός των όσων δηλώνονται στη ΠΠ/ΔΠΠ.

10.4.9.3.1. Ανάκληση του πιστοποιητικού από το συνδρομητή

Απαιτείται η πιστοποίηση της ταυτότητας του συνδρομητή σύμφωνα με τη παράγραφο 10.3.4.

10.4.9.3.2. Ανάκληση του πιστοποιητικού από άλλη οντότητα

Ισχύει ότι αναφέρεται στη παράγραφο 10.4.9.2.

10.4.9.4. Χρονική περίοδος στην οποία ο συνδρομητής μπορεί να καταθέσει αίτημα ανάκλησης

Ο συνδρομητής μπορεί να καταθέσει αίτημα ανάκλησης οποιαδήποτε στιγμή μέσα στη διάρκεια ισχύος του αρχικού πιστοποιητικού εφόσον η ΑΠ που τα εξέδωσε συνεχίζει να βρίσκεται σε λειτουργία.

10.4.9.5. Χρόνος απόκρισης της Υπηρεσίας Πιστοποίησης για ανακλήσεις πιστοποιητικών

Η ΑΕ υποχρεούται να επεξεργάζονται τα αιτήματα ανάκλησης εντός μίας (1) εργάσιμης ημέρας εκτός περιπτώσεων ανωτέρας βίας.

10.4.9.6. Έλεγχος κατάστασης των πιστοποιητικών από τα Βασιζόμενα Μέρη(Relying Parties) μετά την ανάκληση.

Τα βασιζόμενα μέρη στην υπηρεσία θα πρέπει προτού βασιστούν σε κάποιο πιστοποιητικό να ακολουθούν τις διαδικασίες της παραγράφου 10.1.3.4.

10.4.9.7. Συχνότητα έκδοσης ΛΑΠ

Η ΛΑΠ θα εκδίδεται τουλάχιστον κάθε εξήντα (60) ημέρες. Η ΛΑΠ θα ισχύει για χρονικό διάστημα ίσο με τη μέγιστη περίοδο έκδοσής της. Σε περίπτωση έκθεσης του ιδιωτικού κλειδιού συνδρομητή θα εκδίδεται άμεσα ενημερωμένη ΛΑΠ.

10.4.9.8. Ενημέρωση αποθήκης και ΛΑΠ

Μετά από την ανάκληση κάποιου πιστοποιητικού εκδίδεται η ΛΑΠ και ενημερώνεται η αποθήκη. Στην αποθήκη το πιστοποιητικό χαρακτηρίζεται ως ανακλημένο.

10.4.9.9. Διαθεσιμότητα υπηρεσίας ελέγχου κατάστασης πιστοποιητικών σε πραγματικό χρόνο (OCSP)

Στην ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας συνιστάται να λειτουργεί υπηρεσία ελέγχου κατάστασης πιστοποιητικών σε πραγματικό χρόνο (On-line Certificate Status Protocol – OCSP). Η διεύθυνση της υπηρεσίας θα πρέπει να είναι ενσωματωμένη στα πιστοποιητικά που εκδίδονται.

10.4.9.10. Απαιτήσεις μερών που βασίζονται στην υπηρεσία (Relying Parties) για να ελέγχουν την κατάσταση των πιστοποιητικών πάνω στα οποία θα βασίζονται μέσω OCSP.

Τα μέρη που βασίζονται στην υπηρεσία θα πρέπει προτού βασιστούν σε κάποιο πιστοποιητικό να ακολουθούν τις διαδικασίες της παραγράφου 10.1.3.4. Επίσης, θα πρέπει κάθε φορά πριν εμπιστευθούν οποιοδήποτε πιστοποιητικό της ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας να ελέγχουν την υπηρεσία OCSP της ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας και να ρωτούν για την κατάσταση του πιστοποιητικού. Η διεύθυνση της υπηρεσίας OCSP βρίσκεται ενσωματωμένη σε κάθε πιστοποιητικό που έχει εκδοθεί.

10.4.9.11. Άλλες μορφές ανακοίνωσης ανάκλησης πιστοποιητικών

Δεν ορίζεται.

10.4.9.12. Ειδικές απαιτήσεις περίπτωση έκθεσης του ιδιωτικού κλειδιού

Ισχύει ότι ορίζεται στη παράγραφο 10.4.9.

10.4.9.13. Περιπτώσεις αναστολής πιστοποιητικών

Δεν επιτρέπεται αναστολή των πιστοποιητικών.

10.4.9.14. Ποιος μπορεί να αιτηθεί αναστολή πιστοποιητικών

Δεν επιτρέπεται αναστολή των πιστοποιητικών.

10.4.9.15. Διαδικασία αιτήματος αναστολής πιστοποιητικού

Δεν επιτρέπεται αναστολή των πιστοποιητικών.

10.4.9.16. Χρονική περίοδος αναστολής πιστοποιητικού

Δεν επιτρέπεται αναστολή των πιστοποιητικών.

10.4.10. Υπηρεσίες ελέγχου κατάστασης πιστοποιητικών

10.4.10.1. Χαρακτηριστικά λειτουργίας

Τα μέρη που βασίζονται στην υπηρεσία, προκειμένου να αποφανθούν για την εγκυρότητα ή μη κάποιων πιστοποιητικών, μπορούν να χρησιμοποιήσουν μια από τις παρακάτω προσφερόμενες υπηρεσίες ελέγχου κατάστασης ή συνδυασμό τους.

10.4.10.1.1. Διαδικασίες ελέγχου κατάστασης πιστοποιητικών πραγματικού χρόνου OCSP

Ισχύουν όσα περιγράφονται στην παράγραφο 10.4.9.10

10.4.10.1.2. On-line Αποθήκη πιστοποιητικών

Η on-line αποθήκη πιστοποιητικών, προσφέρει ένα περιβάλλον αναζήτησης πιστοποιητικών μέσω ιστοσελίδων, στο οποίο γίνονται ερωτήσεις που μπορεί να περιλαμβάνουν το σειριακό αριθμό ή το διακεκριμένο όνομα των πιστοποιητικών. Στα αποτελέσματα των αναζητήσεων, εμφανίζονται τα στοιχεία των πιστοποιητικών και μια περιγραφή που αναφέρει αν το πιστοποιητικό βρίσκεται σε ισχύ ή αν έχει ανακληθεί.

10.4.10.1.3. Χρήση των Λιστών Ανάκλησης Πιστοποιητικών (ΛΑΠ)

Ισχύουν όσα περιγράφονται στην παράγραφο 10.4.9.6.

10.4.10.2. Διαθεσιμότητα υπηρεσίας ελέγχου κατάστασης πιστοποιητικών

Θα καταβάλλεται προσπάθεια για από τις αρμόδιες αρχές προκειμένου η διαθεσιμότητα των υπηρεσιών ελέγχου κατάστασης πιστοποιητικών να είναι υψηλή.

10.4.11. Λήξη συνδρομής

Μετά τη λήξη της χρονικής ισχύος των πιστοποιητικών της ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας, ο χρήστης επιτρέπεται να κάνει αίτηση έκδοσης νέου πιστοποιητικού όπως περιγράφεται στη παράγραφο 11.4.3.

10.4.12. Συνοδεία ιδιωτικού κλειδιού (key escrow) και επαναφορά Κλειδιού

10.4.12.1. Διαδικασίες και πρακτικές συνοδείας ιδιωτικού κλειδιού και επαναφοράς

Δεν ορίζεται.

10.4.12.2. Ενθυλάκωση κλειδιού συνόδου (session key) και διαδικασίες και πρακτικές επαναφοράς

Δεν ορίζεται.

10.5. Διοικητικοί, Τεχνικοί και Λειτουργικοί Έλεγχοι

10.5.1. Φυσική ασφάλεια και έλεγχος πρόσβασης

10.5.1.1. Τοποθεσία εγκαταστάσεων

Η Αρχή Πιστοποίησης του Πανεπιστημίου Στερεάς Ελλάδας βρίσκεται εγκατεστημένη στο Κέντρο Λειτουργίας Δικτύου, στον 1ο όροφο του κτιρίου Πανεπιστημίου Στερεάς Ελλάδος, Λαμία.

10.5.1.2. Φυσική πρόσβαση

Η φυσική πρόσβαση στον εξοπλισμό των ΑΠ και της Αρχής Εγγραφής επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό. Απαγορεύεται η σύνδεση της ΑΠ σε δίκτυο ή οποιοδήποτε τηλεπικοινωνιακό μέσο.

10.5.1.3. Κλιματισμός και ρύθμιση τροφοδοσίας με ρεύμα

Όλος ο εξοπλισμός της Υποδομής Δημοσίου Κλειδιού που είναι υπό τη διαχείριση του ΚΛΔ, βρίσκεται σε κλιματιζόμενους χώρους.

10.5.1.4. Έκθεση σε νερό

Ο εξοπλισμός της Υ.Δ.Κ που είναι υπό τη διαχείριση του ΚΛΔ βρίσκεται σε χώρο που δεν κινδυνεύει σε μεγάλο βαθμό από πλημμύρες.

10.5.1.5. Πρόληψη και προστασία από φωτιά

Οι εγκαταστάσεις του Κ.Λ.Δ υπόκεινται στην ελληνική νομοθεσία σχετικά με την πρόληψη και την προστασία πυρκαγιάς στα δημόσια κτίρια.

10.5.1.6. Αποθηκευτικά μέσα

Τα ιδιωτικά κλειδιά των Αρχών Πιστοποίησης είναι υπό τη διαχείριση του Κ.Λ.Δ, βρίσκονται σε εύκαμπτους μαγνητικούς δίσκους (floppy disks) σε κρυπτογραφημένη μορφή, με κωδικό (passphrase) που γνωρίζει μόνο εξουσιοδοτημένο προσωπικό του.

Αντίγραφα ασφαλείας όλης της Υποδομής Δημοσίου Κλειδιού του, βρίσκονται σε μαγνητικές ταινίες ή memory flash disks που κατέχουν εξουσιοδοτημένα στελέχη του Πανεπιστημίου Στερεάς Ελλάδας.

Και τα δύο παραπάνω αποθηκευτικά μέσα προτείνεται να βρίσκονται σε φυσικές τοποθεσίες διαφορετικές από το Κ.Λ.Δ, προστατευμένα από έκθεση σε νερό και φωτιά.

10.5.1.7. Διάθεση απορριμμάτων

Απορρίμματα που μπορεί να περιέχουν οποιαδήποτε εμπιστευτική πληροφορία όπως εύκαμπτοι μαγνητικοί δίσκοι, σκληροί δίσκοι κ.α. καταστρέφονται πριν απορριφθούν.

10.5.1.8. Τήρηση αντιγράφων ασφαλείας εκτός εγκαταστάσεων

Ισχύει ότι αναφέρεται στη παράγραφο 10.5.1.6.

10.5.2. Έλεγχος διαδικασιών

10.5.2.1. Έμπιστοι ρόλοι

Το προσωπικό που ορίζεται είναι εξουσιοδοτημένο για να λειτουργεί τον εξυπηρετητή της ΑΠ, να διαχειρίζεται όλες τις εργασίες της Αρχής Εγγραφής και να εκτελεί τις εργασίες τήρησης αντιγράφων ασφαλείας και θεωρείται έμπιστο.

10.5.2.2. Αριθμός ατόμων που απαιτούνται ανά εργασία

Δεν ορίζεται.

10.5.2.3. Εξακρίβωση ταυτότητας για κάθε ρόλο

Δεν ορίζεται.

10.5.2.4. Ρόλοι που απαιτούν διαχωρισμό καθηκόντων

Το προσωπικό που εξουσιοδοτείται για να εκτελέσει τα καθήκοντα της Αρχής Εγγραφής είναι διαφορετικό από το προσωπικό που εκτελεί τα καθήκοντα της Αρχής Πιστοποίησης.

10.5.3. Έλεγχος προσωπικού

10.5.3.1. Προσόντα, εμπειρία και ειδικές εξουσιοδοτήσεις που πρέπει το προσωπικό να διαθέτει

Το προσωπικό που διαχειρίζεται και λειτουργεί την ΑΠ και ΑΕ πρέπει να διαθέτει γνώσεις σε θέματα ψηφιακών πιστοποιητικών και σε θέματα υποδομής δημοσίου κλειδιού. Ειδικές εξουσιοδοτήσεις δεν ορίζονται.

10.5.3.2. Διαδικασίες ελέγχου παρελθόντος για το προσωπικό της ΑΠ και της ΑΕ.

Ακολουθείται η κείμενη νομοθεσία και το πλαίσιο που ισχύει για το προσωπικό του Πανεπιστημίου Στερεάς Ελλάδας.

10.5.3.3. Απαιτήσεις και διαδικασίες εκπαίδευσης

Το προσωπικό που λειτουργεί την Αρχή Πιστοποίησης και Αρχή Εγγραφής έχει πρόσβαση στις κρυπτογραφικές διαδικασίες, εκπαιδεύεται και καταρτίζεται στα θέματα της Υποδομής Δημοσίου Κλειδιού και πρέπει να γνωρίζει την Δήλωση Διαδικασιών Πιστοποίησης και την Πολιτική Πιστοποίησης της ΥΔΚ.

10.5.3.4. Διαδικασίες και συχνότητα επανεκπαιδεύσεων

Δεν ορίζεται.

10.5.3.5. Εναλλαγή και σειρά αλλαγής ρόλων

Δεν ορίζεται.

10.5.3.6. Επιβαλλόμενες κυρώσεις για μη εξουσιοδοτημένες ενέργειες

Ακολουθούνται όλες οι νόμιμες διαδικασίες που προβλέπονται για συγκεκριμένα αδικήματα και ο κανονισμός λειτουργίας του Κέντρου Διαχείρισης Δικτύου του Πανεπιστημίου Στερεάς Ελλάδας

10.5.3.7. Έλεγχος σε ανεξάρτητο προσωπικό που εργάζονται εκτός του Πανεπιστημίου Στερεάς Ελλάδας και εμπλέκονται με την Υ.Δ.Κ Πανεπιστημίου Στερεάς Ελλάδας.

