ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων

Κατεύθυνση: Ασφάλεια Ψηφιακών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΥΠΟΔΟΜΕΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ
PUBLIC KEY INFRASTRUCTURES

ΚΛΕΑΝΘΗΣ ΝΟΟΥ

ΠΕΙΡΑΙΑΣ – ΜΑΙΟΣ 2013

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων

Κατεύθυνση: Ασφάλεια Ψηφιακών Συστημάτων

Διπλωματική Εργασία

Θέμα : Υποδομές Δημόσιου Κλειδιού – Public Key Infrastructures

Κλεάνθης Νόου

Υπεύθυνος : Επίκουρος Καθηγητής Κωνσταντίνος Λαμπρινουδάκης

Πειραιάς, Μάιος 2013

Στη Λίνα

ΕΥΧΑΡΙΣΤΙΕΣ

Ολοκληρώνοντας την παρούσα διπλωματική εργασία, θα ήθελα να ευχαριστήσω θερμά τον καθηγητή κύριο Κωνσταντίνο Λαμπρινουδάκη, Επίκουρο Καθηγητή του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς, για την ανάθεση του συγκεκριμένου θέματος, την εμπιστοσύνη που μου έδειξε, την πολύτιμη καθοδήγησή του, καθώς και τις επιστημονικές γνώσεις που μου μετάδωσε κατά τη διάρκεια των σπουδών μου.

Επιπλέον, θα ήθελα να ευχαριστήσω όλους τους διδάσκοντες Καθηγητές του Προγράμματος Μεταπτυχιακών Σπουδών Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων με κατεύθυνση Ασφάλεια Ψηφιακών Συστημάτων του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς, για την παιδεία και την ενθάρρυνση που μου παρείχαν στην πορεία ολοκλήρωσης του μεταπτυχιακού προγράμματος.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Σκοπός της παρούσας διπλωματικής εργασίας είναι η ολοκληρωμένη προσέγγιση του θέματος Υποδομές Δημόσιου Κλειδιού (Public Key Infrastructures) σε επιστημονικό, επιχειρησιακό και τεχνικό επίπεδο.

Στόχοι της εργασίας είναι να προσδιορισθούν οι κρίσιμοι παράγοντες επιτυχίας για την ανάπτυξη και λειτουργία μίας Υποδομής Δημόσιου Κλειδιού (ΥΔΚ) και να υλοποιηθεί ένα πλήρως λειτουργικό εργαστηριακό περιβάλλον εκπαίδευσης και εργασίας, το οποίο να επιτρέπει την εκπόνηση εργασιών και μελετών περίπτωσης αναφορικά με τη σχεδίαση, ανάπτυξη, διαχείριση και λειτουργία μίας ΥΔΚ.

Η μεθοδολογία που ακολουθήθηκε για την επίτευξη των παραπάνω στόχων ήταν η κριτική ανασκόπηση της σχετικής επιστημονικής βιβλιογραφίας και των τεχνικών προδιαγραφών, η διεξοδική ανάλυση του επιχειρησιακού μοντέλου ανάπτυξης και λειτουργίας μίας ΥΔΚ ευρείας κλίμακας, για την παροχή προηγμένων ηλεκτρονικών υπηρεσιών προστιθέμενης αξίας, καθώς και η υλοποίηση μίας ολοκληρωμένης ΥΔΚ για τη διαχείριση του κύκλου ζωής των ψηφιακών πιστοποιητικών χρησιμοποιώντας λογισμικό ανοιχτού κώδικα.

Αναλυτικότερα, στο πρώτο κεφάλαιο παρουσιάζεται μία σύντομη εισαγωγή στο θέμα, ενώ ο πυρήνας του γνωστικού αντικειμένου εξετάζεται στο δεύτερο κεφάλαιο, αναφορικά με τα επίσημα πρότυπα Public Key Infrastructure X.509 (PKIX) της Ομάδας Δράσης για τη Διαδικτυακή Μηχανική (Internet Engineering Task Force). Στο τρίτο κεφάλαιο παρουσιάζεται η επιχειρησιακή ανάλυση του αρχιτεκτονικού μοντέλου PKIX με στόχο να προσδιορισθούν τα πλεονεκτήματα, τα μειονεκτήματα, οι ευκαιρίες και οι απειλές, καθώς και οι κρίσιμοι παράγοντες επιτυχίας των ΥΔΚ. Η τεχνική υλοποίηση μίας πλήρως λειτουργικής ΥΔΚ τεκμηριώνεται αναλυτικά στο τέταρτο κεφάλαιο, επιβεβαιώνοντας τα συμπεράσματα της προηγούμενης επιχειρησιακής ανάλυσης.

Προτείνεται μία τεχνική μάθησης η οποία προβλέπει την εκπόνηση εργασιών βασισμένες σε σενάρια παροχής ηλεκτρονικών υπηρεσιών, που περιλαμβάνουν την ανάλυση των απαιτήσεων ασφάλειας, τον προσδιορισμό και τεκμηρίωση των κατάλληλων πολιτικών πιστοποιητικών, τη σχεδίαση, καθώς και την πρακτική υλοποίηση της ΥΔΚ που θα υποστηρίζει την παροχή της υπηρεσίας. Επιπλέον, στο τέταρτο κεφάλαιο περιγράφεται η υλοποίηση της εκπαιδευτικής πρότασης, με την εγκατάσταση ενός ολοκληρωμένου εργαστηριακού περιβάλλοντος εκπαίδευσης και εργασίας για τη σχεδίαση, ανάπτυξη, διαχείριση και λειτουργία μίας ΥΔΚ μέσω γραφικού περιβάλλοντος προσομοίωσης.

Επίσης, παρουσιάζεται μία μελέτη περίπτωσης η οποία αφορά την ανάπτυξη μίας ιεραρχικής ΥΔΚ με στόχο τη διαχείριση των πιστοποιητικών, τα οποία θα διατίθενται στα μέλη ΔΕΠ και στους φοιτητές ενός πανεπιστημίου για την υποστήριξη της ηλεκτρονικής υπηρεσίας υποβολής των εργασιών στο πλαίσιο των μαθημάτων. Εξετάζονται οι απαιτήσεις ασφάλειας και αναλύονται οι διαδικασίες εγγραφής και χρήσης της ηλεκτρονικής υπηρεσίας. Οι προτάσεις και τα συμπεράσματα της διπλωματικής εργασίας καταγράφονται στο πέμπτο και τελευταίο κεφάλαιο.

ABSTRACT

This thesis aims to provide a thorough analysis of the subject Public Key Infrastructures in an academic, operational and engineering level.

Main objectives are to determine the critical factors of success for the design and implementation of a Public Key Infrastructure (PKI) and to develop in a laboratory environment a fully functional test infrastructure for the establishment, deployment, management, operation and support of a complete PKI infrastructure.

The applied methodology for achieving the above mentioned goals was the critical review of the related scientific literature, the detailed examination of a large scale PKI development and operation business model, for the provision of advanced value added electronic services and the implementation of an open source platform independent PKI for testing with digital certificate life cycle management.

Analytically, in the first section there is a short introduction, while the core of the cognitive subject is examined in the second section, in relation to the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) architectural model. The third section presents the results of a SWOT analysis performance aiming to determine the benefits, drawbacks, opportunities and threats and especially the critical factors of success in PKI. The documented implementation of an open source, platform independent, flexible, and component based PKI is presented in the fourth section, with a detailed analysis of typical case studies. The conclusions are discussed in the fifth and final section of this thesis.

1. ΕΙΣΑΓΩΓΗ

Η ψηφιακή εποχή χαρακτηρίζεται από την ανάπτυξη και καθιέρωση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ) σε όλες τις διαστάσεις της ζωής και τους τομείς δραστηριότητας των ανθρώπων. Η αξία των συναλλαγών και ο όγκος των δεδομένων που επεξεργάζονται και διακινούνται ηλεκτρονικά, από πληροφοριακά συστήματα και δίκτυα σε παγκόσμιο επίπεδο, αυξάνεται εκθετικά με την πάροδο του χρόνου και συνεπώς, η ασφάλεια της πληροφορίας και η προστασία της ιδιωτικότητας αποτελούν πλέον στρατηγικές επιλογές σε κάθε σύγχρονη κοινωνία.

Η παροχή προηγμένων ηλεκτρονικών υπηρεσιών και η μετάδοση κρίσιμων δεδομένων, ικανοποιώντας τις βασικές απαιτήσεις ασφάλειας, οι οποίες είναι η ακεραιότητα, η αυθεντικοποίηση, η εμπιστευτικότητα και η μη αποποίηση ευθύνης, προϋποθέτει την ανάπτυξη σύγχρονων υποδομών πληροφορικής και μοντέλων εμπιστοσύνης με στόχο την αποτελεσματική διαχείριση του κινδύνου, μέσω της εφαρμογής αυστηρών πολιτικών ασφάλειας και προηγμένων κρυπτογραφικών μηχανισμών.

Η επιτυχημένη υλοποίηση και η αποδοτική λειτουργία ολοκληρωμένων υποδομών ασφάλειας της πληροφορίας, σε επίπεδο επιχείρησης, οργανισμού ή πολιτείας, απαιτεί την έμπρακτη δέσμευση της ηγεσίας για την εξασφάλιση των αναγκαίων πόρων, ένα ισχυρό νομοθετικό πλαίσιο που να θεσμοθετεί τη χρήση των ψηφιακών υπογραφών, την επίγνωση και εκπαίδευση των χρηστών σε θέματα διαχείρισης πιστοποιητικών, μία αποτελεσματική οργανωτική δομή, μία άρτια τεχνική υλοποίηση των συστημάτων, έμπειρο και ικανό προσωπικό, καθώς και τη συμμόρφωση με τα αναγνωρισμένα διεθνή ελεγκτικά πρότυπα και πιστοποιήσεις ασφάλειας.