Δεν ορίζεται

10.5.3.8. Γνωστικά αρχεία που παρέχεται στο προσωπικό κατά τη διάρκεια εκπαίδευσης

Δεν ορίζεται.

10.5.4. Διαδικασίες ελέγχου συμβάντων

10.5.4.1. Τύποι συμβάντων που καταγράφονται

Καταγράφονται εξής τύποι συναλλαγών :

- Οι αιτήσεις που έγιναν για έκδοση πιστοποιητικού
- Τα εκδοθέντα πιστοποιητικά
- Οι εκδιδόμενες ΛΑΠ
- Τα μηνύματα που ανταλλάχθηκαν με την Αρχή Εγγραφής.

Επίσης καταγράφονται στους εξυπηρετητές της ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας και άλλες διεργασίες των λειτουργικών συστημάτων και των εφαρμογών όπως π.χ. οι http συνδέσεις με τους εξυπηρετητές ιστοσελίδων κ.α.

10.5.4.2. Συχνότητα αρχειοθέτησης των επεξεργασμένων συμβάντων

Το σύστημα αρχειοθετεί όλες τις συναλλαγές καθημερινά.

10.5.4.3. Διάστημα τήρησης του αρχείου συμβάντων

Τα αρχεία συναλλαγών τηρούνται για χρονικό διάστημα δύο (2) ετών, ώστε να είναι διαθέσιμα για ενδεχόμενο νόμιμο έλεγχο.

10.5.4.4. Προστασία του αρχείου συμβάντων

Ισχύει ότι αναφέρεται στην παράγραφο 10.5.1.

10.5.4.5. Διατηρείται αντίγραφο ασφαλείας του αρχείου εγγραφών

10.5.4.6. Σύστημα συγκέντρωσης αρχείων συμβάντων (εσωτερικό ή εξωτερικό σε σχέση με την οντότητα)

Δεν ορίζεται.

10.5.4.7. Ενημέρωση του υποκειμένου που προκάλεσε καταγραφή εγγραφής, για την ύπαρξη της καταγραφής

Δεν ορίζεται.

10.5.4.8. Αξιολογήσεις ευπάθειας του συστήματος καταγραφής εγγραφών.

Δεν ορίζεται.

10.5.5. Αρχειοθέτηση εγγραφών

10.5.5.1. Τύποι εγγραφών που αρχειοθετούνται

Όλα τα αρχεία συμβάντων που αναφέρονται στην παράγραφο 10.5.4 Όπως και τα σχετικά έγγραφα που προσκομίστηκαν κατά τα αιτήματα έκδοσης/ανάκλησης ψηφιακών πιστοποιητικών.

10.5.5.2. Διάστημα διατήρησης του αρχείου εγγραφών

Τα αρχεία εγγραφών τηρούνται για χρονικό διάστημα δύο (2) ετών, ώστε να είναι διαθέσιμα για κάθε έλεγχο.

10.5.5.3. Προστασία του αρχείου εγγραφών

Ισχύει ότι αναφέρεται στην παράγραφο 10.5.1.

10.5.5.4. Διαδικασίες αντιγράφων ασφαλείας αρχείων εγγραφών

Τηρείται αντίγραφο ασφαλείας των αρχείων εγγραφών.

10.5.5.5. Απαίτηση χρονοσήμανσης-χρονοσφραγίδας αρχείων εγγραφών

Δεν ορίζεται.

10.5.5.6. Σύστημα συγκέντρωσης αρχείων εγγραφών (εσωτερικό ή εξωτερικό σε σχέση με την οντότητα)

Δεν ορίζεται.

10.5.5.7. Διαδικασίες για ανάκτηση και επαλήθευση των στοιχείων των αρχείων εγγραφών

Δεν ορίζεται.

10.5.6. Ριζική αλλαγή κλειδιού

Σε περίπτωση αλλαγής κλειδιού της Αρχής Πιστοποίησης, τα κλειδιά των πιστοποιητικών των συνδρομητών πρέπει να ακυρωθούν και να ξαναδημιουργηθούν με τις διαδικασίες της παραγράφου 10.4.1.

10.5.7. Ανάκαμψη από παραβίαση ασφάλειας και καταστροφή

10.5.7.1. Διαδικασίες και χειρισμός περιστατικών παραβίασης

Όλα τα αρχεία ελέγχονται ανά χρονικά διαστήματα για ανίχνευση παραβίασης ασφάλειας συστημάτων ή υποσυστημάτων. Στην περίπτωση εύρεσης κάποιας δυσλειτουργίας ή υπάρχει υποψία παραβίασης, διακόπτεται η παροχή της υπηρεσίας και ελέγχεται όλα το σύστημα της ΥΔΚ.

10.5.7.2. Διαδικασίες αντιμετώπισης σε περίπτωση παραβίασης-καταστροφής υπολογιστικών συστημάτων, λογισμικού, δεδομένων.

Στην περίπτωση εύρεσης κάποιας δυσλειτουργίας ή υπάρχει υποψία παραβίασης, διακόπτεται η παροχή της υπηρεσίας και ελέγχεται όλο το σύστημα της ΥΔΚ.

10.5.7.3. Διαδικασίες αντιμετώπισης σε περίπτωση απώλειας ιδιωτικών κλειδιών

Σε περίπτωση απώλειας ή αποκάλυψης των ιδιωτικών κλειδιών των πιστοποιητικών των συνδρομητών, γίνεται ανάκληση τους από την ΑΠ και έκδοση νέων χωρίς την διακοπή της υπηρεσίας Σε περίπτωση απώλειας του ιδιωτικού κλειδιού της Αρχής Πιστοποίησης, η ΑΠ υποχρεούται να διακόψει την υπηρεσία, να ειδοποιήσει όλους τους συνδρομητές, να προχωρήσει στην ανάκληση όλων των πιστοποιητικών, να εκδώσει μια τελευταία ΛΑΠ. Στη συνέχεια η ΥΔΚ επαναδημιουργεί νέα ΑΠ.

10.5.7.4. Δυνατότητες αδιάλειπτης λειτουργίας της υπηρεσίας σε περίπτωση φυσικών ή άλλων καταστροφών.

Η ΑΠ του Πανεπιστημίου Στερεάς Ελλάδας έχει προβλέψει δυνατότητες αδιάλειπτης λειτουργίας με αποθήκευση αντιγράφων όλων των συστημάτων σε ασφαλή τοποθεσία εκτός των χώρων του Πανεπιστημίου Στερεάς Ελλάδας.

10.5.8. Λήξη Αρχής Πιστοποίησης ή Αρχής Εγγραφής

Κατά τη λήξη της, η ΑΠ θα πρέπει να ενημερώσει τους συνδρομητές να ανακαλέσει όλα τα πιστοποιητικά που έχει εκδώσει και το δικό της, να ανακοινώνει τη σχετική ΛΑΠ και να

δημοσιεύσει το τερματισμό της λειτουργίας της. Τα αρχεία καταγραφής των ΑΕ και ΑΠ τηρούνται για χρονικό διάστημα δύο (2) ετών, ώστε να είναι διαθέσιμα για κάθε έλεγχο.

10.6. Έλεγχοι ασφάλειας τεχνικού επιπέδου

10.6.1. Δημιουργία ζεύγους κλειδιών και εγκατάσταση

10.6.1.1. Δημιουργία ζεύγους κλειδιών

Τα κλειδιά των συνδρομητών δημιουργούνται με κατάλληλο λογισμικό παραμένουν κάτω από τον πλήρη έλεγχό των συνδρομητών για τη όλη διάρκεια της ισχύος τους.

10.6.1.2. Παράδοση ιδιωτικού κλειδιού σε οντότητα

Δεν επιτρέπεται η παράδοση του ιδιωτικού κλειδιού σε τρίτη οντότητα. Η παράδοση του ιδιωτικού κλειδιού γίνεται αποκλειστικά στον συνδρομητή κάτοχο του πιστοποιητικού με φυσική παρουσία του κάνοντας χρήση κάποιου επιλεγμένου μέσου αποθήκευσης.

10.6.1.3. Παράδοση δημόσιου κλειδιού συνδρομητή στην Αρχή Πιστοποίησης

Ο εγγραφόμενος υποβάλλει στην Αρχή Εγγραφής το δημόσιο κλειδί του μέσω δομημένης αίτησης για έκδοση πιστοποιητικού. Η αίτηση είναι υπογεγραμμένη με το σχετικό ιδιωτικό κλειδί. Η ΑΕ επαληθεύει την ορθότητα της υπογραφής και συμπεραίνει ότι ο αιτών κατέχει πράγματι το σχετικό με την αίτηση ιδιωτικό κλειδί.

10.6.1.4. Παράδοση του δημόσιου κλειδιού της Αρχής Πιστοποίησης σε οντότητες που εμπιστεύονται τα πιστοποιητικά

Το κάθε ψηφιακό πιστοποιητικό που εκδίδει η ΑΠ περιέχει το δημόσιο κλειδί για τις ενδιαφερόμενες οντότητες. Η ΑΠ δημοσιοποιεί στην αποθήκη της παραγράφου 10.2.1 το Πιστοποιητικό της.

10.6.1.5. Μεγέθη κλειδιών

Το ελάχιστο επιτρεπτό μέγεθος κλειδιού συνδρομητή ή εξυπηρετητή είναι 1024bits, 2048bits για το πιστοποιητικό της Αρχής Πιστοποίησης

10.6.1.6. Παράμετροι δημιουργίας κλειδιών

Δεν ορίζεται.

10.6.1.7. Σκοποί χρήσης των κλειδιών (ως προς το αντίστοιχο πεδίο του X.509)

Οι σκοποί χρήσης ενός κλειδιού αναφέρονται στο σχετικό βασικό πεδίο και στη σχετική επέκταση του πιστοποιητικού τύπου X.509v3. Οι αναφερόμενοι σκοποί Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης χρήσης του πιστοποιητικού δεν είναι περιοριστικοί αλλά προτεινόμενοι. Ο έλεγχος συμμόρφωσης με τους επιτρεπόμενους σκοπούς χρήσης γίνεται κατά την κρίση των βασιζόμενων μερών.

10.6.2. Προστασία ιδιωτικών κλειδιών

10.6.2.1. Προδιαγραφές για κρυπτογραφικές μονάδες

Δεν ορίζεται.

10.6.2.2. Έλεγχος ιδιωτικού κλειδιού από πολλαπλά πρόσωπα (N-M)

Δεν ορίζεται.

10.6.2.3. Συνοδεία ιδιωτικού κλειδιού (key escrow)

Δεν ορίζεται.

10.6.2.4. Αντίγραφα ασφαλείας ιδιωτικών κλειδιών

Το ιδιωτικό κλειδί της Αρχής Πιστοποίησης πρέπει να φυλάσσεται σε αντίγραφα ασφαλείας. Το κλειδί στο αντίγραφο πρέπει να είναι πάντα κρυπτογραφημένο και να ακολουθούνται οι διαδικασίες που περιγράφονται στην Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης Υποδομής Δημοσίου Κλειδιού του Πανεπιστημίου Στερεάς Ελλάδας Η πρόσβαση στο αντίγραφο ασφαλείας επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

10.6.2.5. Αρχειοθέτηση αντιγράφων ασφαλείας ιδιωτικών κλειδιών

Το αντίγραφο ασφαλείας του ιδιωτικού κλειδιού της Αρχής Πιστοποίησης πρέπει να αρχειοθετείται και να φυλάσσεται με ασφαλείς μεθόδους και σε ασφαλή χώρο. Τα ιδιωτικά κλειδιά στο αντίγραφο είναι πάντα κρυπτογραφημένα.Η πρόσβαση στο αρχειοθετημένο αντίγραφο ασφαλείας επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

10.6.2.6. Μεταφορά ιδιωτικού κλειδιού από και προς ένα κρυπτογραφικό σύστημα.

Οι κάτοχοι των ιδιωτικών κλειδιών, μπορούν να μεταφέρουν κατά την κρίση τους το ιδιωτικό κλειδί τους από ειδικό κρυπτογραφικό σύστημα μορφής λογισμικού(software certificate store) σε οποιοδήποτε κρυπτογραφικό σύστημα μορφής υλικού (hardware) πχ crypto-tokens smartcards. Η αντίστροφη διαδικασία δεν επιτρέπεται

10.6.2.7. Μορφή αποθήκευσης του ιδιωτικού κλειδιού σε κρυπτογραφικό σύστημα.

Δεν ορίζεται

10.6.2.8. Μέθοδοι ενεργοποίησης ιδιωτικών κλειδιών.

Για την ενεργοποίηση ενός ιδιωτικού κλειδιού απαιτείται η εισαγωγή κάποιου κωδικού (pass-phrase) προκειμένου να αποκρυπτογραφηθεί και να χρησιμοποιηθεί το ιδιωτικό κλειδί σε συνδυασμό με το πιστοποιητικό. Ειδικά για κρυπτογραφικά συστήματα υλικού (πχ crypto-tokens) απαιτείται η εισαγωγή κάποιου PIN.

10.6.2.9. Μέθοδοι απενεργοποίησης ιδιωτικών κλειδιών.

Δεν ορίζεται.

10.6.2.10. Μέθοδοι καταστροφής ιδιωτικών κλειδιών.

Δεν ορίζεται.

10.6.2.11. Βαθμολόγηση-αξιολόγηση κρυπτογραφικών συστημάτων

Δεν ορίζεται.

10.6.3. Άλλες πτυχές διαχείρισης ζεύγους κλειδιών

10.6.3.1. Αρχειοθέτηση των δημόσιων κλειδιών

Τα δημόσια κλειδιά ενσωματώνονται στα ψηφιακά πιστοποιητικά κατά την έκδοσή τους και αρχειοθετούνται σύμφωνα με τις διαδικασίες που περιγράφονται στις παραγράφους 10.5.4 και 10.5.5.

10.6.3.2. Περίοδοι χρήσης των πιστοποιητικών και των ζευγών κλειδιών

Η διάρκεια χρήσης των ζευγών κλειδιών προσδιορίζεται από την περίοδο ισχύος του ψηφιακού πιστοποιητικού που αντιστοιχούν. Η μέγιστη διάρκεια χρήσης των κλειδιών είναι οκτώ (8) έτη για ΑΠ και σε δύο (2) έτη για πιστοποιητικά τελικών χρηστών και εξυπηρετητών. Η διάρκεια χρήσης αποφασίζεται σε συνάρτηση με το μέγεθος των κλειδιών και τις τεχνολογικές εξελίξεις στο χώρο της κρυπτογραφίας, έτσι ώστε να επιτυγχάνεται το βέλτιστο επίπεδο ασφάλειας.

10.6.4. Δεδομένα ενεργοποίησης

10.6.4.1. Δημιουργία δεδομένων ενεργοποίησης και εγκατάσταση

Τα δεδομένα ενεργοποίησης, δηλαδή οι μυστικοί κωδικοί και τα PIN, πρέπει να επιλέγονται έτσι ώστε να είναι δύσκολο να ανακαλυφθούν. Το ελάχιστο μέγεθος του μυστικού κωδικού και του PIN είναι οκτώ (8) ψηφία.

10.6.4.2. Προστασία δεδομένων ενεργοποίησης

Δεν ορίζεται.

10.6.4.3. Άλλα θέματα σχετικά με τα δεδομένα ενεργοποίησης

Δεν ορίζεται.

10.6.5. Έλεγχοι ασφαλείας υπολογιστών

10.6.5.1. Συγκεκριμένες τεχνικές απαιτήσεις ασφάλειας

Η ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας διατηρεί τα Λειτουργικά Συστήματα των υπολογιστών της ασφαλή εφαρμόζοντας τα διεθνή προτύπων οδηγιών ασφάλειας. Τα προγράμματα που συνοδεύουν το Λειτουργικό Σύστημα είναι τα απολύτως απαραίτητα για την ορθή λειτουργία των ΑΕ/ΑΠ.

10.6.5.2. Βαθμολόγηση ασφάλειας υπολογιστών

Δεν ορίζεται.

10.6.6. Έλεγχοι ασφαλείας κύκλου ζωής

10.6.6.1. Έλεγχοι ανάπτυξης συστημάτων

Δεν ορίζεται.

10.6.6.2. Έλεγχοι διαχείρισης ασφάλειας

Δεν ορίζεται.

10.6.6.3. Βαθμολόγηση ασφάλειας κύκλου ζωής

Δεν ορίζεται.

10.6.7. Έλεγχοι ασφαλείας δικτύου

Δεν επιτρέπεται η σύνδεση των ΑΠ σε άλλα δίκτυα (πχ Internet) ή άλλο τηλεπικοινωνιακό μέσο (πχ στο τηλεφωνικό δίκτυο μέσω modem).

10.6.8. Χρονοσφραγίδες-Χρονοσήμανση

Δεν ορίζεται.

10.7. Σχεδιάγραμμα (profile) πιστοποιητικού και ΛΑΠ

10.7.1. Σχεδιάγραμμα πιστοποιητικού

Χρησιμοποιείται σχεδιάγραμμα πιστοποιητικού σύμφωνα με το RFC 3280 **[42]** "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

10.7.1.1. Έκδοση

Ο αριθμός έκδοσης του πιστοποιητικού είναι 3, που αντιστοιχεί στα πιστοποιητικά X.509v3.

10.7.1.2. Επεκτάσεις πιστοποιητικού

Σε κάθε πιστοποιητικό που εκδίδεται συνιστάται να περιλαμβάνεται η επέκταση Basic Constraints χαρακτηρισμένη ως κρίσιμη και οι επεκτάσεις KeyUsage, SubjectKeyIdentifier, AuthorityKeyIdentifier και CertificatePolicies χαρακτηρισμένες ως μη κρίσιμες.

10.7.1.3. Αναγνωριστικά αντικειμένων αλγορίθμων

Δεν ορίζεται

.

10.7.1.4. Μορφή ονομάτων

Η μορφή των ονομάτων είναι σύμφωνη με τους κανόνες της παραγράφου 10.3.1.

10.7.1.5. Περιορισμοί ονομάτων

Δεν ορίζεται.

10.7.1.6. Αναγνωριστικό πολιτικής πιστοποίησης

Η Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού του Πανεπιστημίου Στερεάς Ελλάδος έχει το αναγνωριστικό της πολιτικής πιστοποίησης, OID (Object Identifier) :*χ.χ.χ.χ.χ.χ.χ.χ.χχχχ*.α.α.1.0

10.7.1.7. Χρήση της επέκτασης περιορισμού πολιτικής

Δεν ορίζεται.

10.7.1.8. Σύνταξη και σημασιολογία του χαρακτηριστικού πολιτικής

Το χαρακτηριστικό πολιτικής είναι URI το οποίο δείχνει στην δημοσιευμένη ΠΠ/ΔΔΠ της ΥΔΚ.

10.7.1.9. Επεξεργασία σημασιολογίας για την κρίσιμη επέκταση πολιτικής πιστοποίησης

Δεν ορίζεται.

10.7.2. Περίγραμμα ΛΑΠ

10.7.2.1. Έκδοση

Ο αριθμός έκδοσης της είναι 1 ή/και 2, που αντιστοιχεί σε ΛΑΠ X.509v2, ακολουθώντας το RFC-3280.

10.7.2.1.1. ΛΑΠ και επεκτάσεις των εγγραφών της ΛΑΠ

Δεν ορίζεται.

10.7.3. Περίγραμμα OCSP

10.7.3.1. Έκδοση

Δεν ορίζεται.

10.7.3.2. OCSP και επεκτάσεις των εγγραφών

Δεν ορίζεται.

10.8. Έλεγχοι Συμμόρφωσης και Αξιολόγησης

10.8.1. Συχνότητα και συνθήκες αξιολόγησης

Δεν προτείνεται άλλος εξωτερικός έλεγχος συμμόρφωσης παρά μόνο έλεγχος συμμόρφωσης της ΥΔΚ προς την ΠΠ/ΔΔΠ από την ίδια την ΥΔΚ.

10.8.2. Ταυτότητα και προσόντα του ελεγκτή

Έλεγχος συμμόρφωσης μπορεί να διεξαχθεί από τους ενδιαφερόμενους για συνεργασία με την Υπηρεσία, μετά από άδεια του φορέα που λειτουργεί την Υπηρεσία και εφόσον ο ενδιαφερόμενος καλύψει όλα τα έξοδα του ελέγχου.

10.8.3. Σχέση ελεγκτή με την ελεγχόμενη οντότητα

Δεν ορίζεται.

10.8.4. Θέματα που καλύπτει η αξιολόγηση

Δεν ορίζεται.

10.8.5. Ενέργειες που λαμβάνονται σε περίπτωση ανεπάρκειας

Δεν ορίζεται.

10.8.6. Επικοινωνία των αποτελεσμάτων

Δεν ορίζεται

10.9. Διοικητικά και Νομικά θέματα

10.9.1. Κόστη εγγραφής

Δεν επιβάλλεται χρέωση για τις παρεχόμενες υπηρεσίες. Απαγορεύεται ρητά κάθε είδους μεταπώληση ή άλλου τύπου εκμετάλλευση των παρεχόμενων υπηρεσιών.

10.9.1.1. Κόστος έκδοσης και ανανέωσης πιστοποιητικών

Δεν ορίζεται

10.9.1.2. Κόστος πρόσβασης σε πιστοποιητικά

Δεν ορίζεται

10.9.1.3. Κόστος ανάκλησης ή ερώτηση κατάστασης πιστοποιητικών

Δεν ορίζεται

10.9.1.4. Κόστος άλλων υπηρεσιών όπως πρόσβαση στα κείμενα πολιτικής και διαδικασιών πιστοποίησης

Δεν ορίζεται

10.9.1.5. Διαδικασίες επιστροφής χρημάτων

Δεν ορίζεται

10.9.2. Οικονομική ευθύνη

Η Υποδομή Δημοσίου Κλειδιού Πανεπιστημίου Στερεάς Ελλάδας δεν φέρει καμία οικονομική ευθύνη.

10.9.3. Εμπιστευτικότητα πληροφοριών εμπορικού χαρακτήρα

Η ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας δεν διαχειρίζεται πληροφορίες εμπορικού χαρακτήρα.

10.9.4. Εμπιστευτικότητα πληροφοριών προσωπικού χαρακτήρα

10.9.4.1. Σχέδιο εμπιστευτικότητας

Δεν ορίζεται.

10.9.4.1.1. Πληροφορίες που χαρακτηρίζονται εμπιστευτικές

Οι πληροφορίες που θεωρούνται ως εμπιστευτικές, είναι τα ιδιωτικά κλειδιά της Αρχής Πιστοποίησης και ο μηχανισμός ασφαλούς αποθήκευσης και χρήσης τους. Η Αρχή Εγγραφής είναι πιθανό να επεξεργάζεται προσωπικά δεδομένα κατά τη διαδικασία πιστοποίησης της ταυτότητας των αιτούντος.

10.9.4.1.2. Πληροφορίες που δεν θεωρούνται εμπιστευτικές

Οι πληροφορίες που περιέχονται στα ψηφιακά πιστοποιητικά που εκδίδονται δεν θεωρούνται εμπιστευτικές.

10.9.4.2. Δήλωση προστασίας δεδομένων προσωπικού χαρακτήρα

Η ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας συμμορφώνεται με τη σχετική νομοθεσία περί προστασίας Προσωπικών Δεδομένων.

10.9.4.3. Διάθεση πληροφοριών σε αρχές επιβολής του νόμου

Οι μη εμπιστευτικές πληροφορίες που τηρεί η Υπηρεσία είναι διαθέσιμες στις δικαστικές αρχές, μετά από έγγραφη αίτησή τους.

10.9.4.4. Πληροφορίες που μπορούν να διατεθούν για τη αναζήτηση Οντοτήτων

Δεν ορίζεται.

10.9.4.5. Όροι για τη διάθεση πληροφοριών μετά από αίτημα του ιδιοκτήτη τους

Οι πληροφορίες που διατηρεί η ΑΠ είναι διαθέσιμες στον ιδιοκτήτη τους, μετά από αίτησή του.

10.9.4.6. Άλλες περιπτώσεις στις οποίες διατίθενται εμπιστευτικές πληροφορίες

Δεν ορίζεται.

10.9.5. Δικαιώματα πνευματικής ιδιοκτησίας

Η ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας δεν έχει δικαιώματα πνευματικής ιδιοκτησίας στα εκδιδόμενα πιστοποιητικά. Οποιοσδήποτε, μπορεί να αντιγράφει μέρη της παρούσας ΠΠ/ΔΔΠ με την προϋπόθεση αναφοράς του αρχικού κειμένου.

10.9.6. Αντιπροσωπεύσεις και εξουσιοδοτήσεις

Δεν ορίζεται

10.9.7. Αποκηρύξεις και Εγγυήσεις

Δεν ορίζεται

10.9.8. Περιορισμοί ευθυνών

Η χρήση της ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας και των υπηρεσιών Πιστοποίησης προϋποθέτει την ανεπιφύλακτη παραδοχή εκ μέρους του χρήστη ότι η ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας δεν ευθύνεται για ζημία ή βλάβη, δεν αναλαμβάνει, ούτε μπορούν να τις αποδοθούν οικονομικές, αστικές ή άλλου είδους ευθύνες, παρά μόνο σε περιπτώσεις που αποδεικνύεται ή αμέλεια της.

10.9.9. Αποζημιώσεις

Η Υποδομή Δημοσίου Κλειδιού Πανεπιστημίου Στερεάς Ελλάδας και οι υπηρεσίες Πιστοποίησης δεν αναλαμβάνουν ούτε μπορούν να τις αποδοθούν οικονομικές, αστικές ή άλλου είδους ευθύνες, παρά μόνο σε περιπτώσεις που αποδεικνύεται δόλος ή αμέλεια τους.

Επίσης χρησιμοποιείται αποκλειστικά για Ακαδημαϊκούς και Ερευνητικούς σκοπούς και απαγορεύεται ρητά η εμπορική εκμετάλλευσή της. Συνεπώς δεν αναλαμβάνει να καταβάλλει κανενός είδους αποζημιώσεις.

10.9.10. Χρονική περίοδος ισχύος της παρούσας ΠΠ/ΔΠΠ και τερματισμός της

Η παρούσα ΠΠ/ΔΠΠ ισχύει όσο θα λειτουργεί η ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας

10.9.11. Ατομικές ειδοποιήσεις και επικοινωνία μεταξύ των αποτελούμενων μερών

Δεν ορίζεται

10.9.12. Τροποποιήσεις

10.9.12.1. Διαδικασία τροποποιήσεων

Συντακτικές αλλαγές μπορούν να γίνουν στην ΠΠ/ΔΔΠ χωρίς ειδοποίηση και χωρίς ανάγκη αλλαγής του αναγνωριστικού του κειμένου (OID).

10.9.12.2. Μηχανισμοί ενημέρωσης και περίοδος ενημέρωσης

Οι συνδρομητές θα ενημερώνονται πρίν από σημαντικές αλλαγές στην ΠΠ/ΔΠΠ.

10.9.12.3. Συνθήκες κάτω από τις οποίες το OID θα πρέπει να αλλάζει

Σε περίπτωση σημαντικών αλλαγών που ενδέχεται να επηρεάσουν την δυνατότητα αποδοχής της ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας, θα πρέπει να μεταβληθεί το όνομα και το αναγνωριστικό (OID) της πολιτικής πιστοποίησης το οποίο αναφέρεται στην παράγραφο 10.1.2.

10.9.13. Διαδικασίες επίλυσης διαφορών

Σε περίπτωση που προκύψουν διαφορές από την ερμηνεία της ΠΠ/ΔΔΠ και τη λειτουργία της ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας θα επιλύονται σύμφωνα με την Ακαδημαϊκή δεοντολογία και τον Ελληνικό Νόμο.

10.9.14. Ισχύουσα νομοθεσία

Η λειτουργία της ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας συμμορφώνεται στα Ακαδημαϊκά ήθη και στην Ελληνική Νομοθεσία. Ιδιαίτερα όσο αφορά το Προεδρικό Διάταγμα 150/2001 «Προσαρμογή στην οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές», τα πιστοποιητικά που εκδίδονται μέσω της ΥΔΚ του Πανεπιστημίου Στερεάς Ελλάδας δεν θεωρούνται «Αναγνωρισμένα Πιστοποιητικά».