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI) δημιουργεί ένα πλαίσιο εμπιστοσύνης κατάλληλο για την παροχή ποιοτικών ηλεκτρονικών υπηρεσιών προστιθέμενης αξίας, ικανοποιώντας τις απαιτήσεις ασφάλειας, με την εφαρμογή της ασύμμετρης κρυπτογραφίας και τη δυνατότητα διαχείρισης ολόκληρου του κύκλου ζωής των ψηφιακών πιστοποιητικών. Αποτελεί μία ώριμη και εφαρμοσμένη τεχνολογία η οποία θεμελιώνει την ασφάλεια της πληροφορίας στη βάση σχεδίασης και ανάπτυξης κάθε νέου ολοκληρωμένου πληροφοριακού συστήματος, εφαρμογής λογισμικού ή διαδικτυακής υπηρεσίας. Θωρακίζει τις επιχειρησιακές διαδικασίες και συμβάλει ουσιαστικά στην επίτευξη των στόχων ενός οργανισμού, καθώς και στη συμμόρφωση με τις πολιτικές και τους κανονισμούς ασφάλειας.

2. ΘΕΩΡΗΤΙΚΗ ΤΕΚΜΗΡΙΩΣΗ

Στόχος της παρούσας ενότητας είναι η κριτική ανασκόπηση της επιστημονικής βιβλιογραφίας και η αποτύπωση των σύγχρονων συναφών τεχνικών προδιαγραφών και προτύπων.

Στον ψηφιακό κόσμο η μετάδοση ευαίσθητης πληροφορίας και η διεκπεραίωση ηλεκτρονικών συναλλαγών προϋποθέτουν την εγκαθίδρυση σχέσεων αμοιβαίας εμπιστοσύνης μεταξύ των οντοτήτων που συμμετέχουν στην επικοινωνία. Η εμπιστοσύνη αποτελεί το θεμέλιο λίθο για την επιτυχημένη παροχή ποιοτικών ηλεκτρονικών υπηρεσιών προστιθέμενης αξίας στο διαδίκτυο. Η ασφάλεια των διαδικτυακών υπηρεσιών δεν μπορεί να είναι υψηλότερη από το επίπεδο προστασίας που εξασφαλίζει το υφιστάμενο σύστημα υποδομής μέσα στο οποίο παρέχονται. Συνεπώς, ο κρισιμότερος παράγοντας επιτυχίας για την εδραίωση της εμπιστοσύνης είναι ο τρόπος προσδιορισμού της ταυτότητας των συμμετεχόντων στην επικοινωνία.

Η κρυπτογραφία δημόσιου κλειδιού είναι το αποτέλεσμα της έρευνας των επιστημόνων Diffie και Hellman που δημοσιεύθηκε το 1976 με στόχο την επίλυση του προβλήματος διαχείρισης κρυπτογραφικών κλειδιών [1]. Η πρότασή τους αφορούσε την τροποποίηση ενός τηλεφωνικού καταλόγου τον οποίο ονόμασαν Δημόσιο Αρχείο (Public File). Στη θέση των πεδίων “όνομα”, “διεύθυνση” και “αριθμός τηλεφώνου” το Δημόσιο Αρχείο θα περιείχε τα πεδία “όνομα”, “σειριακός αριθμός” και “δημόσιο κλειδί”.

Για την αποστολή ενός εμπιστευτικού μηνύματος ήταν απαραίτητη η εύρεση του δημόσιου κλειδιού του παραλήπτη από το Δημόσιο Αρχείο και στη συνέχεια η κρυπτογράφηση του μηνύματος με αυτό το κλειδί πριν την αποστολή του. Μόνο ο παραλήπτης, κάτοχος του αντίστοιχου ιδιωτικού κλειδιού, θα μπορούσε να αποκρυπτογραφήσει το μήνυμα. Το δύσκολο πρόβλημα ανταλλαγής των κλειδιών είχε πλέον λυθεί, όμως τώρα δημιουργήθηκε εκείνο της ονοματολογίας και της διαχείρισης των ονομάτων.

Ο Kohnfelder, στην εκπόνηση της διπλωματικής του εργασίας στο MIT το 1978, πρότεινε οι καταχωρήσεις στο Δημόσιο Αρχείο να υπογράφονται ψηφιακά [2]. Η υπογεγραμμένη έκδοση των πεδίων ονομάστηκε “πιστοποιητικό”. Τα πιστοποιητικά αυτά θα μπορούσαν τώρα να διανεμηθούν σε όλους όσους τα ζητούσαν.

Η ιδέα της ΥΔΚ γεννήθηκε τη δεκαετία του 80’ ως αποτέλεσμα των εργασιών για τη σύσταση του προτύπου X.509, που αποτελεί τμήμα της σειράς συστάσεων X.500 οι οποίες ορίζουν μία υπηρεσία καταλόγου. Το πρότυπο X.509 εκδόθηκε αρχικά το 1988 και αποτελεί ένα πλαίσιο για την παροχή υπηρεσιών αυθεντικοποίησης από τον κατάλογο X.500 προς τους χρήστες του [3]. Ο κατάλογος ουσιαστικά λειτουργεί ως ένα αποθετήριο για τα πιστοποιητικά δημόσιων κλειδιών. Κάθε πιστοποιητικό περιέχει το δημόσιο κλειδί του χρήστη στον οποίο ανήκει και είναι υπογεγραμμένο με το ιδιωτικό κλειδί μιας έμπιστης αρχής πιστοποίησης.

Επιπλέον, το πρότυπο X.509 ορίζει εναλλακτικά πρωτόκολλα πιστοποίησης τα οποία βασίζονται στη χρήση των πιστοποιητικών δημόσιου κλειδιού. Το X.509 βασίζεται στη χρήση κρυπτογραφίας δημόσιου κλειδιού και ψηφιακών υπογραφών. Το πρότυπο δεν υπαγορεύει τη χρήση κάποιου συγκεκριμένου αλγορίθμου, ωστόσο προτείνει τον κρυπτογραφικό αλγόριθμο RSA [4],[5],[6],[7].

Η Υποδομή Δημόσιου κλειδιού (Public Key Infrastructure – PKI) είναι το σύνολο υλικού, λογισμικού, ανθρώπων, πολιτικών και διαδικασιών που απαιτούνται για την έκδοση, τη διαχείριση, την αποθήκευση, τη διανομή και την ανάκληση ψηφιακών πιστοποιητικών που βασίζονται στην ασύμμετρη κρυπτογραφία [5],[8].

Η Υποδομή Δημόσιου κλειδιού σχεδιάζεται με σκοπό τη δημιουργία του αναγκαίου βαθμού εμπιστοσύνης χρησιμοποιώντας τη δομή ενός ψηφιακού πιστοποιητικού, το

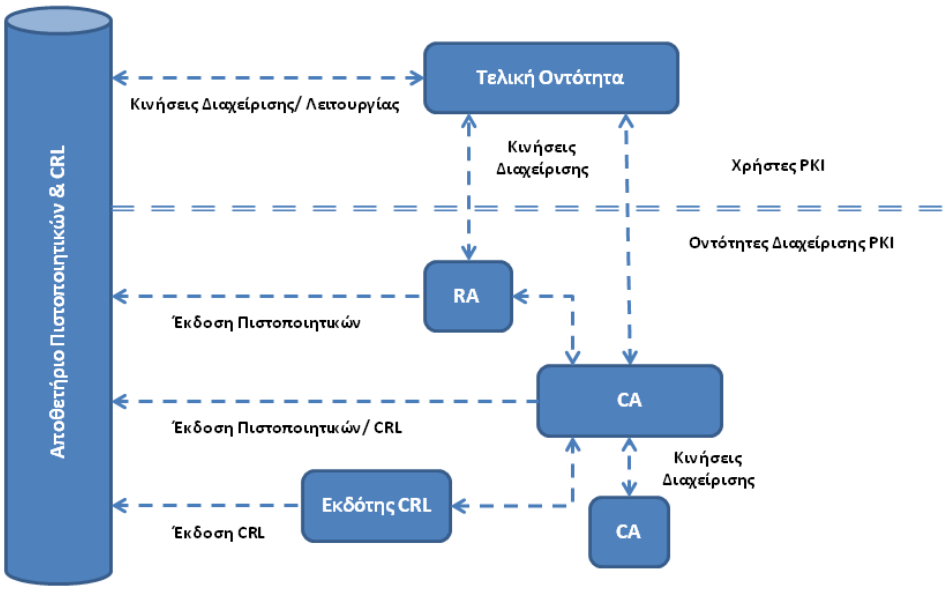
οποίο αποτελεί ένα δεσμό μεταξύ ενός δημόσιου κλειδιού και των αναγνωριστικών στοιχείων του ιδιοκτήτη του. Στόχος της υποδομής είναι η έκδοση και η διαχείριση των ψηφιακών πιστοποιητικών για λογαριασμό όλων των συμμετεχόντων μερών στο υφιστάμενο πληροφοριακό σύστημα.

Μία Υποδομή Δημόσιου Κλειδιού (ΥΔΜ) καλείται να επιλύσει ένα πρακτικό πρόβλημα εφαρμογής της ασύμμετρης κρυπτογραφίας. Ενώ ο ιδιοκτήτης ενός ζευγαριού κρυπτογραφικών κλειδιών (δημόσιο – ιδιωτικό) φυλάσσει υπό τον αποκλειστικό του έλεγχο το ιδιωτικό κλειδί και κοινοποιεί ελεύθερα το δημόσιο, δεν μπορεί να εγγυηθεί με ασφάλεια σε όσους επικοινωνούν μαζί του ότι το δημόσιο κλειδί πράγματι ανήκει στο πρόσωπο που ισχυρίζεται ότι του ανήκει. Κατά συνέπεια, προκύπτει η ανάγκη πιστοποίησης, μέσω ενός αξιόπιστου μηχανισμού, της σχέσης μεταξύ μίας τελικής οντότητας και του δημόσιου κλειδιού της.

Το πρόβλημα αντιμετωπίζεται ορίζοντας μία Έμπιστη Τρίτη Οντότητα (ΕΤΟ) η οποία καλείται Αρχή Πιστοποίησης (ΑΠ). Η Αρχή Πιστοποίησης (Certification Authority – CA) λειτουργεί ως Πάροχος Υπηρεσιών Πιστοποίησης (ΠΥΠ) δημόσιων κλειδιών, επικυρώνοντας τη σχέση ενός δημόσιου κλειδιού με τον ιδιοκτήτη του [9],[10].

2.1. Αρχιτεκτονικό Μοντέλο

Στα μέσα της δεκαετίας του 90’ συστάθηκε, από την IETF (Internet Engineering Task Force), η ομάδα εργασίας Public Key Infrastructure X.509 (PKIX) με σκοπό την κατασκευή ενός πρότυπου γενικού μοντέλου που να στηρίζεται στο X.509 και να είναι κατάλληλο για την ανάπτυξη μίας αρχιτεκτονικής θεμελιωμένης πάνω στη χρήση των ψηφιακών πιστοποιητικών από εφαρμογές και πρωτόκολλα στο διαδίκτυο. Το RFC 5280 αποτελεί το νεότερο έγγραφο προδιαγραφών που προσδιορίζει τις λεπτομέρειες του προφίλ ενός ψηφιακού πιστοποιητικού X.509 v3 [5],[6],[7].



Εικόνα 1. Το Αρχιτεκτονικό Μοντέλο PKIX [RFC 5280]

Οι διασυνδέσεις μεταξύ των βασικών στοιχείων του μοντέλου PKIX, σύμφωνα με το έγγραφο RFC 5280, παρουσιάζονται στην Εικόνα 1 [6]. Τα βασικά στοιχεία του μοντέλου PKIX είναι τα παρακάτω:

- **Τελική Οντότητα (ΤΟ).** Είναι ο χρήστης των πιστοποιητικών PKI ή/και το σύστημα του χρήστη που αποτελεί τον ιδιοκτήτη του πιστοποιητικού.
- **CA.** Είναι η Αρχή Πιστοποίησης (ΑΠ) υπεύθυνη για την κοινοποίηση της κατάστασης εγκυρότητας των πιστοποιητικών που εκδίδει. Η πληροφορία αναφορικά με το εάν ένα πιστοποιητικό παραμένει έγκυρο ή έχει ανακληθεί μπορεί να δοθεί διαμέσου του πρωτοκόλλου Online Certificate Status Protocol (OCSP) [RFC 2560], από τους Καταλόγους Ανάκλησης Πιστοποιητικών (Certificate Revocation Lists – CRLs) ή μέσω κάποιου άλλου μηχανισμού. Κατάλογος Ανακληθέντων Πιστοποιητικών (ΚΑΠ) ονομάζεται ο κατάλογος, περιοδικός (ή έκτακτος) που εκδίδεται ηλεκτρονικά και είναι υπογεγραμμένος από μια ΑΠ, των πιστοποιητικών που έχουν ανακληθεί πριν από την ημερομηνία λήξης τους. Ο ΚΑΠ αναφέρει το όνομα του εκδότη, την ημερομηνία έκδοσης, την ημερομηνία της επόμενης προγραμματισμένης έκδοσης του ΚΑΠ, τους αριθμούς σειράς των ανακληθέντων Πιστοποιητικών, καθώς και τους συγκεκριμένους χρόνους και λόγους ανάκλησής τους.
- **RA.** Είναι η Αρχή Εγγραφής (ΑΕ) η οποία αποτελεί ένα προαιρετικό σύστημα στο οποίο η Αρχή Εγγραφής αναθέτει ορισμένες διαχειριστικές λειτουργίες.
- **Εκδότης CRL.** Ένα σύστημα το οποίο εκδίδει και υπογράφει καταλόγους ανάκλησης πιστοποιητικών.
- **Αποθετήριο.** Ένα σύστημα ή ένα σύνολο κατανεμημένων συστημάτων το οποίο αποθηκεύει πιστοποιητικά και καταλόγους ανάκλησης πιστοποιητικών και λειτουργεί ως μέσο διανομής των πιστοποιητικών και των ΚΑΠ στις τελικές οντότητες.

2.2. Λειτουργίες Διαχείρισης

Η εφαρμογή του μοντέλου PKIX απαιτεί την ανάπτυξη πρωτοκόλλων διαχείρισης και λειτουργίας για την παροχή των πιστοποιητικών και των ΚΑΠ στους τελικούς χρήστες, καθώς και για την υποστήριξη της επικοινωνίας μεταξύ των χρηστών ΥΔΚ και των οντοτήτων διαχείρισης [5],[6]. Το σύνολο των διαχειριστικών λειτουργιών που θα πρέπει να υποστηρίζονται από τα πρωτόκολλα διαχείρισης περιλαμβάνει:

- **Εγγραφή.** Είναι η διαδικασία με την οποία ένας χρήστης συστήνεται αρχικά σε μία CA (απευθείας ή μέσω μίας RA) και προηγείται της διαδικασίας έκδοσης του πιστοποιητικού του χρήστη από την Αρχή Πιστοποίησης.
- **Αρχικοποίηση.** Πριν ένα σύστημα τελικού χρήστη μπορέσει να λειτουργήσει με ασφάλεια, είναι απαραίτητη η εγκατάσταση των ψηφιακών πιστοποιητικών των στοιχείων της ΥΔΚ για την επικύρωση της διαδρομής των πιστοποιητικών.
- **Πιστοποίηση.** Είναι η διαδικασία με την οποία μία CA εκδίδει ένα πιστοποιητικό για το δημόσιο κλειδί ενός χρήστη και επιστρέφει το πιστοποιητικό αυτό στο σύστημα του χρήστη ή/και το δημοσιεύει σε ένα αποθετήριο.

- **Ανάκτηση ζεύγους κλειδιών.** Είναι η δυνατότητα αποθήκευσης ενός εφεδρικού αντιγράφου του ιδιωτικού κλειδιού ενός χρήστη, από τη CA ή από ένα σύστημα λήψης αντιγράφων ασφάλειας κρυπτογραφικών κλειδιών, για την περίπτωση κατά την οποία προκύψει η ανάγκη ανάκτησης ενός απολεσθέντος κρυπτογραφικού κλειδιού.
- **Ανανέωση ζεύγους κλειδιών.** Όλα τα κρυπτογραφικά κλειδιά χρειάζεται να ανανεώνονται ανά τακτικά χρονικά διαστήματα και να εκδίδονται νέα ψηφιακά πιστοποιητικά.
- **Αίτηση ανάκλησης.** Ένα εξουσιοδοτημένο άτομο ενημερώνει τη CA αναφορικά με ένα έκτακτο περιστατικό το οποίο απαιτεί την ανάκληση ενός πιστοποιητικού.
- **Δια-πιστοποίηση.** Δύο CAs ανταλλάσουν πληροφορίες σχετικά με τη δημιουργία ενός δια-πιστοποιητικού. Ένα δια-πιστοποιητικό είναι ένα πιστοποιητικό το οποίο εκδίδεται από μία CA για κάποια άλλη CA και περιέχει ένα κλειδί υπογραφής CA που χρησιμοποιείται για την έκδοση πιστοποιητικών.

2.3. Πρωτόκολλα

Αναφορικά με την υποστήριξη των λειτουργιών διαχείρισης και επικοινωνίας μεταξύ των οντοτήτων μίας ΥΔΚ, έχουν καθοριστεί δύο εναλλακτικά πρωτόκολλα διαχείρισης από την ομάδα εργασίας PKIX. Το RFC 4210 καθορίζει το πρωτόκολλο CMP (Certificate Management Protocol), σύμφωνα με το οποίο η κάθε λειτουργία διαχείρισης πιστοποιητικών προσδιορίζεται ρητά μέσω συγκεκριμένων μηνυμάτων επικοινωνίας. Η βασική δομή της αίτησης πιστοποιητικού ορίζεται στο RFC 4211. Το CMP έχει σχεδιαστεί με γνώμονα την ευελιξία και την ικανότητα να ενσωματώνει μία πλειάδα τεχνικών, λειτουργικών και επιχειρησιακών μοντέλων [5],[11],[12].

Το RFC 5272 ορίζει τα μηνύματα Certificate Management Messages over CMS (CMC), όπου το CMS αναφέρεται στο RFC 5652 Cryptographic Message Syntax. Το CMC έχει βασιστεί σε προγενέστερο έργο και στοχεύει στη βελτίωση υφιστάμενων εφαρμογών. Μολονότι υποστηρίζονται όλες οι λειτουργίες της ΥΔΚ, δεν υπάρχει πλήρης αντιστοίχηση με συγκεκριμένα μηνύματα επικοινωνίας [5],[13],[14].

Τα επιχειρησιακά πρωτόκολλα λειτουργίας είναι εκείνα που χρησιμοποιούνται για τη μετάδοση των πιστοποιητικών, των ΚΑΠ, καθώς και όλης της σχετικής πληροφορίας διαχείρισης μεταξύ των διαφόρων συστατικών στοιχείων της PKIX αρχιτεκτονικής. Το μοντέλο PKIX υποστηρίζει τα πρωτόκολλα LDAP, HTTP, FTP και X.500.

Το Πρωτόκολλο Δικτυακού Ελέγχου Κατάστασης Πιστοποιητικών (Online Certificate Status Protocol – OCSP), το οποίο έχει καθοριστεί από το RFC 2560, χρησιμοποιείται για τον έλεγχο της κατάστασης ανάκλησης των πιστοποιητικών που έχουν εκδοθεί από την Αρχή Πιστοποίησης [15]. Για κάθε αίτηση ελέγχου κατάστασης η υπηρεσία OCSP ελέγχει, σε πραγματικό χρόνο, την κατάσταση ανάκλησης του αντίστοιχου πιστοποιητικού απευθείας από την Αρχή Πιστοποίησης και αποκρίνεται άμεσα στην αίτηση για το αν το πιστοποιητικό έχει ανακληθεί ή όχι.