Βασικές προϋποθέσεις για την αναγνώριση του πιστοποιητικού και της παραγόμενης ψηφιακής υπογραφής ως ισότιμης με τη χειρόγραφη, είναι α) η χρήση ασφαλούς διάταξηδημιουργίας υπογραφής στην πλευρά του χρήστη (π.χ. έξυπνη κάρτα όπου δημιουργείται,

αποθηκεύεται και χρησιμοποιείται αποκλειστικά το ιδιωτικό κλειδί του πελάτη) και β) η έγκριση του εκάστοτε αρμόδιου οργάνου.

10.9.15. Συμμόρφωση με την κείμενη νομοθεσία

Η ΥΔΚ Πανεπιστημίου Στερεάς Ελλάδας συμμορφώνεται πλήρως με την κείμενη Ελληνική νομοθεσία.

10.9.16. Διάφορες Παροχές/Δεσμεύσεις

10.9.16.1. Υποχρεώσεις των Αρχών Πιστοποίησης

Μια Αρχή Πιστοποίησης είναι υπεύθυνη για την έκδοση και τη διαχείριση των πιστοποιητικών.

Συγκεκριμένα, η Αρχή Πιστοποίησης υποχρεούται:

- Να παρέχει και να συντηρεί την ένα αξιόπιστο και διαθέσιμο σύστημα που απαιτείται για την ορθή λειτουργία της ΥΔΚ και να λειτουργεί σύμφωνα με τους κανόνες της Πολιτική και τις Διαδικασίες Πιστοποίησης που περιγράφονται στο παρόν έγγραφο.
- Να ικανοποιεί τις απαιτήσεις ασφαλείας σύμφωνα με τα όσα αναφέρονται στις σχετικές παραγράφους του παρόντος εγγράφου.
- Να διατηρεί ένα χώρο αποθήκευσης ευρείας πρόσβασης για την αποθήκευση των πιστοποιητικών και των Λιστών Ανάκληση Πιστοποιητικών.
- Να ανακαλεί πιστοποιητικά όταν το κρίνει σκόπιμο ή μετά από αίτημα του συνδρομητή.
- Να διατηρεί τις Λίστες Ανάκλησης Πιστοποιητικών σύμφωνα με τους όρους που περιγράφησαν στο παρόν έγγραφο.
- Να διαχειρίζεται εμπιστευτικά όλες τις προσωπικές πληροφορίες που παρέχονται από τους εγγραφόμενους στην Αρχή Εγγραφής.
- Να ενημερώνει τους συνδρομητές και τις βασιζόμενες οντότητες, για έκθεση, απώλεια, ή τροποποίηση.
- Να διατηρεί αντίγραφα ασφαλείας των κλειδιών των συνδρομητών και των δικών της, των πιστοποιητικών που εκδίδει και να τα αποθηκεύει σε ασφαλή τοποθεσία.
- Να τηρεί αρχείο με όλες τις διαδικασίες που πραγματοποιεί.
-

10.9.16.2. Υποχρεώσεις υφιστάμενων ΑΠ

Δεν ορίζεται.

10.9.16.3. Υποχρεώσεις της Αρχής Εγγραφής

Κάθε Αρχή Εγγραφής διαχειρίζεται τις αιτήσεις και ανάκλησης των χρηστών.

- Η ΑΕ είναι αρμόδια για τη παραλαβή των αιτήσεων πιστοποίησης, την ανθεντικοποίηση της ταυτότητας του αιτών, την επικύρωση της αντιστοιχίας του δημόσιου κλειδιού που αναγράφεται στο πιστοποιητικό με τον χρήστη που αιτείται και για τη μεταβίβαση της αίτηση με ασφαλή τρόπο στην ΑΠ.
- Η ΑΕ είναι υπεύθυνη να ελέγχει τις αιτήσεις για λάθη σύνταξης και για το εάν ο τύπος του πιστοποιητικού που αιτείται δεν έρχεται προβλέπεται από τους όρους του κειμένου Δήλωση Διαδικασιών Πιστοποίησης.
- Η παραλαβή των αιτήσεων μπορεί να πραγματοποιηθεί είτε με τη φυσική παρουσία του ενδιαφερόμενου, είτε μέσω ειδικής φόρμας σε ιστοσελίδα, όπου υπάρχει μηχανισμός αυθεντικοποίησης του χρήστη. Η αίτηση θα πρέπει να περιλαμβάνει τα προσωπικά στοιχεία ταυτότητας του εγγραφόμενου και στη περίπτωση που έχει ο ίδιος δημιουργήσει το ζεύγος κλειδιών του να υπογράφει ψηφιακά την αίτηση.

10.9.16.4. Υποχρεώσεις των συνδρομητών

Συνδρομητές είναι οι κάτοχοι ψηφιακών πιστοποιητικών.

- Οι συνδρομητές στην Υπηρεσία είναι υποχρεωμένοι να μελετήσουν, να αποδεχθούν τους όρους και τους κανόνες της ΠΠ/ΔΔΠ.
- Οι συνδρομητές είναι υποχρεωμένοι να κάνουν χρήσεις του πιστοποιητικού χωρίς να έρχονται σε αντίθεση με την ΠΠ/ΔΔΠ και το ισχύον νομοθετικό πλαίσιο.
- Οι συνδρομητές πρέπει να λάβουν τις απαραίτητες προφυλάξεις για την προστασία του ιδιωτικού κλειδιού τους από τυχαία καταστροφή απώλεια ή κλοπή και να μην το αποκαλύπτουν σε τρίτους.
- Οι συνδρομητές με την παραλαβή του πιστοποιητικού, αποδέχονται ότι οι πληροφορίες που συμπεριλαμβάνονται σε αυτό είναι ορθές και ισχύουν.
- Οι συνδρομητές είναι υποχρεωμένοι να αιτούνται από την ΑΕ την ανάκληση του πιστοποιητικού τους όταν τα στοιχεία που περιέχει έχουν αλλάξει και

όταν έχει εκτεθεί ή χαθεί ή υπάρχει υποψία έκθεσης του ιδιωτικού τους κλειδιού.

10.9.16.5. Υποχρεώσεις των οντοτήτων που εμπιστεύονται τα πιστοποιητικά

- Οι οντότητες που εμπιστεύονται τα πιστοποιητικά είναι υποχρεωμένες να μελετούν και να αποδεχθούν τους όρους και τους κανόνες που θέτει η ΠΠ/ΔΔΠ
- Οι οντότητες που εμπιστεύονται τα πιστοποιητικά είναι υποχρεωμένες να κάνουν χρήσεις του πιστοποιητικού χωρίς να έρχονται σε αντίθεση με την ΠΠ/ΔΔΠ και το ισχύον εθνικό νομικό πλαίσιο.
- Οι οντότητες που εμπιστεύονται τα πιστοποιητικά πρέπει να ελέγχουν την εγκυρότητα της υπογραφής του ψηφιακού πιστοποιητικού, να ελέγχουν την περίοδο ισχύος του πιστοποιητικού και να ενημερώνονται περιοδικά από τη ΛΑΠ που εκδίδει η ΑΠ για τυχόν ανάκληση του πιστοποιητικού.

10.9.16.6. Υποχρεώσεις αποθήκης

Η Αρχή Πιστοποίησης είναι υποχρεωμένη να διατηρεί μια ευρέως προσβάσιμη αποθήκη δεδομένων στην οποία να καταχωρεί το ψηφιακό πιστοποιητικό της, την ΠΠ/ΔΔΠ, τα εκδοθέντα πιστοποιητικά και τη ΛΑΠ.

11 *Κεφάλαιο*

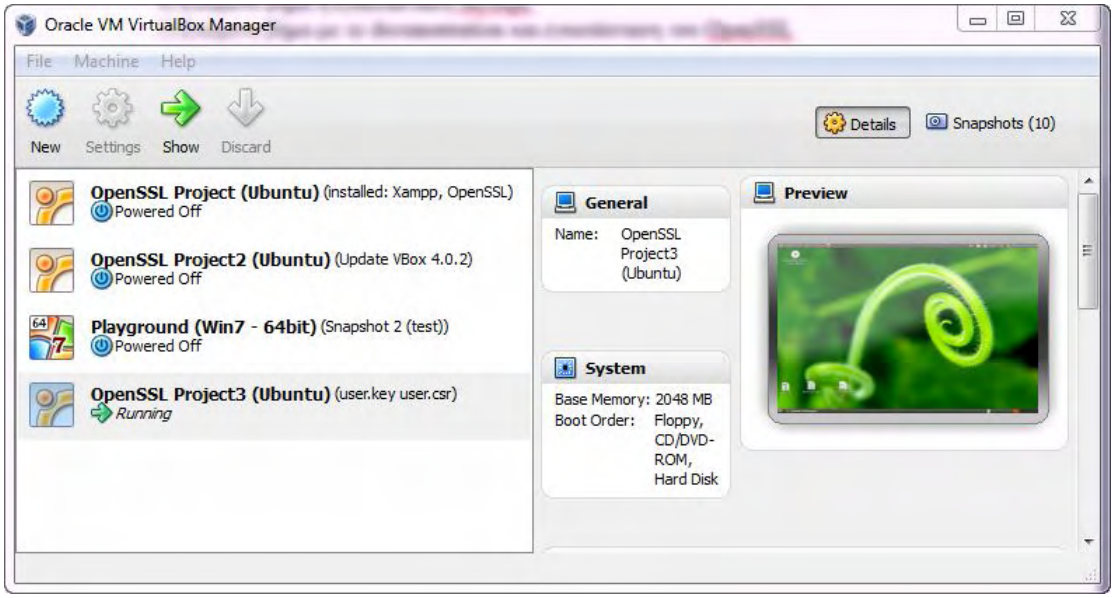
ΒΗΜΑΤΑ ΥΛΟΠΟΙΗΣΗΣ

Σε αυτό το Κεφάλαιο παρατίθενται τα λογισμικά και οι μέθοδοι που χρησιμοποιούνται για την υλοποίηση μιας Πρότυπης Υπηρεσίας Πιστοποίησης.

Open-source λογισμικού OpenCA

- Εγκατάσταση λογισμικού για Virtualisation.

Εγκαταστάθηκε το πακέτο της Oracle, VirtualBox 3.2.12 (http://www.virtualbox.org/)



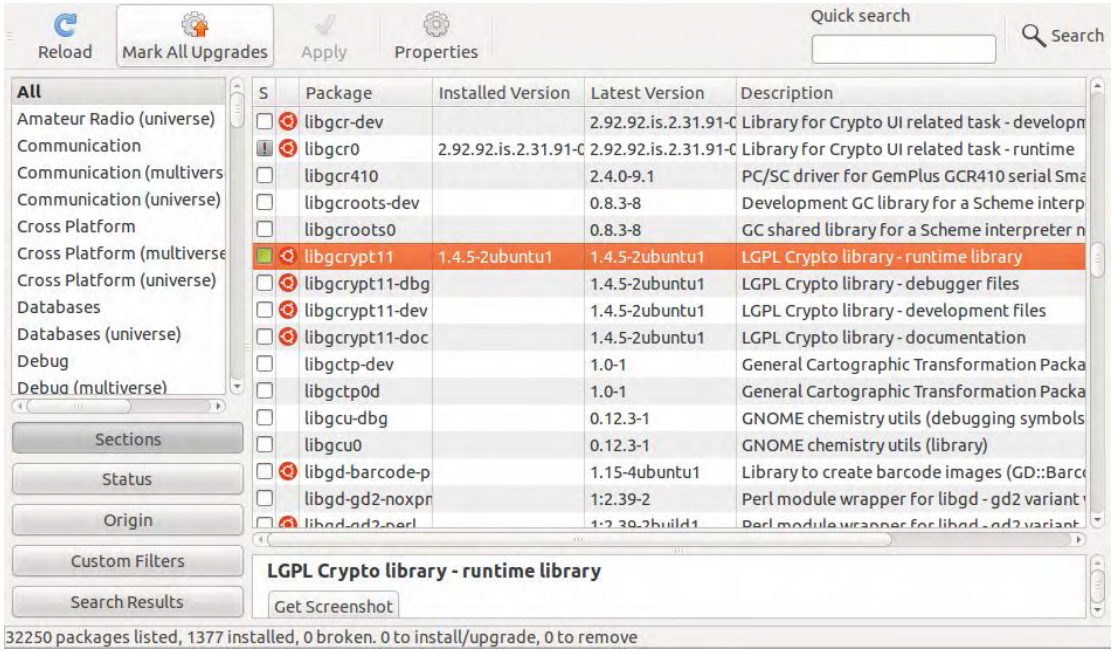
Εικόνα 20

Δημιουργήθηκε ένα partition με χωρητικότητα 8 GB χώρο και μνήμη 2048 MB.

- Εγκατάσταση σε virtual machine λογισμικού Ubuntu έκδοση: 10.0.0 (32-bit) (http://www.ubuntu.com/desktop/get-ubuntu/download)

Η εγκατάσταση έγινε από αρχείο ISO.

- Εγκατάσταση στο Ubuntu βιβλιοθηκών που προαπαιτούνται για τη λειτουργία του OpenCA.