2.4. Πολιτική Πιστοποιητικών και Δήλωση Πρακτικής

Η ΥΔΚ λειτουργεί σύμφωνα με μία Πολιτική Πιστοποιητικών (Certification Policy) και με μία Δήλωση Πρακτικής (Certification Practice Statement), οι οποίες καλύπτουν νομικά και τεχνικά θέματα που αφορούν τα ψηφιακά πιστοποιητικά και τη διαδικασία έκδοσης. Το πρότυπο Internet X.509 Public Key Infrastructure Certificate Policy and

Certification Practices Framework (Πλαίσιο Πολιτικής Πιστοποιητικού Υποδομής Δημόσιου Κλειδιού και Κανονισμών Πιστοποίησης X.509 για το Διαδίκτυο), γνωστό και ως RFC 3647, της Ομάδας Δράσης για τη Διαδικτυακή Μηχανική (Internet Engineering Task Force), φορέας ο οποίος είναι υπεύθυνος για τον καθορισμό προτύπων στο Διαδίκτυο, ορίζει την Πολιτική Πιστοποιητικού ως ένα επώνυμο σύνολο κανόνων το οποίο δηλώνει την εφαρμοσιμότητα ενός πιστοποιητικού σε κάποια συγκεκριμένη κοινότητα ή/και κατηγορία εφαρμογών με παρόμοιες απαιτήσεις ασφάλειας.

Ένα πιστοποιητικό X509 έκδοση 3 μπορεί να προσδιορίζει μία συγκεκριμένη ισχύουσα πολιτική πιστοποιητικού, η οποία μπορεί να χρησιμοποιηθεί από μία οντότητα που βασίζεται στην υπηρεσία για να αποφασίσει εάν πρέπει ή όχι να εμπιστευθεί ένα πιστοποιητικό, ένα συσχετιζόμενο δημόσιο κλειδί, ή μία οποιαδήποτε ψηφιακή υπογραφή που επαληθεύεται χρησιμοποιώντας το δημόσιο κλειδί για κάποιο συγκεκριμένο σκοπό [5],[16].

Μία πολιτική πιστοποιητικού χαρακτηρίζεται μοναδικά από έναν Προσδιοριστή Αντικειμένου (Object Identifier – OID), ο οποίος μπορεί να χρησιμοποιηθεί μέσα σε ένα πιστοποιητικό ως αναφορά προς την ισχύουσα πολιτική πιστοποιητικού [16],[17],[18].

Η Δήλωση Πρακτικής περιέχει τις πράξεις των εκδοτριών ΑΠ με τις οποίες καθορίζονται οι όροι και οι προϋποθέσεις για την παροχή των υπηρεσιών πιστοποίησης που προσφέρουν. Η Δήλωση Πρακτικής συχνά αναφέρεται και ως Κανονισμός Πιστοποίησης [16],[17].

2.5. Χρονοσήμανση

Χρονοσήμανση είναι μία αλληλουχία χαρακτήρων ή στοιχεία τα οποία δηλώνουν με ασφάλεια την ημερομηνία και ώρα που έχει λάβει χώρα μία πράξη ή ενέργεια. Η Υπηρεσία Χρονοσήμανσης παρέχεται από έναν Πάροχο Υπηρεσιών Χρονοσήμανσης (ΠΥΧ), ο οποίος αποτελεί μία ΕΤΟ που ονομάζεται Αρχή Χρονοσήμανσης (Time Stamp Authority – TSA) και ικανοποιεί την απαίτηση ασφάλειας για μη αποποίηση.

Υπηρεσία Χρονοσήμανσης είναι η δημιουργία των απαραίτητων τεκμηρίων για ένα σύνολο δεδομένων σε ψηφιακή μορφή, έτσι ώστε να μπορεί να αποδειχθεί ότι τα δεδομένα αυτά υπήρχαν σε μία συγκεκριμένη χρονική στιγμή. Οι χρονοσημάνσεις παράγονται σύμφωνα με την τεχνική προδιαγραφή ETSI TS 102 023 V1.2.2 (2008-10) “Electronic Signatures and Infrastructures (ESI), Policy requirements for time-stamping authorities” και το RFC 3628 για τις απαιτήσεις που πρέπει να πληρούν οι ΠΥΧ, καθώς και σύμφωνα με την τεχνική προδιαγραφή ETSI TS 101 861 V1.4.1 (2011-07) “Electronic Signatures and Infrastructures (ESI), Time stamping profile” και το RFC 3161 για την έκδοση και τη λήψη ασφαλών χρονοσημάνσεων [19],[20],[21],[22].

2.6. Μοντέλα Εμπιστοσύνης

Οι Αρχές Πιστοποίησης δημιουργούν σχέσεις εμπιστοσύνης εκδίδοντας πιστοποιητικά σε άλλες ΑΠ. Οι σχέσεις μεταξύ των ΑΠ κατηγοριοποιούνται στην Ιεραρχική Πιστοποίηση και στην Ομότιμη ή Διμερή Δια-πιστοποίηση. Σε μία δομή ιεραρχικής πιστοποίησης υπάρχουν δύο τύποι ΑΠ: Ανώτερη ΑΠ και Υποκείμενη ΑΠ. Ανώτερη ΑΠ είναι αυτή που εκδίδει το πιστοποιητικό μίας Υποκείμενης ΑΠ. Η Δια-πιστοποίηση μπορεί να είναι μονόδρομη ή αμφίδρομη [13].

Σε μία ιεραρχική δομή μία ΑΠ δημιουργεί μία γονική σχέση ως προς μία άλλη ΑΠ. Υπάρχουν δύο είδη ιεραρχικής σχέσης, ανάλογα με το αν χρησιμοποιείται ένα πιστοποιητικό Υποκείμενης ΑΠ ή ένα μονόδρομο δια-πιστοποιητικό. Όταν μία ανώτερη ΑΠ εκδώσει ένα πιστοποιητικό υποκείμενης ΑΠ σε μία άλλη, η ΑΠ στην κορυφή της

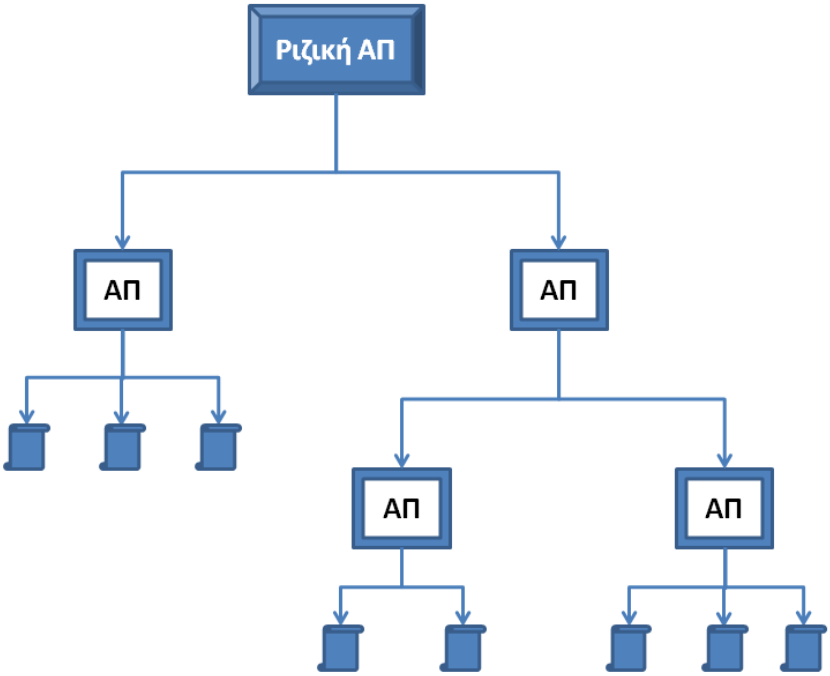
ιεραρχίας, η οποία θα πρέπει να διαθέτει ένα αυτό-υπογεγραμμένο (self-signed) πιστοποιητικό, ονομάζεται ριζική ΑΠ (root CA). Στην περίπτωση που μία ΑΠ εκδίδει μονόδρομα δια-πιστοποιητικά σε άλλες ΑΠ, τότε ονομάζεται ενωτική ΑΠ (unifying CA). Οι ενωτικές ΑΠ χρησιμοποιούν αποκλειστικά μονόδρομα δια-πιστοποιητικά [23],[24].

Σε μία ομότιμη δομή δεν υπάρχουν γονικές σχέσεις. Για τη δημιουργία ομότιμων σχέσεων χρησιμοποιούνται μόνο δια-πιστοποιητικά. Οι ομότιμες σχέσεις μπορούν να είναι είτε μονόδρομες είτε αμφίδρομες. Όταν μία ΑΠ υφίσταται αποκλειστικά και μόνο για τη διαχείριση δια-πιστοποιητικών, τότε ονομάζεται ΑΠ έμπιστος μεσολαβητής (bridge CA). Το είδος της δια-πιστοποίησης μεταξύ του έμπιστου μεσολαβητή και των ΑΠ μπορεί να είναι μονόδρομη ή αμφίδρομη [23],[24].

2.7. Αρχιτεκτονικές Υλοποίησης

Η απλούστερη αρχιτεκτονική μίας ΥΔΚ ονομάζεται Ομοπάτρια και μπορεί να σχεδιαστεί χρησιμοποιώντας μία μόνο ΑΠ, με ένα αυτό-υπογεγραμμένο πιστοποιητικό, η οποία εκδίδει πιστοποιητικά σε τελικούς χρήστες. Η διαδρομή πιστοποίησης είναι ενός βήματος. Διαδρομή πιστοποίησης (certification path) ονομάζεται μία διατεταγμένη ακολουθία, ή ένα κατευθυνόμενο μονοπάτι, πιστοποιητικών όπου το υποκείμενο του κάθε πιστοποιητικού στη διαδρομή είναι ο εκδότης του επόμενου πιστοποιητικού. Μία διαδρομή πιστοποίησης ξεκινά από το πιστοποιητικό μίας ΕΤΟ και καταλήγει στο πιστοποιητικό του τελικού χρήστη.

Σε μία δομή με περισσότερες από μία ΑΠ υπάρχουν εναλλακτικά η ιεραρχική, η μικτή και η υβριδική αρχιτεκτονική. Η ιεραρχική ΥΔΚ (Εικόνα 2) αποτελείται από μία μοναδική ριζική ΑΠ και από μία ή περισσότερες υποκείμενες ΑΠ οι οποίες εκδίδουν πιστοποιητικά στους τελικούς χρήστες. Μία ιεραρχική ΥΔΚ μπορεί να έχει ενδιάμεσες ΑΠ, οι οποίες είναι υποκείμενες ΑΠ και που οι ίδιες έχουν άλλες υποκείμενες ΑΠ.



Εικόνα 2. Ιεραρχική Αρχιτεκτονική

Η μεικτή αρχιτεκτονική αποτελείται από πολλαπλές ΑΠ με αυτό-υπογεγραμμένα πιστοποιητικά, οι οποίες εκδίδουν ψηφιακά πιστοποιητικά στις τελικές οντότητες και δια-πιστοποιητικά μεταξύ τους. Η υβριδική αρχιτεκτονική προκύπτει από το συνδυασμό του ιεραρχικού και του μεικτού μοντέλου [23].

2.8. Τομέας

Η εγκαθίδρυση σχέσεων εμπιστοσύνης μεταξύ δύο ή περισσότερων ΥΔΚ οδηγεί στη δημιουργία ενός Τομέα. Οι συγκεκριμένες σχέσεις εμπιστοσύνης υλοποιούνται τεχνικά με την έκδοση δια-πιστοποιητικών.

Τομέας ΥΔΚ ονομάζεται το σύνολο δύο ή περισσότερων ΥΔΚ, οι οποίες επέλεξαν να συνάψουν μεταξύ τους σχέσεις εμπιστοσύνης με τη χρήση δια-πιστοποιητικών. Η δημιουργία ενός Τομέα ΥΔΚ προϋποθέτει την υιοθέτηση μίας κοινής Τομεακής Πολιτικής Πιστοποιητικών που θα χαρακτηρίζεται από έναν Προσδιοριστή Αντικειμένου Πολιτικής Τομέα (OID). Κάθε ΑΠ μέλος του Τομέα ΥΔΚ θα μπορεί να εφαρμόζει τη δική της πολιτική, όμως θα πρέπει ταυτόχρονα να συμμορφώνεται και με την πολιτική πιστοποιητικών του Τομέα [23]. Οι ιδιότητες ενός Τομέα ΥΔΚ είναι οι παρακάτω:

- Ένας Τομέας ΥΔΚ μπορεί να λειτουργήσει με μία ΑΠ έμπιστος μεσολαβητής ή με μία ενωτική ΑΠ, η οποία θα ορίζει τα μέλη του Τομέα εκδίδοντας δια-πιστοποιητικά.
- Μία ΥΔΚ μπορεί ταυτόχρονα να ανήκει σε δύο ή περισσότερους Τομείς ΥΔΚ.
- Ένας Τομέας ΥΔΚ μπορεί να περιέχει ως μέλη του Τομείς ΥΔΚ.
- Δύο ή περισσότεροι Τομείς ΥΔΚ μπορούν να συνάψουν μεταξύ τους σχέσεις εμπιστοσύνης δημιουργώντας ένα νέο Τομέα. Μπορούν να επιλέξουν να διατηρήσουν τους υφιστάμενους Τομείς ΥΔΚ μαζί με το νέο Τομέα ή να ενσωματώσουν τους υφιστάμενους Τομείς στον καινούργιο.
- Ένα μέλος ενός Τομέα ΥΔΚ μπορεί να επιλέξει ότι θα συμμετέχει στον Τομέα αλλά να περιορίσει ή να αποκλείσει την εμπιστοσύνη σε ένα ή περισσότερα άλλα μέλη του συγκεκριμένου Τομέα.

Όταν δύο ή περισσότεροι Τομείς ΥΔΚ αποφασίσουν να συνάψουν μεταξύ τους σχέσεις εμπιστοσύνης, τότε δημιουργείται ένας μεγαλύτερος Τομέας εγκαθιδρύοντας μία νέα ΑΠ ως έμπιστο μεσολαβητή, ή μία ενωτική ΑΠ, ή εκδίδοντας δια-πιστοποιητικά μεταξύ των ριζικών ΑΠ.

2.9. Λίστα Εμπιστοσύνης

Η εγκαθίδρυση σχέσεων εμπιστοσύνης μπορεί να επιτευχθεί και χωρίς την εμπλοκή των ίδιων των ΥΔΚ, από εξωτερικές οντότητες που ορίζουν τοπικά μία Λίστα Εμπιστοσύνης (Trust List).

Λίστα Εμπιστοσύνης ονομάζεται το σύνολο που αποτελείται από μία ή περισσότερες ριζικές ΑΠ, το οποίο χρησιμοποιείται από έναν χρήστη για να εμπιστευθεί μία ή περισσότερες ΥΔΚ. Οι Λίστες Εμπιστοσύνης συχνά δημιουργούνται χωρίς την ενημέρωση των ΥΔΚ οι οποίες περιλαμβάνονται σε αυτές [23].

Εφόσον μία Λίστα δημιουργηθεί, εγκατασταθεί και συντηρείται από έναν χρήστη πιστοποιητικών για προσωπική χρήση, ονομάζεται Τοπική Λίστα Εμπιστοσύνης και αποτελεί την απλούστερη μέθοδο για την αποδοχή και εμπιστοσύνη πιστοποιητικών τελικών οντοτήτων.

Εναλλακτικά, μία λίστα μπορεί να δημιουργηθεί και να ενημερώνεται για λογαριασμό πολλών τελικών χρηστών. Στην περίπτωση αυτή, η οντότητα που διαχειρίζεται τη λίστα ονομάζεται Αρχή Εμπιστοσύνης (Trust Authority). Μία Αρχή Εμπιστοσύνης μπορεί να λειτουργεί στο πλαίσιο μίας ΥΔΚ, από μία ομάδα χρηστών, από έναν οργανισμό για τα μέλη του ή και από έναν τρίτο ανεξάρτητο φορέα.

3. ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΑΝΑΛΥΣΗ

Στόχος της παρούσας ενότητας είναι, μέσα από την κριτική ανασκόπηση της επιστημονικής βιβλιογραφίας και από τη διεθνή εμπειρία στην υλοποίηση έργων ΥΔΚ ευρείας κλίμακας, να προσδιορισθούν οι κρίσιμοι παράγοντες επιτυχίας για την ανάπτυξη και λειτουργία μίας ΥΔΚ.

3.1. Ανάλυση SWOT

Η ανάλυση SWOT (Strengths, Weaknesses, Opportunities, Threats) αποτελεί ένα πολύτιμο εργαλείο αξιολόγησης και λήψης αποφάσεων. Το ερώτημα που τίθεται στη συγκεκριμένη περίπτωση είναι εάν η ανάπτυξη μίας ΥΔΚ είναι προς το συμφέρον ενός οργανισμού ή εάν κρύβει κινδύνους και επιφέρει περιττά έξοδα.

Η ανάλυση SWOT είναι ένα αποδοτικό εργαλείο προσδιορισμού των πλεονεκτημάτων, των αδυναμιών, των ευκαιριών και των απειλών που επιφέρει η λήψη μιας απόφασης για την εκτέλεση μιας ενέργειας. Επιτρέπει την αξιολόγηση μιας νέας προοπτικής, με έναν απλό και αποτελεσματικό τρόπο, καταγράφοντας όλα τα θετικά και αρνητικά σημεία που σχετίζονται με την υιοθέτησή της. Αποτυπώνοντας με αντικειμενικότητα και πληρότητα όλα τα επιχειρήματα που αφορούν μία προτεινόμενη δράση, προκύπτουν τα συμπεράσματα εκείνα που θα οδηγήσουν στη λήψη της ορθής απόφασης ή στην ανάδειξη της ανάγκης για περαιτέρω εμπεριστατωμένες αναλύσεις.

Στην Εικόνα 3 εμφανίζονται συνοπτικά τα πλεονεκτήματα, τα μειονεκτήματα, οι ευκαιρίες και οι απειλές που χαρακτηρίζουν την ανάπτυξη και λειτουργία μίας ΥΔΚ.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	**ΑΔΥΝΑΜΙΕΣ**
Αυθεντικοποίηση Έλεγχος Πρόσβασης Διαχείριση Πιστοποιητικών Ψηφιακές Υπογραφές Χρονοσήμανση Ασφαλές Ηλεκτρονικό Ταχυδρομείο Κρυπτογράφηση Δεδομένων Ηλεκτρονική Διακίνηση Εγγράφων	Κόστος Πολυπλοκότητα Υπηρεσίες Καταλόγου Έλλειψη Εκπαίδευσης Πιστοποίηση
ΕΥΚΑΙΡΙΕΣ	**ΑΠΕΙΛΕΣ**
Εδραίωση Εμπιστοσύνης Εξατομικευμένες Ηλεκτρονικές Υπηρεσίες Απλούστευση Επιχειρησιακών Διαδικασιών Προστασία της Ιδιωτικότητας Συμμόρφωση με Διεθνή Πρότυπα	Θεσμικό Πλαίσιο Μη Βιώσιμο Επιχειρησιακό Μοντέλο Διαλειτουργικότητα PKI Συστημάτων Απόδοση και Κλιμάκωση Διαχείριση

Εικόνα 3. Ανάλυση SWOT

Στη συνέχεια εξετάζονται και τεκμηριώνονται αναλυτικά τα πλεονεκτήματα, τα μειονεκτήματα, οι ευκαιρίες και οι απειλές που χαρακτηρίζουν την ανάπτυξη μίας ΥΔΚ.