Εικόνα 21

- Από την επίσημη σελίδα του OpenCA (http://www.openca.org/projects/openca/) Κατεβάζουμε το πακέτο:

1. openca-tools-1.3.0.tar.gz
   Size: 373 Kb - Downloads: 2799
   [Sha1: 7a36db2d9fd642627f785a116043bd3801ef971e]

   και το πακέτο:

   - openca-base-1.1.1.tar.gz
     Size: 7.71 MB - Downloads: 907
     [Sha1: 7a4dbbc61eb632a8d0bcc26072ec84ab8c89d476]

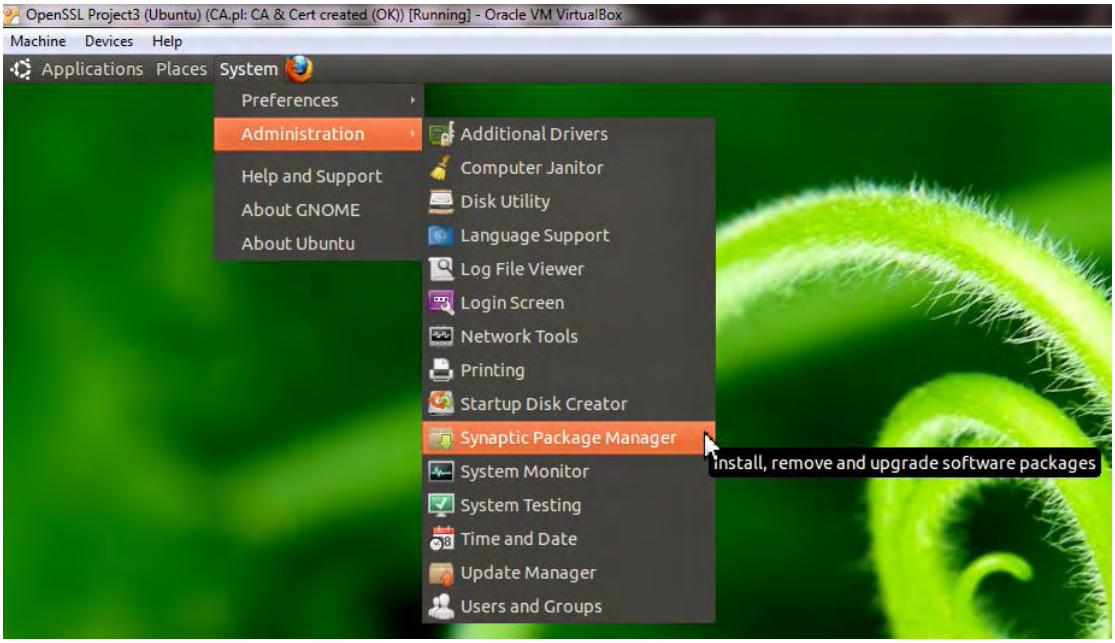
     (σε μορφή source files: http://www.openca.org/projects/openca/tools-sources.shtml)

     Από την επίσημη σελίδα του OpenSSL (http://www.openssl.org/) το πακέτο:

   - OpenSSL 0.9.8r (including important bug and security fixes)
     (ημερομηνία έκδοσης: 08-Feb-2011)

ΠΡΟΣΟΧΗ: πρέπει να είναι η έκδοση 0.9.8r και όχι νεότερη έκδοση!

- Χρησιμοποιούμε την εφαρμογή `System > Administration > Synaptic Package Manager` του Ubuntu, για να εγκαταστήσουμε τα αναγκαία πακέτα λογισμικού:



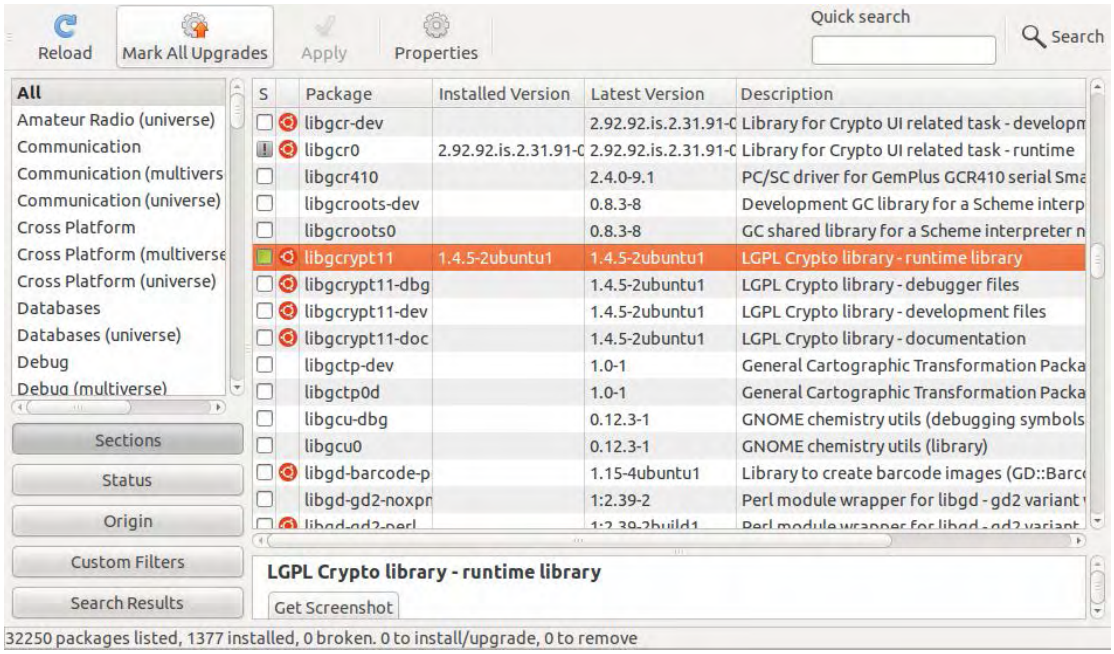
Εικόνα 22

Τα αναγκαία πακέτα – βιβλιοθήκες είναι τα εξής:

Όνομα	Λειτουργία
`apache-ssl`	`Secure HTTP functionality`
`libconvert-ber-perl`	`For perl - Convert::BER`
`libmime-perl`	`For perl - MIME::* [cpan MIME-Base64]`
`liburi-perl`	`For perl - URI [cpan URI]`
`libdigest-md5-perl`	`For perl - Digest::* [cpan Digest-MD5]`
`libnet-ldap-perl`	`For perl - [cpan perl-ldap]`
`libxml-sax-expat-perl`	`For perl - XML::Parser`
`libexpat1-dev`	`Expat development libraries libs & incs`
`libclass-dbi-loader - perl`	`For perl – dbi`
`libssl-dev`	`SSL libraries`
`libnet:ssleay`	`SSL support`
`libapachedbi-perl`	`Apache server`
`libcgi-ssesion perl`	`Cgi functionality`
`libmysqlclient-dev`	`MySQL client`
`mysqlserver`	`MySQL server`

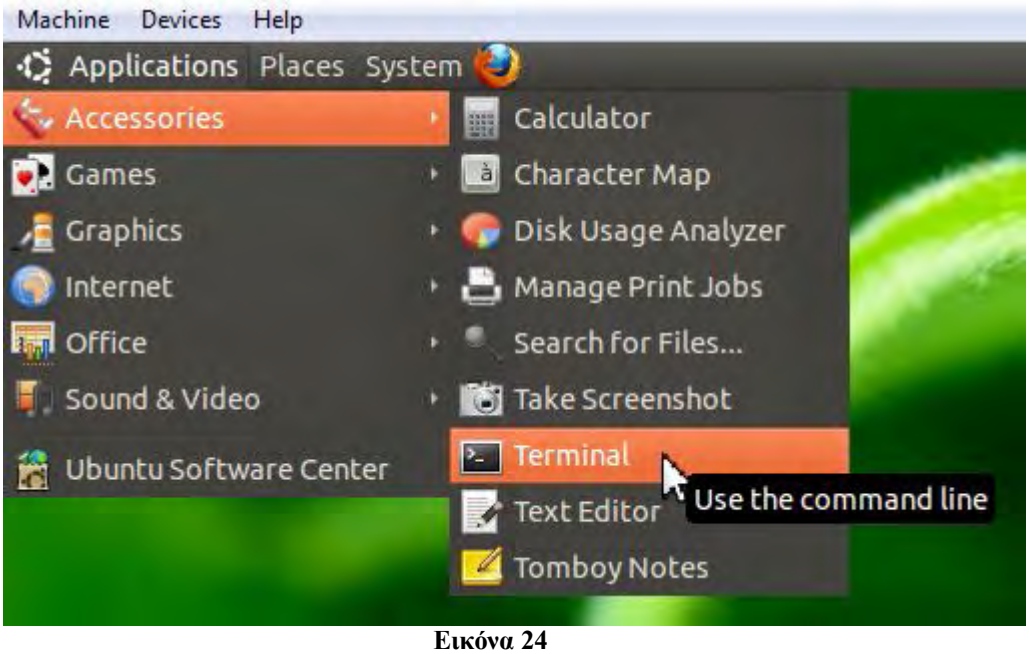
Πίνακας 2:Αναγκαίες βιβλιοθήκες

Η μορφή της εφαρμογής είναι η εξής:



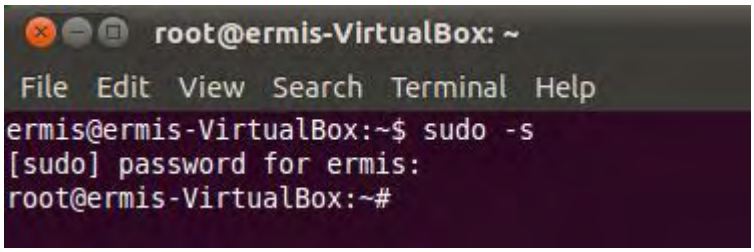
Εικόνα 23

- Ανοίγουμε την γραμμή εντολών `Accessories > Terminal` για να μπορέσουμε να προχωρήσουμε με τις εντολές της εγκατάστασης:



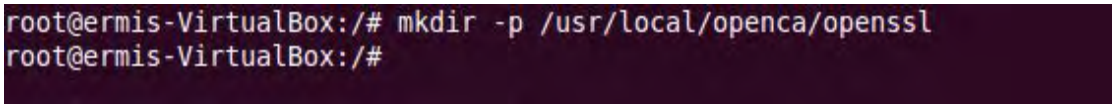
Εικόνα 24

Εκτελούμε την εντολή `sudo -s`, εισάγοντας τον κωδικό που έχουμε βάλει κατά την εγκατάσταση του Ubuntu, ώστε να συνδεθούμε στο λειτουργικό σύστημα ως διαχειριστές (super user):



Εικόνα 25

- Κατασκευάζουμε ένα νέο φάκελο:
  - `mkdir -p /usr/local/openca/openssl`



- Κάνουμε την εγκατάσταση του OpenSSL:
  - `/config --prefix=/usr/local/openca/openssl --openssldir=/usr/local/openca/openssl/openssl`
  - `make`
  - `make install`
- Δημιουργούμε τους κατάλληλους φακέλους και κάνουμε την εγκατάσταση με τις παρακάτω εντολές:
  - `tar xzvf openca-tools`
  - `cd openca-tools`
  - `./configure`
  - `make`
  - `make install`
  - `tar xzvf openca-base`
  - `cd openca-base`
  - `./configure`
  - `make`
  - `make install -offline`
  - `make install -online`

Τα σχετικά στοιχεία του συστήματος είναι τα εξής:

```
OpenCA Server:
* OpenCA prefix ..................: /usr/local
* Build prefix ...................:
* OpenCA User ....................: root
* OpenCA Group ...................: root
* OpenCA Tools prefix ............:
```

```
Web Server:
* httpd User ....................: www-data
* httpd Group ...................: www-data
* httpd prefix ..................: /var/www
* htdocs prefix .................: /var/www/html/pki
* cgi prefix ....................: /var/www/cgi-bin/pki
* htdocs URL prefix .............: /pki
* cgi URL prefix ................: /cgi-bin/pki

Other:
* OpenSSL Prefix ................: /usr
* OpenSSL Libs ..................: -Wl,-rpath,/usr/lib -L/usr/lib
-L/usr -lcrypto -lssl

Done.
```

- Κατασκευάζουμε ένα χρήστη (user) και μια ομάδα χρηστών (group) στο Ubuntu με τις εντολές:
  - `addgroup openca`
  - `adduser -g openca openca`

και δηλώνουμε ως κωδικό (password) τη λέξη "**openca**"

- Χρειάζονται δύο επιπλέον αρχεία με κώδικα για τη σωστή λειτουργία της εγκατάστασης (http://www.opensubscriber.com/message/openca-users@lists.sourceforge.net/14930417.html)

Α) Το αρχείο `initServer`, το οποίο πρέπει να τοποθετηθεί στο φάκελο `/usr/local/lib/openca/functions`

Β) το αρχείο `User.pm`, το οποίο πρέπει να τοποθετηθεί στο φάκελο `/usr/local/lib/openca/perl_modules/perl5/OpenCA/`

Η διαδικασία είναι η εξής:
Για το αρχείο (Α) μεταφερόμαστε στο φάκελο:
- `cd /usr/local/lib/openca/functions`

δημιουργούμε ένα κενό αρχείο με το όνομα InitServer με την εντολή:
- `:> InitServer`

Ανοίγουμε το αρχείο με την εντολή:
- `nano InitServer`
- Κάνουμε *Αντιγραφή-Επικόλληση* τον κώδικα του αρχείου
- Πατάμε Alt+X και 'Yes' για έξοδο

Για το αρχείο (Β) μεταφερόμαστε στο φάκελο:
- `cd /usr/local/lib/openca/perl_modules/perl5/OpenCA/`

δημιουργούμε ένα κενό αρχείο με το όνομα User.pm με την εντολή:
- `:> User.pm`

Ανοίγουμε το αρχείο με την εντολή:
- `nano User.pm`

- Κάνουμε *Αντιγραφή-Επικόλληση* τον κώδικα του αρχείου
- Πατάμε Alt+X και 'Yes' για έξοδο

Ο κώδικας των αρχείων επισυνάπτεται στο τέλος.

- Δημιουργούμε τη Βάση Δεδομένω MySQL ως εξής:

(http://wiki.openca.org/wiki/index.php/Installing_OpenCA)

Συνδεόμαστε με το DBMS:

- mysql -u root -p -h localhost

Δημιουργούμε τη Βάση Δεδομένων:

- mysql > CREATE DATABASE openca;

Επιλέγουμε την εν λόγω βάση:

- mysql > use openca;

Ορίζουμε τα δικαιώματα του νέου χρήστη της βάσης openca:

- mysql > GRANT ALL PRIVILEGES ON *.* TO 'openca'@'localhost' IDENTIFIED BY 'password';

Ο χρήστης και η Βάση Δεδομένων δημιουργούνται τώρα.
Για να εξέγξουμε ότι η εγκατάσταση έγινε σωστά, κάνουμε «έξοδο» από την MySQL και την επανεκινούμε χρησιμοποιόντας το νέο χρήστη:

- mysql -u openca -p -h localhost openca

Εάν γίνει η σύνδεση επιτυχώς, τότε η Βάση Δεδομένων έχει ορισθεί σωστά.