Πλεονεκτήματα

Η ΥΔΚ δημιουργεί ένα ολοκληρωμένο πλαίσιο λειτουργίας ηλεκτρονικών συναλλαγών για την παροχή υπηρεσιών ασφάλειας όπως: αυθεντικοποίηση αποστολέα και παραλήπτη, έλεγχο πρόσβασης, ακεραιότητα δεδομένων, μη αποποίηση ευθύνης και ασφαλή διαδικτυακή μεταφορά δεδομένων. Επίσης, προσφέρει τους απαραίτητους μηχανισμούς ασφάλειας για την υποστήριξη διάφορων επιχειρησιακών διαδικασιών και υπηρεσιών όπως: ψηφιακή υπογραφή, χρονοσήμανση, κρυπτογράφηση, διαχείριση πιστοποιητικών, μοναδιαία αυθεντικοποίηση (single-sign-on), εξουσιοδότηση και ασφαλές ηλεκτρονικό ταχυδρομείο [25],[26]. Ουσιαστικά, παρά τις προσπάθειες της επιστημονικής κοινότητας τα τελευταία χρόνια, δεν έχει προταθεί μία πειστική και ολοκληρωμένη εναλλακτική λύση στις ΥΔΚ [7].

Αδυναμίες

Κύριο εμπόδιο στη δημιουργία μίας ΥΔΚ είναι η αντικειμενική δυσκολία προσδιορισμού του κόστους υλοποίησης και υποστήριξης. Το Συνολικό Κόστος Ιδιοκτησίας (Total Cost of Ownership – TCO) εξαρτάται από μία πληθώρα παραμέτρων όπως για παράδειγμα το είδος του λογισμικού και του εξοπλισμού, το βαθμό διαθεσιμότητας του συστήματος, την ανάγκη διαλειτουργικότητας με άλλα υφιστάμενα πληροφοριακά συστήματα, το κόστος εκπαίδευσης του προσωπικού, καθώς και το επιθυμητό παρεχόμενο επίπεδο τεχνικής υποστήριξης.

Η πολυπλοκότητα της τεχνικής υλοποίησης και της επιχειρησιακής λειτουργίας μίας ΥΔΚ είναι αποθαρρυντικοί παράγοντες για την υιοθέτηση ανάλογων συστημάτων. Επίσης ο βαθμός εξοικείωσης του μεγαλύτερου ποσοστού των χρηστών διαδικτυακών εφαρμογών στη διαχείριση ψηφιακών πιστοποιητικών είναι ακόμη πολύ χαμηλός [27].

Η λειτουργία μίας ΥΔΚ στηρίζεται στη δημιουργία ενός καταλόγου χρηστών, των οποίων τα ψηφιακά πιστοποιητικά θα βρίσκονται αποθηκευμένα μέσα σε ένα κεντρικό αποθετήριο. Οι χρήστες θα πρέπει να έχουν τη δυνατότητα εγγραφής μέσω του διαδικτύου στον κατάλογο και να αιτούνται την έκδοση ψηφιακών πιστοποιητικών. Θα πρέπει επίσης, να υπάρχει μία διαδικασία ταυτοποίησης και ένας μηχανισμός έγκρισης των αιτημάτων, πριν από την τελική έκδοση και διάθεση των πιστοποιητικών μέσα από ένα κεντρικό ευρετήριο. Η σχεδίαση και η ανάπτυξη μιας τέτοιας υπηρεσίας καταλόγου αποτελεί μία σημαντική δυσκολία στην υλοποίηση ΥΔΚ μεγάλης κλίμακας [26],[28].

Η εκπαίδευση των διαχειριστών, του προσωπικού εργασίας, αλλά και των τελικών χρηστών της ΥΔΚ είναι ένα ακόμη ζήτημα που θα πρέπει να απασχολήσει σοβαρά τον οργανισμό που θα αναλάβει την ευθύνη ανάπτυξης, λειτουργίας και υποστήριξης όλων των συστημάτων της υποδομής.

Ένας οργανισμός για να μπορέσει να λειτουργήσει ως Πάροχος Υπηρεσιών Ταυτοποίησης και να εκδίδει αναγνωρισμένα ψηφιακά πιστοποιητικά για χρήση προηγμένης ηλεκτρονικής υπογραφής και επιβεβαίωσης της ταυτότητας του χρήστη, θα πρέπει να έχει πιστοποιηθεί και να συμμορφώνεται με μια σειρά από αυστηρές νομοθετικές διατάξεις και διεθνή ελεγκτικά πρότυπα.

Ευκαιρίες

Η ανάπτυξη μίας ΥΔΚ αποτελεί μία εξαιρετική ευκαιρία για την εδραίωση εμπιστοσύνης μεταξύ των χρηστών της υποδομής. Η εμπιστοσύνη λειτουργεί ενθαρρυντικά για την επιτυχημένη και ομαλή παροχή ποιοτικών ηλεκτρονικών υπηρεσιών και την ασφαλή διεκπεραίωση διαδικτυακών συναλλαγών.

Επίσης, η χρήση ψηφιακών πιστοποιητικών δημιουργεί τις κατάλληλες προϋποθέσεις για τη σχεδίαση εξατομικευμένων προηγμένων ποιοτικών ηλεκτρονικών υπηρεσιών προστιθέμενης αξίας αυξάνοντας το βαθμό ικανοποίησης των τελικών χρηστών.

Η ΥΔΚ θέτει τα θεμέλια και παρέχει το κατάλληλο πλαίσιο για την απλούστευση των παραδοσιακών επιχειρησιακών διαδικασιών, διότι καθιστά εφικτή την ηλεκτρονική έκδοση και διακίνηση των εγγράφων, επιτρέποντας την αντικατάσταση της ιδιόχειρης υπογραφής και των χρονοβόρων μηχανισμών επικύρωσης της γνησιότητας με αυτοματοποιημένες αποτελεσματικές και αποδοτικές ψηφιακές διαδικασίες.

Μία ΥΔΚ παρέχει τις υπηρεσίες και τους μηχανισμούς ασφάλειας που απαιτούνται για την αποτελεσματική προστασία της ιδιωτικότητας των δεδομένων σε ένα διαδικτυακό περιβάλλον και επιτρέπει την ανταλλαγή της ευαίσθητης πληροφορίας με ασφάλεια.

Ο οργανισμός που υλοποιεί μία ΥΔΚ αποκτά τεχνογνωσία, οργάνωση, κανονισμούς λειτουργίας, πολιτικές ασφάλειας και διαδικασίες που του δίνουν το πλεονέκτημα και τη δυνατότητα ευκολότερης συμμόρφωσης και πιστοποίησης σύμφωνα με τα διεθνή ελεγκτικά πρότυπα.

Απειλές

Η αποτελεσματική λειτουργία μίας ΥΔΚ απειλείται από την έλλειψη του κατάλληλου θεσμικού και νομοθετικού πλαισίου το οποίο αποτελεί αναγκαία προϋπόθεση για την έκδοση αναγνωρισμένων ψηφιακών πιστοποιητικών και για την εφαρμογή της προηγμένης ηλεκτρονικής υπογραφής.

Η ΥΔΚ αποτελεί μία ολοκληρωμένη τεχνολογική πλατφόρμα πάνω στην οποία μπορούν να σχεδιασθούν διαδικτυακές εφαρμογές και να αναπτυχθούν ποιοτικές ηλεκτρονικές υπηρεσίες. Είναι πολύ σημαντικό να υπάρχει ένα βιώσιμο επιχειρησιακό μοντέλο προσανατολισμένο στην εξυπηρέτηση των τελικών χρηστών και στην παροχή αξιόλογου και χρήσιμου περιεχομένου που να ανταποκρίνεται στις πραγματικές τους ανάγκες. Χωρίς την παροχή υπηρεσιών προστιθέμενης αξίας που να αναβαθμίζουν το επίπεδο διαβίωσης των χρηστών του συστήματος, η ΥΔΚ κινδυνεύει να απαξιωθεί από τους ίδιους τους κατόχους των πιστοποιητικών.

Σημαντικό πρόβλημα αποτελεί η έλλειψη διαλειτουργικότητας μεταξύ διαφορετικών συστημάτων ΥΔΚ. Μολονότι, ο κάθε κατασκευαστής συμμορφώνεται με τα τεχνικά RFC έγγραφα σχετικά με το PKIX, σχεδιάζει και υλοποιεί με το δικό του τρόπο το σύστημα που παρέχει την υπηρεσία καταλόγου και την αρχή πιστοποίησης, προσπαθώντας να δεσμεύσει τον πελάτη μέσα σε μια κλειστή αρχιτεκτονική. Συνεπώς, η συμβατότητα μεταξύ ΥΔΚ διαφορετικών κατασκευαστών αποδεικνύεται περιορισμένη, δημιουργώντας σημαντικά προβλήματα διαλειτουργικότητας στην περίπτωση που προκύψει η ανάγκη συνεργασίας ή ενοποίησης ανάλογων συστημάτων.

Στην περίπτωση υλοποίησης μίας ΥΔΚ ευρείας κλίμακας με μεγάλο αριθμό χρηστών και διαφορετικά προφίλ ψηφιακών πιστοποιητικών, δημιουργούνται σοβαρά θέματα απόδοσης της υπηρεσίας καταλόγου και επεκτασιμότητας των συστημάτων που υλοποιούν τις αρχές πιστοποίησης. Θα πρέπει να δίνεται μεγάλη προσοχή στην αρχική σχεδίαση και διαστασιολόγηση της ΥΔΚ προβλέποντας με σχετική ακρίβεια τον αριθμό και τις απαιτήσεις των χρηστών.

Το δυσκολότερο πρόβλημα στη λειτουργία μίας ΥΔΚ ευρείας κλίμακας είναι η διαχείριση του κύκλου ζωής των ψηφιακών πιστοποιητικών, ειδικά στην περίπτωση ενός ΠΥΠ ο οποίος πρέπει να συμμορφώνεται με αυστηρούς κανονισμούς, διαδικασίες και πρότυπα ασφάλειας.

Η γενικότερη διαπίστωση που προκύπτει από την κριτική βιβλιογραφική ανασκόπηση είναι ότι τα πλεονεκτήματα, οι δυνατότητες και οι προοπτικές που προσφέρει η ΥΔΚ υπερτερούν των προβλημάτων, των αδυναμιών και των απειλών. Άλλωστε, δεν φαίνεται να υπάρχει κάποια καλύτερη εναλλακτική λύση που να καλύπτει σε ικανοποιητικό βαθμό το σύνολο των απαιτήσεων ασφάλειας που παρέχει μία ΥΔΚ [7].