- Κάνουμε το configuration του openca-tool:

- `./configure --prefix=/usr/local/openca --with-openca-user=openca --with-openca-group=openca`

- `make`
- `make install`

- Κάνουμε το configuration του openca-base:

- `./configure --prefix=/usr/local/openca --exec-prefix=/usr/local/openca --with-openssl-prefix=/usr/local/openca/openssl --with-web-host=localhost --with-httpd-host=localhost --with-httpd-user=www-data --with-httpd-group=www-data --`

```
with-httpd-fs-prefix=/var/www/openca --with-htdocs-fs-
prefix=/var/www/openca --with-ca-
organization="University of Greece" --with-ca-
locality=Athens --with-ca-country=GR --with-db-
name=openca -with-db-user=openca --with-db-
passwd=openca --with-db-type=mysql --with-db-port=3306
--with-auth-user=openca --with-auth-password=openca
```

- `make`
- `make install`

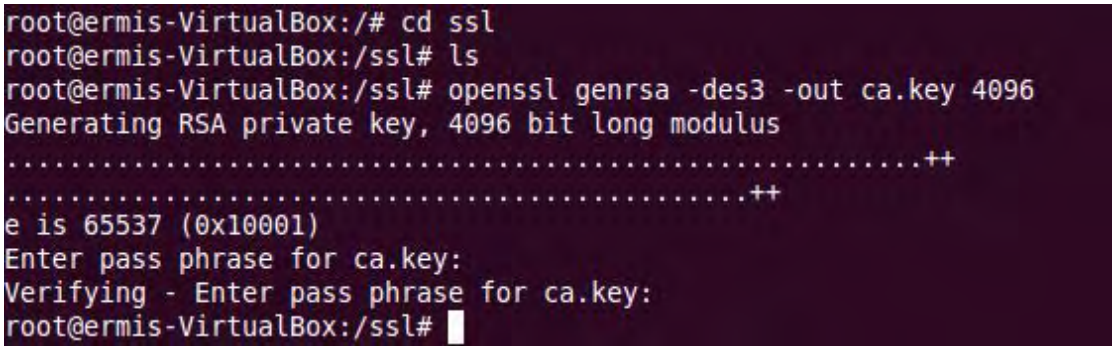
- Κατασκευάζουμε ένα φάκελο με το όνομα ‘ssl’ μέσα στο φάκελο `etc/apache2`

```
1. mkdir ssl
```

Μέσα στο φάκελο ssl, δημιουργούμε ένα νέο Certificate Authority (CA), με τα παρακάτω βήματα.

α) Κατασκευάζουμε ένα κλειδί για το CA (CA key) και ένα πιστοποιητικό για το CA (CA certificate):

- `openssl genrsa -des3 -out ca.key 4096`



Εικόνα 26

- `openssl req -new -x509 -days 365 -key ca.key -out ca.crt`

```
root@ermis-VirtualBox:/ssl# openssl req -new -x509 -days 365 -key ca.key -out ca.crt
Enter pass phrase for ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GR
State or Province Name (full name) [Some-State]:Lamia
Locality Name (eg, city) []:Lamia
Organization Name (eg, company) [Internet Widgits Pty Ltd]:University
Organizational Unit Name (eg, section) []:University
Common Name (eg, YOUR name) []:administrator
Email Address []:admin@university.gr
root@ermis-VirtualBox:/ssl#
```

Εικόνα 27

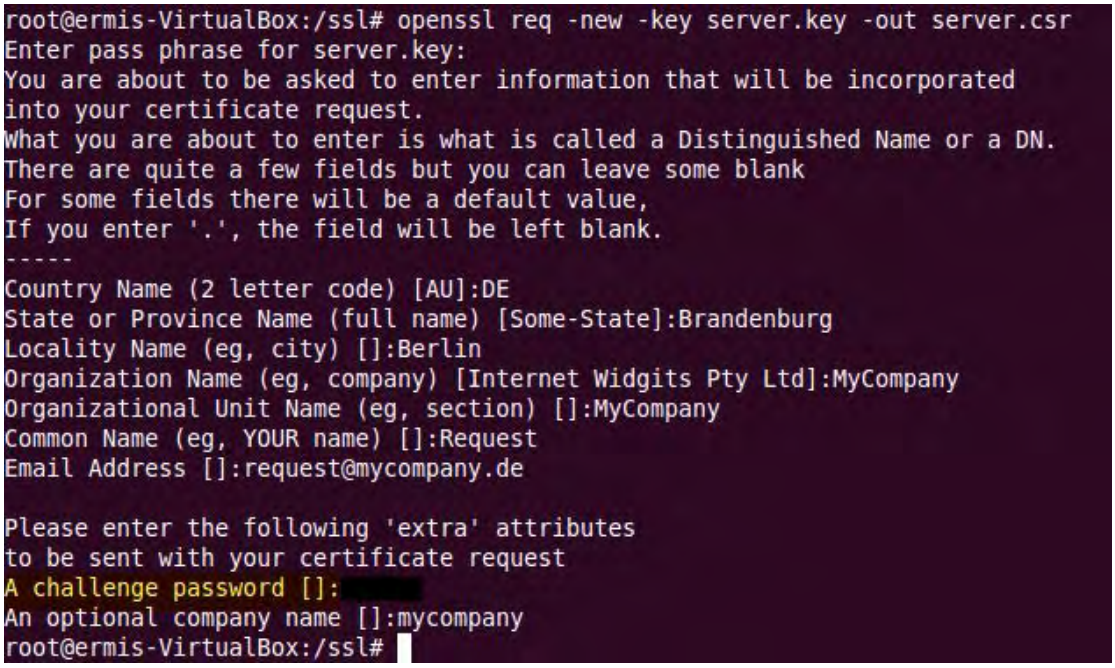
β) Κατασκευάζουμε ένα κλειδί για το διακομιστή (server key) και κάνουμε το αίτημα για υπογραφή (request for signing - csr):

- `openssl genrsa -des3 -out server.key 4096`

```
root@ermis-VirtualBox:/ssl# openssl genrsa -des3 -out server.key 4096
Generating RSA private key, 4096 bit long modulus
...........++
.....................................................................++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
root@ermis-VirtualBox:/ssl#
```

Εικόνα 28

- `openssl req -new -key server.key -out server.csr`



Εικόνα 29

γ) Από τα στοιχεία που εισάγουμε κατά το αίτημα (signing request - csr) δημιουργείται ένα πιστοποιητικό (signed server certificate - crt) που θα είναι ενεργό για 365 ημέρες.

Για να γίνει αυτό, πρέπει να δηλώσουμε ποιο CA θα χρησιμοποιηθεί, ποιο κλειδί να χρησιμοποιήσει (private CA key) και ποιο κλειδί διακομιστεί να υπογράψει (Server key). Ορίζουμε ένα σειριακό αριθμό (01) και εξάγουμε το υπογεγραμένο κλειδί στο αρχείο server.crt

- `openssl x509 -req -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt`

Εικόνα 30

Τα δύο αρχεία `server.crt` και `server.key` βρίσκονται στο φάκελο `ssl` και ο `Apache` θα πρέπει να τα εντοπίσει με κάποιο τρόπο. Για το λόγο αυτό:

- Ενεργοποιούμε το `ssl` για τον `Apache` με την παρακάτω εντολή:

- `a2enmod ssl`

- Μεταφερόμαστε στο φάκελο `/etc/apache2/sites-available` και κάνουμε `edit` το αρχείο `default-ssl`:

- `nano  default-ssl`

όπου και δηλώνουμε τις σωστές διαδρομές (paths) για το `server.key` και για το `server.crt` στις μεταβλητές:

```
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key
```

- Πρέπει επίσης να δηλώσουμε τη διαδρομή (path) του `cgi-bin` μέσα στο αρχείο `default-ssl:`

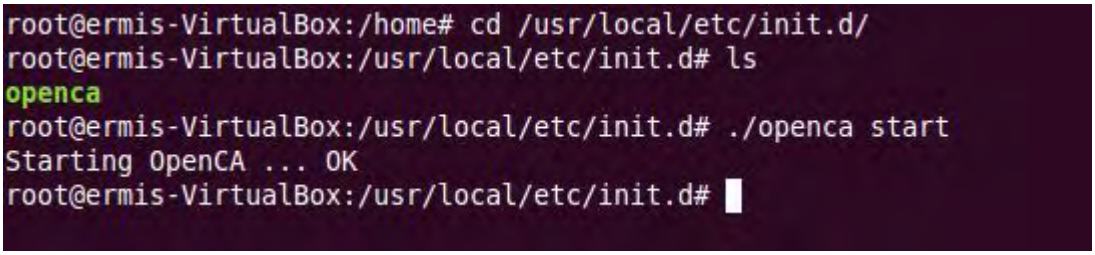
- `nano  default-ssl`

-
```
DocumentRoot /var/www/html
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        </Directory>
        <Directory /var/www/html>
                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
        </Directory>


ScriptAlias /cgi-bin/ /var/www/cgi-bin/
        <Directory "/var/www/cgi-bin">
                AllowOverride None
                Options +ExecCGI -MultiViews
+SymLinksIfOwnerMatch
                Order allow,deny
                Allow from all
        </Directory>
```

- Μπορούμε να εξέγξουμε ότι το OpenCA λειτουργεί εάν μεταφερθούμε στο φάκελο `/usr/local/etc/init.d/` και εκτελέσουμε την εντολή:

- `./openca start`



Εικόνα 31

12 *Κεφάλαιο*

ΑΠΟΤΕΛΕΣΜΑΤΑ-ΟΔΗΓΙΕΣ ΧΡΗΣΗΣ

Στο παρόν Κεφάλαιο δίνονται παραδείγματα δημιουργίας πιστοποιητικού για την Υπηρεσία Πιστοποίησης (CA) και δημιουργίας και υπογραφής πιστοποιητικού για χρήστη από τη Υπηρεσία. Τα παραδείγματα αυτά παρατίθενται για την πληρέστερη κατανόηση του τρόπου λειτουργίας της Πρότυπης Υπηρεσίας Πιστοποίησης.

1)Παράδειγμα δημιουργίας πιστοποιητικού και κλειδιών για το CA με τη χρήση του script CA.pl

(**Σημ:** τα σημαντικά σημεία κατά την εμφάνιση αποτελεσμάτων έχουν τονισθεί και έχουν τυπωθεί με πράσινο χρώμα)

- Επιλογή directory για την εγκατάσταση του CA (myCA).
  - `mkdir myCA`
  - `cd myCA`
- Αντιγραφή των αρχείων CA.pl και openssl.cnf στο directory myCA. Τα αρχεία αυτά συμπεριλαμβάνονται στην εγκατάσταση του πακέτου OpenSSL.
  - `cp /usr/lib/ssl/misc/CA.pl CA.pl`
  - `cp /usr/lib/ssl/openssl.cnf openssl.cnf`
- Δημιουργία του CA:
  - `./CA.pl -newca`

  Το νέο CA δημιουργείται στο directory myCA.

```
Making CA certificate...
Generating a 1024 bit RSA private key
......++++++
.........++++++
```

```
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase: ********
Verifying - Enter PEM pass phrase: ********
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:GR
State or Province Name (full name) [Some-State]:Macedonia
Locality Name (eg, city) []:Thessaloniki
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DemoCA
Organizational Unit Name (eg, section) []:DemoCA Unit
Common Name (eg, YOUR name) []:Admin of CA
Email Address []:admin@ca.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:********
An optional company name []:DemoCA Ltd
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
```

Serial Number: e7:95:62:aa:bb:20:e9:a1		
Validity	Not Before: Feb 16 23:56:46 2011 GMT Not After : Feb 15 23:56:46 2014 GMT	
Subject:	countryName	= GR
	stateOrProvinceName	= Macedonia
	organizationName	= DemoCA
	organizationalUnitName	= DemoCA Unit
	commonName	= Admin of CA
	emailAddress	= admin@ca.org
X509v3 extensions:		
X509v3SubjectKeyIdentifier: 97:AB:02:E5:2A:0D:41:C8:22:D8:EA:57:82:C1:3F:57:5D:7B:D1:78		
X509v3AuthorityKeyIdentifier: keyid:97:AB:02:E5:2A:0D:41:C8:22:D8:EA:57:82:C1:3F:57:5D:7B:D1:78		
DirName:/C=GR/ST=Macedonia/O=DemoCA/OU=DemoCA Unit/CN=Admin of CA/emailAddress=admin@ca.org		
serial:E7:95:62:AA:BB:20:E9:A1		
X509v3 Basic Constraints:		
CA:TRUE		
Certificate is to be certified until Feb 15 23:56:46 2014 GMT (1095 days)		

Πίνακας 3: Μορφή και δεδομένα CA πιστοποιητικού

```
Write out database with 1 new entries
Data Base Updated
```

Το self-signed πιστοποιητικό του CA είναι το **demoCA/cacert.pem** και το αντίστοιχο ζεύγος κλειδιών RSA (key pair) είναι το **demoCA/private/cakey.pem**

Μπορούμε να δούμε το κλειδί της CA που δημιουργήθηκε (**cakey**) με την εντολή 'cat' :

- «cat demoCA/private/cakey.pem»