3.2. Ηλεκτρονική Διακυβέρνηση

Η Ηλεκτρονική Διακυβέρνηση αποτελεί ένα χαρακτηριστικό επιχειρησιακό πεδίο εφαρμογής των ΥΔΚ ευρείας κλίμακας για την παροχή ηλεκτρονικών υπηρεσιών σε πολίτες, επιχειρήσεις και κυβερνητικούς οργανισμούς. Επίσης, αποτελεί μία ιδανική περίπτωση μελέτης διότι τα συστήματα ηλεκτρονικής διακυβέρνησης παρουσιάζουν μεγάλο βαθμό πολυπλοκότητας, σύνθετα προβλήματα διαλειτουργικότητας, καθώς και υψηλές απαιτήσεις ασφάλειας και ιδιωτικότητας.

Σε μία επιστημονική δημοσίευση το 2003 αποδείχθηκε ότι οι υπηρεσίες ασφάλειας που παρέχονται από μία ΥΔΚ μπορούν να ικανοποιήσουν τις περισσότερες από τις απαιτήσεις ασφάλειας ενός ολοκληρωμένου πληροφοριακού συστήματος ηλεκτρονικής διακυβέρνησης [29].

Αναλυτικότερα, οι επιστήμονες απέδειξαν το γεγονός ότι η ΥΔΚ μπορεί να αποτελέσει το θεμέλιο λίθο για να υλοποιηθεί το κατάλληλο επίπεδο ασφάλειας που απαιτείται από μία κυβερνητική διαδικτυακή πύλη για την παροχή υπηρεσιών μίας στάσης. Οι απαιτήσεις που ενδέχεται να επιβάλουν την ανάγκη λήψης πρόσθετων μέτρων ασφάλειας σχετίζονται είτε με θέματα απόδοσης/ διαθεσιμότητας του εξοπλισμού και αξιοπιστίας του λογισμικού, είτε με ιδιαίτερα εξειδικευμένες προδιαγραφές εφαρμογών για την παροχή ανωνυμίας και την προστασία από καταναγκασμό [29].

Οι βασικές απαιτήσεις ασφάλειας των ηλεκτρονικών συναλλαγών, οι οποίες παρουσιάζονται στον Πίνακα 1, μπορούν να ικανοποιηθούν με τις υπηρεσίες μίας ΥΔΚ. Εξατομικευμένες υπηρεσίες, οι οποίες χαρακτηρίζονται από υψηλό βαθμό ολοκλήρωσης, παρέχονται αποτελεσματικά και αποδοτικά με τη χρήση ψηφιακών πιστοποιητικών υπογραφής και κρυπτογράφησης. Η κατανόηση των προδιαγραφών, με τις οποίες θα πρέπει να συμμορφώνονται οι παρεχόμενες ηλεκτρονικές υπηρεσίες, είναι ιδιαίτερα σημαντική για τη σχεδίαση των κατάλληλων λύσεων και μηχανισμών προστασίας της πληροφορίας.

Πίνακας 1. Απαιτήσεις Ασφάλειας

ΑΠΑΙΤΗΣΕΙΣ	ΥΔΚ
Εγκυρότητα = Αυθεντικότητα + Ακεραιότητα	Ψηφιακές υπογραφές
Εμπιστευτικότητα	Κρυπτογράφηση
Μη αποποίηση ευθύνης	Ψηφιακές υπογραφές & Χρονοσήμανση & πιστοποιητικά σκληρής αποθήκευσης
Εξουσιοδότηση	Εγγραφή, διαχείριση πιστοποιητικών, υπηρεσίες καταλόγου

Η ανάπτυξη μίας ΥΔΚ σε εθνική κλίμακα για την παροχή ποιοτικών ηλεκτρονικών υπηρεσιών, με γνώμονα την προστασία της πληροφορίας και της ιδιωτικότητας των χρηστών, απαιτεί στοχευόμενες παρεμβάσεις και πρωτοβουλίες σε διοικητικό, θεσμικό, οργανωτικό και τεχνικό επίπεδο.

Η Ευρωπαϊκή Ένωση, την τελευταία δεκαετία, στο πλαίσιο της προσπάθειας ενίσχυσης της ανάπτυξης, της ανταγωνιστικότητας και της συνεργασίας μεταξύ των κρατών μελών, δίνει μεγάλη έμφαση στην παροχή διαδικτυακών υπηρεσιών με ασφάλεια σε πολίτες και επιχειρήσεις. Η επιτυχία της όλης προσπάθειας στηρίζεται στην υιοθέτηση μηχανισμών αυθεντικοποίησης, εμπιστευτικότητας, ακεραιότητας και μη αποποίησης της ευθύνης, επιτρέποντας την ανταλλαγή πληροφοριών, τη διακίνηση ψηφιακών εγγράφων και τη διεκπεραίωση ηλεκτρονικών συναλλαγών με ασφάλεια.

Η οδηγία 1999/93/ΕΚ «σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές» του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, θεσπίζει το νομικό πλαίσιο για τις ηλεκτρονικές υπογραφές και ορισμένες υπηρεσίες πιστοποίησης, ώστε να εξασφαλίσει την ομαλή λειτουργία της εσωτερικής αγοράς. Έχει ως στόχο να διευκολύνει τη χρήση ηλεκτρονικών υπογραφών και να συμβάλει στη νομική αναγνώρισή τους [30].

Η ανάπτυξη και λειτουργία μίας ΥΔΚ αποτελεί ένα δύσκολο έργο το οποίο απαιτεί προσεκτική σχεδίαση και υψηλό επίπεδο τεχνογνωσίας. Το πρότυπο X.509 είναι αρκετά σύνθετο και η διαχείριση ολόκληρου του κύκλου ζωής των ψηφιακών πιστοποιητικών αποδεικνύεται στην πράξη μία ιδιαίτερα πολύπλοκη διαδικασία. Ο μεγάλος βαθμός ελευθερίας που υπάρχει στον καθορισμό του προφίλ ενός πιστοποιητικού X.509 v3 οδηγεί σε προβλήματα διαλειτουργικότητας μεταξύ των διαφορετικών υλοποιήσεων, τα οποία περιορίζουν τη δημιουργία ΥΔΚ ευρείας κλίμακας.

Επιπλέον, η δυνατότητα δια-πιστοποίησης είναι εξαιρετικά δύσκολο να εφαρμοστεί στην πράξη διότι οι αντίστοιχες πολιτικές πιστοποιητικών και δηλώσεις πρακτικής θα πρέπει να είναι συγκρίσιμες. Οι ΠΥΠ συνήθως ισχυρίζονται ότι υπηρεσίες πιστοποίησης που παρέχουν είναι ανώτερες από εκείνες των ανταγωνιστών και συνεπώς, δεν μπορούν να αποδεχθούν τη δια-πιστοποίηση. Ιδιαίτερα στην περίπτωση αναγνώρισης πιστοποιητικών μεταξύ διαφορετικών χωρών, μία συμφωνία δια-πιστοποίησης είναι εξαιρετικά απίθανο να επιτευχθεί [31],[32],[33].

Σημαντική πρόκληση στη λειτουργία μίας ΥΔΚ είναι αναμφίβολα η διαχείριση των πιστοποιητικών. Ζητήματα όπως η εγγραφή, η ταυτοποίηση, η έκδοση, η πιστοποίηση, η ανάκληση και η ανανέωση του ζεύγους κλειδιών αποτελούν πολύπλοκες διαδικασίες που δυσχεραίνουν το έργο μίας ΥΔΚ. Χρειάζεται προσεκτική ανάλυση και σχεδίαση της αρχιτεκτονικής δομής που θα υλοποιηθεί με στόχο την ευελιξία, την επεκτασιμότητα και τη διαλειτουργικότητα της όλης υποδομής [32],[33].

Γενικότερα, η έλλειψη αξιόλογων και καινοτόμων διαδικτυακών εφαρμογών που να αξιοποιούν τα ψηφιακά πιστοποιητικών έχει περιορίσει σημαντικά την υιοθέτησή τους από το μεγαλύτερο ποσοστό του πληθυσμού.

3.3. Κρίσιμοι Παράγοντες Επιτυχίας

Η ΥΔΚ αναμφίβολα προσφέρει σημαντικά οφέλη και πλεονεκτήματα, διότι αποτελεί ένα ισχυρό οικοδόμημα για την αποτελεσματική παροχή των υπηρεσιών ασφάλειας: αυθεντικότητα και ακεραιότητα με τη χρήση ψηφιακών υπογραφών, εμπιστευτικότητα με τη χρήση κρυπτογράφησης, καθώς και μη αποποίηση της ευθύνης με τη χρήση Ασφαλής Διάταξης Δημιουργίας Υπογραφής (Secure Signature Creation Device – SSCD), όπως είναι για παράδειγμα οι έξυπνες κάρτες και τα usb tokens.

Ένα ερώτημα που προκύπτει εντελώς αυθόρμητα είναι το πως μία τεχνολογία της δεκαετίας του 80', η οποία είναι εμπορικά διαθέσιμη ήδη από τη δεκαετία του 90', δεν έχει καταφέρει έως σήμερα να εδραιωθεί και να ανταποκριθεί στις αναμενόμενες υψηλές προσδοκίες.

Προφανώς, η μειωμένη αποδοχή των ΥΔΚ δεν οφείλεται σε ένα και μόνο λόγο, αλλά στο συνδυασμό περισσότερων αιτιών, όπως για παράδειγμα το υψηλό κόστος υλοποίησης, η πολυπλοκότητα της τεχνολογίας, η ελλιπή κατανόηση των επιχειρησιακών και λειτουργικών απαιτήσεων, καθώς και η έλλειψη καλά σχεδιασμένων εφαρμογών λογισμικού φιλικών προς τον τελικό χρήστη. Όλες αυτές είναι μερικές από τις αιτίες που συμβάλουν στην αποτυχία των ΥΔΚ.