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9E7BE80001E4B813

go8fpKY5MDA3EjRBVRh+0G9npIh8zf4/FSy0d60vLs8h3haXobauzq07hL4e9Scl
VK7jrD4n7mBLhqXFeKD42DAE2ENfZQs/xPs+UK9RwhC+BpSKoDsv2d9DCfetLVoc
oTOQKyfdyFtQujPbXkGyf7M1Txj330PexvwEL1Xymzw6ude8HUI1fDOwit9B3J3B
d5PcXrqWyE7kN9nt4Nwjt3kBg84M02WJDg3UpeH7j8m6EOwRqw+a9vS5rx1MBLZJ
i0yKBKx5Mdd8EPzGRJrz2ZCUEuXGX3/KJi7kMYof4Emx7qYYTaCh+cDo3Ss/0GP7
yHZyq4hSfrUVApPWcIGWAyUHkEdopO6F4KhZqiT4yc4NgNICwPG0Ln+1UOKp9zNn
XRQsjX6IGaS8oF3xKI2NR35V5uJI8CUd0GP0RDRKipjVn9e1u9SPW6NpzXg6iTRy
oqd0I8xFL9XQRLkjcDkK8hkSQ2tmm61QH0U6r/K4WX81onBRVhwOgZnSrETwkC71
BjFNmLTzueGi35YQ02V1nN+27TH53ZJbAYMGexlyB8XNA0AqRkNEfugls8ZxxX2n
fYLHQ5FHCUogCtHUGBxI/+ZkpufNQD73B/e9+/x4H6Zwb6XBbjkVEavnFLG7z3DG
ySQTqMOfs22SHvAlRePQW1ofERtMkWZbmYYlo7AG7/VoFRrezZPGETxaiPAPMRV1
zxmqZ3+ojhuT6sXK2395PiV1PEYYiSoScmYRY0CV08Bab3ymZUytkIVPG2fj7+eo
lFh1EutLub9E+IeuyMe89vmOQ44QlKeIC7YVyb6moZugSi1rSTIPLQ==
```

Πίνακας 4: Κλειδιά CA σε κρυπτογραφημένη μορφή

```
-----END RSA PRIVATE KEY-----
```

2)Παράδειγμα δημιουργίας πιστοποιητικού και κλειδιά για τον χρήστη με τη χρήση του script CA.pl

Αίτημα πιστοποιητικού χρήστη στη CA:

- Εκτελούμε το certificate request με την εντολή 'newreq' και ο χρήστης συμπληρώνει τα στοιχεία του:

  - «./CA.pl –newreq»

```
Generating a 1024 bit RSA private key
..................++++++
..............++++++
writing new private key to 'newkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
```

```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Brandenburg
Locality Name (eg, city) []:Berlin
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany
Organizational Unit Name (eg, section) []:Berlin Unit
Common Name (eg, YOUR name) []:Requester
Email Address []:mycompany@berlin.de

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:********
An optional company name []:********


Request is in newreq.pem, private key is in newkey.pem
```

Το certificate request και το private key είναι στο αρχείο **newreq.pem** και μπορούμε να το δούμε με την εντολή:

- «cat newreq.pem»

```
-----BEGIN CERTIFICATE REQUEST-----
MIICAzCCAWwCAQAwgZYxCzAJBgNVBAYTAkRFMRQwEgYDVQQIEwtCcmFuZGVuYnVy
ZzEPMA0GA1UEBxMGQmVybGluMRIwEAYDVQQKEwlNeUNvbXBhbnkxFDASBgNVBAsT
C0JlcmxpbiBVbml0MRIwEAYDVQQDEwlSZXF1ZXN0ZXIxIjAgBgkqhkiG9w0BCQEW
E215Y29tcGFueUBiZXJsaW4uZGUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AOb1kB3P/QCPr9Dgj0gTqIX5k4FFJKIV37I0QZRmt8p0wTd1zBuqTB88Bqp/9BWu
dCOaatIUjq1v2FqrbnZ4B5cm8sDlhbK/NtH++6fS/uULuW4gKbHbdK+nBvC5LpYT
UQ0EYUbvYbw7zvAbgasJ1RGH82ZrhA7Metfe4PzcYg3rAgMBAAGgLDAUBgkqhkiG
9w0BCQIxBxMFZXJtaXMwFAYJKoZIhvcNAQkHMQcTBWVybWlzMA0GCSqGSIb3DQEB
BQUAA4GBAKotK4QEWhRJbnG1ihIfmMAvBRilZ7Boe8McM5ErUyGefFhIqvxrqtb+
FtaUemOfDWLnAwYqlAEKyyMtdkyyGCSQz3TFIi3MfNyZKb7HOt3GOWvT3aFmmtt4
3BechshRH7lODgtpmdj9wi+wVS2oTce4h1iFWX6hrLk+ygw1OT9n
-----END CERTIFICATE REQUEST-----
```

Πίνακας 5:Κρυπτογραφημένο αίτημα πιστοποιητικού και κλειδιά χρήστη

Αποκωδικοποίηση του certificate request (χρησιμοποιώντας τον αλγόριθμο RSA) με την εντολή:

- «openssl req -text -noout < newreq.pem»

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject:    C=DE,    ST=Brandenburg,    L=Berlin,    O=MyCompany,
OU=BerlinUnit, CN=Requester/emailAddress=mycompany@berlin.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:e6:f5:90:1d:cf:fd:00:8f:af:d0:e0:8f:48:13:
a8:85:f9:93:81:45:24:a2:15:df:b2:34:41:94:66:
b7:ca:74:c1:37:75:cc:1b:aa:4c:1f:3c:06:aa:7f:
f4:15:ae:74:23:9a:6a:d2:14:8e:ad:6f:d8:5a:ab:
6e:76:78:07:97:26:f2:c0:e5:85:b2:bf:36:d1:fe:
fb:a7:d2:fe:e5:0b:b9:6e:20:29:b1:db:74:af:a7:
06:f0:b9:2e:96:13:51:0d:04:61:46:ef:61:bc:3b:
ce:f0:1b:81:ab:09:d5:11:87:f3:66:6b:84:0e:cc:
7a:d7:de:e0:fc:dc:62:0d:eb
            Exponent: 65537 (0x10001)
```

```
 Attributes:
             unstructuredName         :********
             challengePassword        :********
     Signature Algorithm: sha1WithRSAEncryption
         aa:2d:2b:84:04:5a:14:49:6e:71:b5:8a:12:1f:98:c0:2f:05:
 18:a5:67:b0:68:7b:c3:1c:33:91:2b:53:21:9e:7c:58:48:aa:
 fc:6b:aa:d6:fe:16:d6:94:7a:63:9f:0d:62:e7:03:06:2a:94:
 01:0a:cb:23:2d:76:4c:b2:18:24:90:cf:74:c5:22:2d:cc:7c:
 dc:99:29:be:c7:3a:dd:c6:39:6b:d3:dd:a1:66:9a:db:78:dc:
 17:9c:86:c8:51:1f:b9:4e:0e:0b:69:99:d8:fd:c2:2f:b0:55:
 2d:a8:4d:c7:b8:87:58:85:59:7e:a1:ac:b9:3e:ca:0c:35:39:
 3f:67
```

Πίνακας 6:Αποκρυπτογραφημένο αίτημα πιστοποιητικού και κλειδιά χρήστη

Υπογραφή από το CA του ζητούμενου πιστοποιητικού με τη εντολή :

- «./CA.pl –sign»

```
Using configuration from /usr/lib/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
```

Serial Number:e7:95:62:aa:bb:20:e9:a2		
Validity: Not Before: Feb 17 00:00:05 2011 GMT Not After : Feb 17 00:00:05 2012 GMT		
Subject:		
countryName	=	DE
stateOrProvinceName	=	Brandenburg
localityName	=	Berlin
organizationName	=	MyCompany
organizationalUnitName	=	Berlin Unit

commonName = Requester
emailAddress = mycompany@berlin.de
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier: 3A:18:B6:5E:E5:0C:B4:F6:F8:59:74:19:C9:71:3F:36:CD:91:56:45
X509v3 Authority Key Identifier: keyid:97:AB:02:E5:2A:0D:41:C8:22:D8:EA:57:82:C1:3F:57:5D:7B:D1:78
Certificate is to be certified until Feb 17 00:00:05 2012 GMT (365 days)

Πίνακας 7:Στοιχεία πιστοποιητικού για υπογραφή από CA

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]**y**

Write out database with 1 new entries

Data Base Updated

Signed certificate is in newcert.pem

Το νέο πιστοποιητικό είναι το **newcert.pem** και μπορούμε να το δούμε με την παρακάτω εντολή:

- «cat newcert.pem»

Certificate:
Data:

Version: 3 (0x2)
Serial Number:
e7:95:62:aa:bb:20:e9:a2
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=GR, ST=Macedonia, O=DemoCA, OU=DemoCA Unit, CN=Admin of CA/emailAddress=admin@ca.org
Validity:
Not Before: Feb 17 00:00:05 2011 GMT Not After : Feb 17 00:00:05 2012 GMT
Subject: C=DE, ST=Brandenburg, L=Berlin, O=MyCompany, OU=Berlin Unit, CN=Requester/emailAddress=mycompany@berlin.de
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):

00:e6:f5:90:1d:cf:fd:00:8f:af:d0:e0:8f:48:13: a8:85:f9:93:81:45:24:a2:15:df:b2:34:41:94:66: b7:ca:74:c1:37:75:cc:1b:aa:4c:1f:3c:06:aa:7f: f4:15:ae:74:23:9a:6a:d2:14:8e:ad:6f:d8:5a:ab: 6e:76:78:07:97:26:f2:c0:e5:85:b2:bf:36:d1:fe: fb:a7:d2:fe:e5:0b:b9:6e:20:29:b1:db:74:af:a7: 06:f0:b9:2e:96:13:51:0d:04:61:46:ef:61:bc:3b: ce:f0:1b:81:ab:09:d5:11:87:f3:66:6b:84:0e:cc: 7a:d7:de:e0:fc:dc:62:0d:eb Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier: 3A:18:B6:5E:E5:0C:B4:F6:F8:59:74:19:C9:71:3F:36:CD:91:56:45
X509v3 Authority Key Identifier: keyid:97:AB:02:E5:2A:0D:41:C8:22:D8:EA:57:82:C1:3F:57:5D:7B:D1:78
Signature Algorithm: sha1WithRSAEncryption5c: 19:8f:91:23:ee:95:bf:aa:32:12:ca:7b:de:ea:2a:02:7a: f4:de:9a:87:a2:19:43:2c:59:2a:48:26:99:5d:9f:ba:b0:19: ab:00:91:12:45:ee:6e:51:bb:96:b3:ef:9c:a0:39:b3:37:68: d7:83:e3:33:ea:6b:9e:6d:08:32:e5:1e:c5:4a:78:49:7f:6a: 90:74:39:5d:fd:65:2a:30:33:5e:8c:ae:23:96:ff:68:fe:74: ec:20:f3:39:f5:2c:f4:bf:d5:54:ca:00:15:4c:55:8f:50:b9: 16:00:82:25:1a:ba:67:7a:5d:1f:14:ae:dc:3b:53:23:b8:6a: c4:ca

Πίνακας 8:Μορφή και δεδομένα πιστοποιητικού χρήστη

-----BEGIN CERTIFICATE-----


```
MIIDCzCCAnSgAwIBAgIJAOeVYqq7IOmiMA0GCSqGSIb3DQEBBQUAMHsxCzAJBgNV
BAYTAkdSMRIwEAYDVQQIEwlNYWNlZG9uaWExDzANBgNVBAoTBkRlbW9DQTEUMBIG
A1UECxMLRGVtb0NBIFVuaXQxFDASBgNVBAMTC0FkbWluIG9mIENBMRswGQYJKoZI
hvcNAQkBFgxhZG1pbkBjYS5vcmcwHhcNMTEwMjE3MDAwMDA1WhcNMTIwMjE3MDAw
MDA1WjCBljELMAkGA1UEBhMCREUxFDASBgNVBAgTC0JyYW5kZW5idXJnMQ8wDQYD
VQQHEwZCZXJsaW4xEjAQBgNVBAoTCU15Q29tcGFueTEUMBIGA1UECxMLQmVybGlu
IFVuaXQxEjAQBgNVBAMTCVJlcXVlc3RlcjEiMCAGCSqGSIb3DQEJARYTbXljb21w
YW55QGJlcmxpbi5kZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA5vWQHc/9
AI+v0OCPSBOohfmTgUUkohXfsjRBlGa3ynTBN3XMG6pMHzwGqn/0Fa50I5pq0hSO
rW/YWqtudngHlybywOWFsr820f77p9L+5Qu5biApsdt0r6cG8LkulhNRDQRhRu9h
vDvO8BuBqwnVEYfzZmuEDsx6197g/NxiDesCAwEAAaN7MHkwCQYDVR0TBAIwADAs
BglghkgBhvhCAQ0EHxYdT3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYD
VR0OBBYEFDoYtl7lDLT2+Fl0GclxPzbNkVZFMB8GA1UdIwQYMBaAFJerAuUqDUHI
ItjqV4LBP1dde9F4MA0GCSqGSIb3DQEBBQUAA4GBAFwZj5Ej7pW/qjISynve6ioC
evTemoeiGUMsWSpIJpldn7qwGasAkRJF7m5Ru5az75ygObM3aNeD4zPqa55tCDLl
HsVKeEl/apB0OV39ZSowM16MriOW/2j+dOwg8zn1LPS/1VTKABVMVY9QuRYAgiUa
umd6XR8Urtw7UyO4asTK
```


Πίνακας 9:Κρυπτογραφημένη μορφή πιστοποιητικού χρήστη

-----END CERTIFICATE-----

- Για να αποκρυπτογραφήσουμε το Private Key (newreq.pem) σε ένα νέο αρχείο (`newkey.pem`) μπορούμε να εκτελέσουμε την εντολή:

- «openssl rsa < newreq.pem > newkey.pem»

Τελικά αρχεία:

- **Το πιστοποιητικό είναι το `newcert.pem`.**
- **Το κλειδί του χρήστη είναι το `newreq.pem` (κρυπτογραφημένο) ή**
- **Το `newkey.pem` (μη κρυπτογραφημένο)**

13 *Κεφάλαιο*

ΕΠΙΛΟΓΟΣ

Κατά τη διάρκεια κάθε είδους συναλλαγής σε ευρύ δίκτυα μπορούν να αντιμετωπιστούν ορισμένες απειλές είτε ακούσιες που οφείλονται σε φυσικά αίτια ή άγνοια, είτε απειλές οφειλόμενες σε κακόβουλη ενέργεια με την πραγματοποίηση επίθεσης. Η επίθεση μπορεί να έχει στόχο την υποκλοπή προσωπικών δεδομένων που μεταδίδονται κατά τη διάρκεια πραγματοποίησης της συναλλαγής ή την καταστροφή πληροφοριών και πόρων του συστήματος. Απόρροια όλων αυτών είναι οι ανάπτυξη τεχνολογιών και μηχανισμών που θα δώσουν τη δυνατότητα πραγματοποίησης ασφαλών επικοινωνιακών διαύλων. Οι κυριότερες απαιτήσεις ασφάλειας είναι η Εμπιστευτικότητα, η Ακεραιότητα της πληροφορίας που μεταβιβάζεται και η Διαθεσιμότητα του συστήματος. Παραπάνω αναλύθηκαν οι τεχνολογίες, οι τεχνικές και οι μηχανισμοί που συγκεντρώνονται σε μια ολοκληρωμένη αρχιτεκτονική για την ικανοποίηση των παραπάνω απαιτήσεων. Η Υποδομή Δημόσιου Κλειδιού αποτελεί το πλαίσιο που τα συμπεριλαμβάνει και λειτουργεί για την προστασία των πληροφοριών που μεταφέρονται και κατ'έκταση των χρηστών που συμμετέχουν. Ο στόχος είναι να παράσχει έναν μηχανισμό εμπιστοσύνης που ενισχύει το επίπεδο κρυπτογράφησης που βρίσκεται στα ηλεκτρονικά ταχυδρομεία και στις εφαρμογές Ιστού.

12.1 Σύνοψη και συμπεράσματα

Βασική τεχνολογία που χρησιμοποιείται για την εξασφάλιση των απαιτήσεων ασφάλειας είναι η Κρυπτογραφία. Η Κρυπτογραφία θεωρείται μια επιστήμη η οποία έχει οποία έχει στόχο την απόκρυψη και διατήρηση της μυστικότητας της πληροφορίας. Οι προσπάθειες για τη διατήρηση της μυστικότητας έχουν αναπτυχθεί εδώ και πολλά χρόνια τους σημαντικότερους σταθμούς τον αλγόριθμο του Καίσαρα και τη γερμανική μηχανή Enigma. Η κρυπτογραφία περιλαμβάνει την υλοποίηση περίπλοκων αλγορίθμων οι οποίοι αλγόριθμοι βασίζονται σε μαθηματικές πράξεις και την ύπαρξη ενός κλειδιού για να μετασχηματίσουν το αρχικό κείμενο σε μια μορφή η οποία

θα είναι δυασανάγνωστη.Αυτή η διαδικασία ονομάζεται κρυπτογράφηση. Η αντίστροφη διαδικασία της της επαναφοράς του αρχικού κειμένου από τη μετασχηματισμένη μορφή στο αρχικό κείμενο ονομάζεται αποκρυπτογράφηση και χρησιμοποιεί τον ίδιο αλγόριθμο και το κλειδί για να το αποκτήσει. Οι δύο πιο σημαντικοί μέθοδοι κρυπτογράφησης είναι η Συμμετρική και η Ασύμμετρη.Στη συμμετρική κρυπτογράφηση οι πιο γνωστοί αλγόριθμοι που χρησιμοποιούνται είναι ο DES, ο TDES και ο IDEA και γίνεται χρήση ενός κοινού μυστικού κλειδιού. Στην ασύμμετρη κρυπτογράφηση οι πιο σημαντικοί αλγόριθμοι είναι ο RSA, και Diffe-Helman (ανταλλαγή κλειδιών) και χρησιμοποιεί ένα ζεύγος κλειδιών (δημόσιο,ιδιωτικό).Μία άλλη τεχική που χρησιμοποιείται σήμερα είναι η ψηφιακή υπογραφή η λειτουργεί παρόμοια με την ιδιόχειρη για την αυθεντικοποίηση εγγράφου ή χρήστη. Οι ψηφιακές υπογραφές παράγονται με τη χρήση συναρτήσεων κατακερματιμού (hash functios) για τη παραγωγή συνόψεως ενός κειμένου και στη συνέχεια αλγόριθμους ασύμμετρης κρυπτογράφησης για τη κρυπτογράφηση της σύνοψης.

Τα ψηφιακά πιστοποιητικά δημιουργήθηκαν για να πιστοποιήσουν την ταυτότητα των συμβαλλόμενων μέρων μιας συναλλαγής. Για τη έκδοση και ορθή διαχείριση των ψηφιακών πιστοποιητικών δημιουργήθηκε η Υποδομή Δημόσιου Κλειδιού η οποία αποτελείται από Αρχές Υπηρεσιών που εκτελούν τις διαδικασίες για την εγγραφή ενός χρήστη, την έκδοση,διανομή, αποθήκευση, αναζήτηση, ανάκληση και ανανέωση των πιστοποιητικών. Μια Υποδομή Δημόσιου κλειδιού είναι μια οργανωμένη υποδομή των προαναφερθέντων τεχνολογιών, της ασύμμετρης κρυπτογραφίας, τις ψηφιακές υπογραφές, ασφαλών πρωτοκόλλων επικοινωνίας όπως επίσης των Αρχών Υπηρεσιών που απευθύνονται οι χρήστες για τα πιστοποιητικά τους και τη πολιτική η οποία ορίζει τους τεχινούς και νομικούς όρους που τη διέπουν με αποτέλεσμα να παράγει αποτελεσματικούς μηχανισμούς προστασίας των συναλλαγών μέσω διαδικτύου.Κύριος στόχος είναι η άρτια, επιμελής και αποτελεσματική οργάνωση μιας Υποδομής Δημόσιου Κλειδιού καθώς τα μέρη που την απαρτίζουν συνδέονται μεταξύ τους σαν μια αλυσίδα. Επομένως, κανένα μέρος της δεν θα πρέπει να παρεκκλίνει των υποχρεώσεων του ώστε να θεωρείται έμπιστη και να εξαλειφθεί η περίπτωση αποτυχίας της.

12.2 Μελλοντικές επεκτάσεις

Η παρούσα εργασία παρουσιάζει τη βασική δομή και λειτουργία μιας Υποδομής Δημόσιου Κλειδιού και περιγράφει τους τις τεχνολογίες και τις υπηρεσίες που λειτουργούν σε αυτή. Επιπλέον αναπτύχθηκε μια πρότυπη Πολιτική Πιστοποίησης η οποία ακολουθεί το πρότυπο RFC 3647 και προτείνει τους όρους και τις διαδικασίες που διέπουν μια πρότυπη Υποδομή Δημόσιου Κλειδιού για τις ανάγκες της σχολής. Η πρότυπη Πολιτική Πιστοποίησης

μπορεί να τροποποιηθεί ανάλογα με τις ανάγκες και τις απαιτήσεις που μπορεί να προκύψουν κατά τη δημιουργία μιας Υποδομής Δημόσιου Κλειδιού του Πανεπιστημίου Στερεάς Ελλάδας. Ακόμη δημιουργήθηκε σε λειτουργικό σύστημα Linux Υπηρεσία Πιστοποίησης η οποία λειτουργεί ως Αρχή Πιστοποίησης και δίνει τη δυνατότητα σε ένα χρήστη να αιτηθεί ένα πστοποιητικό συμπληρώνοντας τα στοιχεία που του ζητά η υπηρεσία και στη συνέχεια να δημιουργεί και να υπογράφει το πιστοποιητικό στο όνομα του χρήστη που αιτήθηκε. Μια μελλοντική επέκταση είναι η υλοποίηση σε Web Interface όπου μετά την αίτηση του χρήστη θα του αποστέλλεται ένας κωδικός στη διεύθυνση του mail το οποίο ο χρήστης θα πρέπει να εισάγει κατά την παραλαβή του πιστοποιητικού του, για την επιπλέον επιβεβαίωση της εγκυρότητας των στοιχείων της ταυτότητας του χρήστη. Επίσης θα μπορούσαν να δημιουργηθούν μηχανισμοί για την ασφαλή αποθήκευση των εκδοθέντων πιστοποιητικών αλλά και μηχανισμοί αναζήτησης των πιστοποιητικών σε περιβάλλον φιλικό προς τους χρήστες. Τέλος, σε περίπτωση ανάκλησης πιστοποιητικών προτείνεται η δημοσίευση Λιστών Ανάκλησης Πιστοποιητικών για την έγκαιρη και σωστή ενημέρωση των χρηστών για τη κατάσταση και ισχύς των εκθοθέντων πιστοποιητικών.

Βιβλιογραφία

[1] **S. Harris**, (2008), *CISSP*, by the McCrow Hill Companies

[2] **Σ. Γκρίτζαλη, Σ. Κ. Κάτσικα, Δ. Γκρίτζαλη**,(2003), *Ασφάλεια Δικτύων Υπολογιστών*, Εκδόσεις Παπασωτηρίου

[3] **D.Gollmann**, (1999), *Computer Security*, USA John Wiley and Sons Ltd

[4] **W. Stallings**, (2000), *Network Security Essentials*, Prentice Hall

[5] **W. Stallings**, (2003), *Λειτουργικά Συστήματα Αρχές Σχεδίασης* 4η Έκδοση, Εκδόσεις Τζιόλα

[6] **W. Stallings**, (2003), *Επικοινωνίες Υπολογιστών και Δεδομένων*, Έκτη Έκδοση, Εκδόσεις Τζιόλα

[7] http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html#1

[8] **Phil Zimmermann**, An Introduction to Cryptography, free-ebook

[9] http://www.verisign.com/repository/eca/cps/eca_cps_31jan05_ver1.pdf

[10] http://noc.auth.gr/services/personal/certificates/index.html

[11] **D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang**, (2008), Introduction to Public Key Technology and the Federal PKI Infrastructure

[12] **Forum Ηλεκτρονικής Διακυβέρνησης**, *Διαλειτουργικότητα Οργανισμών, Υπηρεσιών και Συστημάτων Δημόσιας Διοίκησης, Τελικό Παραδοτέο,* Νοέμβριος 2008, Έκδοση 2.6 στο:http://www.iocenter.eu/media/20332/egovforum_interoperability_finalreport.pdf

[13] http://www.pki.auth.gr/documents/CPS.html

[14] **International Telecommunication Union-Telecommunication sector**, (1997), *X.509:The Directory Authentication Framework*, διαθέσιμο στο

(ftp://ftp.bull.com/pub/OSIdirectory/ITU/X.509/97x509final.doc)

[15] **Intel**, (1998), *Intel security Initiative*, White Paper

[16] **Baltimore Technologies**, (1998), *PKI-PLUS Overview*, White Paper

[17] **Comer Douglas E., Steven David L.**, (1999), *Internetworking with TCP/IP: Design, Implementation and Internals*, Volume II, Third Edition, Prentice Hall, Upper Saddle River, NJ

[18] **B. Goodheart, and Cox, J.**, (1994), *The Magic Garden Explained: The Internals of UNIX System* V release 4, Prentice Hall

[19] **RSA Laboratories**, (2002), *RSA Cryptography Standard, RSA,* Security Inc, PKCS#1 v2.1

[20] **PLANET-ΕΠΙΣΕΥ-ATC, Πανεπιστήμιο Αιγαίου**, (2008), *Πλαίσιο Ψηφιακής Αυθεντικοποίησης*.

[21] **A.Henezes, P. van Oorschot, S.Vanstein**, (1997), *Handbook applied cryptography*, by CRC Press Inc. http://www.cacr.math.uwaterloo.ca/hac/

[22] **W. Burr**, (1997), *FPKI Records to support later validation of digital signatures*, PKIX group Internet draft.

[23] **ISO Open Systems Interconnection**, *Basic Reference Model*, Management Framework, 1989

[24] **Σ. Κάτσικα**, (2001), *Προστασία και Ασφάλεια Συστημάτων Υπολογιστών*: Ασφάλεια Δικτύων, Ελληνικό Ανοικτό Πανεπιστήμιο,

[25] **W.Stallings**., (1995), *Network and Internetwork Security*, IEEE Press

[26] http://www.harica.gr/documents/CPS.html

[27] http://pki.syzefxis.gov.gr/page0003.htm

[28] www.iana.org

[29] http://www.digicert.com/csr-creation.htm

[30] **M. Krause, Harold F. Tipton**,*Handbook of Information Security Management* ,CRC Press LLC

[31] **P.Muller**,(1993), *Funtional Model of Trusted Third Party Services*, INFOSEC prospect,.

[32] http://datatracker.ietf.org/doc/rfc3647/

[33] http://www.go-online.gr/ebusiness/specials/article.html

[34] **S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu,** (November 2003)**, "***RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*",IETF. **Διαθέσιμο στο :**(http://www.rfc-editor.org/cgi-bin/rfcsearch.pl)

[35] http://www.cert.org/encyc_article/tocencyc.html#Crypt

[36] http://users.uom.gr/~kaklaman/book/Chapters/C11/Cryptography%20and%20its%20products%204.htm

[37] http://www.eett.gr/opencms/opencms/admin/downloads/telec/PD150.pdf

[38] http://technet.microsoft.com/el-gr/library/

[39] pst.libre.lu/mssi-luxmbg/p3/02_std-prot-art.html

[40] http://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf

[41] http://help.ubuntu-gr.org/10.04/serverguide/el/certificates-and-security.html

[42] **R. Housley, W. Polk, W. Ford and D. Solo**, (April 2002), *"RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"*, IETF. **Διαθέσιμο στο :** (ftp://ftp.rfc-editor.org/in-notes/rfc3280.txt)

[43] **M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams,** (June 1999), **"***X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP",IETF. Διαθέσιμο στο* (http://www.rfc-editor.org/rfc/rfc2560.txt)

[44] **Professional it security**, *Περιοδικό για το Enterprise Computing και την Ασφάλεια στην Πληροφορική*, 2006 Press Line LTD στο (http://www.securitymanager.gr/it_security)

[45] **Alan O. Freier, P.Karlton, Paul C. Kocher**,(November 18, 1996), *The SSL Protocol Version 3.0,*Internet-draft ,Διαθέσιμο στο (http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00) (http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00)

[46] **Κύτταρο, Περιοδικό Επιστήμης και Τεχνολογίας** *(13 Οκτωβρίου 2010)***,** *αρθρο:Κρυπτογραφία*

[47] http://www.tech-faq.com/pki-certificate.html

[48] http://pki.syzefxis.gov.gr/docs/KANONISMOS_PISTOPOIHSHS_PKI%5B1%5D.pdf

[49] http://el.wikipedia.org

Ευρετήριο