Η ιστορική εξέλιξη των ΥΔΚ αποκαλύπτει ότι η προστιθέμενη αξία δεν βρίσκεται στο ίδιο το ψηφιακό πιστοποιητικό αλλά στις υπηρεσίες που μπορούν να το αξιοποιήσουν. Εδώ και πολλά χρόνια οι κύριες υπηρεσίες που υποστηρίζουν τη χρήση πιστοποιητικών είναι η αυθεντικοποίηση στο διαδίκτυο και το ασφαλές ηλεκτρονικό ταχυδρομείο. Η έλλειψη αξιόλογων, χρήσιμων και ουσιαστικών εφαρμογών, καθώς και τα προβλήματα διαλειτουργικότητας μεταξύ διαφορετικών υλοποιήσεων ΥΔΚ δεν επέτρεψαν στην τεχνολογία αυτή να έχει την αναμενόμενη επιτυχία. Επίσης, η δυσκολία προσδιορισμού και εφαρμογής ενός αποδοτικού και ευέλικτου μοντέλου χρέωσης των συνδρομητών ενός ΠΥΠ, που να αντισταθμίζει το υψηλό κόστος ανάπτυξης και λειτουργίας μίας ΥΔΚ, αποτέλεσε ένα επιπλέον εμπόδιο στην αποδοχή και διάδοσή των ΥΔΚ [33],[34].

Τα τελευταία χρόνια η ολοένα και εντονότερη ανάγκη για ισχυρή αυθεντικοποίηση των χρηστών στο διαδίκτυο, καθώς και η θέσπιση νομοθετικών πλαισίων σε Αμερική και Ευρώπη για την αναγνώριση των ψηφιακών υπογραφών και την ηλεκτρονική διακίνηση των εγγράφων, δίνουν νέα ώθηση στις ΥΔΚ. Το κλειδί της επιτυχίας είναι να δοθεί έμφαση στην ικανοποίηση του τελικού χρήστη και στην παροχή καινοτόμων και ποιοτικών υπηρεσιών προστιθέμενης αξίας. Μία ΥΔΚ αποτελεί τα θεμέλια της ασφάλειας της πληροφορίας και κατά συνέπεια, οι εφαρμογές λογισμικού θα πρέπει να είναι σχεδιασμένες ούτως ώστε να την αξιοποιούν και να την υποστηρίζουν [34],[35].

Πολλά από τα εμπόδια που παρουσιάστηκαν κατά το παρελθόν στην ανάπτυξη ΥΔΚ οφείλονται κυρίως στην προσπάθεια δημιουργίας πληροφοριακών συστημάτων αυθεντικοποίησης ευρείας κλίμακας, θεωρώντας εσφαλμένα ότι θα ήταν εφικτή η εκτέλεση επιχειρηματικών ηλεκτρονικών συναλλαγών μεταξύ χρηστών οι οποίοι ήταν εντελώς άγνωστοι μεταξύ τους.

Η ορθή αντίληψη αναφορικά με μία ΥΔΚ στηρίζεται στη διεξαγωγή ηλεκτρονικών συναλλαγών, μέσα σε ένα κοινά αποδεκτό θεσμικό και επιχειρησιακό πλαίσιο, μεταξύ χρηστών οι οποίοι βρίσκονται σε μία καθορισμένη υφιστάμενη σχέση και προσδιορίζονται από συγκεκριμένα χαρακτηριστικά. Σε παρόμοιες περιπτώσεις οι χρήστες μπορεί να μη γνωρίζονται προσωπικά μεταξύ τους, όμως αποδέχονται τις αναγνωρισμένες ιδιότητές τους. Επίσης, για λόγους ασφάλειας και προστασίας της ιδιωτικότητας του ατόμου, είναι προτιμότερη η χρήση πολλαπλών ανεξάρτητων ψηφιακών πιστοποιητικών ανά πεδίο εφαρμογής από την υιοθέτηση ενός μοναδικού πιστοποιητικού ανά χρήστη.

Από την έως τώρα ανάλυση προκύπτει το συμπέρασμα ότι οι κρίσιμοι παράγοντες επιτυχίας μίας ΥΔΚ είναι η δέσμευση της ηγεσίας, το ισχυρό νομικό πλαίσιο, η επίγνωση των χρηστών, το επιχειρησιακό μοντέλο, η οργανωτική δομή, η τεχνική υλοποίηση, καθώς και το υψηλό επίπεδο τεχνογνωσίας και ειδίκευσης των εμπειρογνωμόνων οι οποίοι θα κληθούν να αναπτύξουν την υποδομή. Οι κρίσιμοι παράγοντες επιτυχίας μίας ΥΔΚ παρουσιάζονται στο διάγραμμα της Εικόνας 4.

Εικόνα 4. Κρίσιμοι Παράγοντες Επιτυχίας ΥΔΚ

Η ανάπτυξη και λειτουργία μίας ΥΔΚ αρχικά απαιτεί τη δέσμευση της ηγεσίας του οργανισμού που θα αναλάβει την ευθύνη υλοποίησης, διότι χαρακτηρίζεται από ένα σημαντικά υψηλό Συνολικό Κόστος Ιδιοκτησίας (Total Cost of Ownership – TCO). Συγκεκριμένα, χρειάζεται η έγκριση ενός αρχικού κεφαλαίου επένδυσης για την προμήθεια όλων των αναγκαίων πληροφοριακών συστημάτων, την κατάλληλη διαμόρφωση του κέντρου δεδομένων που θα τα φιλοξενήσει, την εγκατάστασή τους σε διάταξη υψηλής εφεδρείας, την εφαρμογή των απαραίτητων αντιμέτρων ασφάλειας, καθώς και τη διατήρηση των απαραίτητων εγκαταστάσεων επιχειρησιακής συνέχειας που θα πρέπει να διαθέτει ο ΠΥΠ σε περίπτωση μη διαθεσιμότητας της κύριας υποδομής. Επίσης, θα πρέπει να ληφθεί υπόψη το λειτουργικό κόστος για την αναβάθμιση, υποστήριξη και συντήρηση της ΥΔΚ.

Η ανάπτυξη μίας ΥΔΚ αποτελεί μία στρατηγική επιλογή η οποία συνεπάγεται μία μακροπρόθεσμη επένδυση που δεσμεύει μελλοντικά τον οργανισμό. Συνεπώς, χρειάζεται η εκπόνηση ενός επιχειρησιακού σχεδίου, η προσεκτική αξιολόγηση των απαιτήσεων και η έμπρακτη στήριξη από την ηγεσία για να μπορέσει να επιφέρει τα αναμενόμενα και επιθυμητά αποτελέσματα.

Ένα ισχυρό θεσμικό πλαίσιο παίζει καθοριστικό ρόλο στην ευρεία αποδοχή και διάδοση των υπηρεσιών που μπορεί να προσφέρει ένας ΠΥΠ. Κρίσιμα νομικά θέματα αναφορικά με τους όρους, τα κριτήρια και τους κανονισμούς λειτουργίας μίας ΥΔΚ, όπως είναι για παράδειγμα η υποχρέωση εθελοντικής διαπίστευσης του παρόχου, η δυνατότητα έκδοσης αναγνωρισμένων πιστοποιητικών, η νομιμότητα της προηγμένης ηλεκτρονικής (ψηφιακής) υπογραφής, τα είδη των πιστοποιητικών και των ΑΔΔΥ (Ασφαλή Διάταξη Δημιουργίας Υπογραφής), οι φορείς εποπτείας και ελέγχου των ΠΥΠ, οι απαραίτητες πιστοποιήσεις, οι υποχρεώσεις συμμόρφωσης με τα διεθνή ελεγκτικά πρότυπα, η δια-πιστοποίηση με άλλους ΠΥΠ, το περιεχόμενο της πολιτικής πιστοποιητικών και η δήλωση πρακτικής, ρυθμίζονται από τις σχετικές διεθνείς οδηγίες και το εθνικό δίκαιο.

Ο κρισιμότερος παράγοντας επιτυχίας μίας ΥΔΚ είναι η ποιότητα και το περιεχόμενο των υπηρεσιών που παρέχονται και υποστηρίζονται από την υποδομή. Η ανάπτυξη της ΥΔΚ πρέπει να είναι βαθιά συνυφασμένη με ένα βιώσιμο επιχειρησιακό μοντέλο που να βασίζεται σε καινοτόμες εφαρμογές και στην παροχή προηγμένων ηλεκτρονικών υπηρεσιών προστιθέμενης αξίας.

Ο τελικός χρήστης θα πρέπει εύκολα να μπορεί να αντιλαμβάνεται τα οφέλη και τα πλεονεκτήματα, όπως το επίπεδο ασφάλειας και προστασίας της ιδιωτικότητας, που του εξασφαλίζουν τα ψηφιακά πιστοποιητικά στη διεξαγωγή ηλεκτρονικών συναλλαγών, ούτως ώστε να επιλέγει συνειδητά εφαρμογές και να χρησιμοποιεί υπηρεσίες που τα αξιοποιούν και τα υποστηρίζουν.

Η επίγνωση των θεμάτων ασφάλειας της πληροφορίας είναι απαραίτητη προϋπόθεση για τη δημιουργία κλίματος θετικής προδιάθεσης μεταξύ των χρηστών, ως προς την επιλογή υπηρεσιών και διαδικασιών που βασίζονται πάνω σε ΥΔΚ. Η διαχείριση των πιστοποιητικών στα διάφορα λειτουργικά συστήματα των υπολογιστών και η χρήση τους στις εφαρμογές λογισμικού απαιτεί την απόκτηση εξειδικευμένων γνώσεων και δεξιοτήτων, καθώς και την εξοικείωση με τη χρήση των ΑΔΔΥ. Η επιμόρφωση των τελικών χρηστών και η εκπαίδευσή τους στη διαχείριση και λειτουργία των πιστοποιητικών μπορεί να συμβάλει αποφασιστικά στην ευρεία αποδοχή και χρήση των υπηρεσιών που παρέχουν οι ΥΔΚ.

Η οργανωτική δομή μίας ΥΔΚ έχει τεράστια σημασία για τη λειτουργία και υποστήριξη των συστημάτων. Η ανάπτυξη της ΥΔΚ στηρίζεται στην ορθή σχεδίαση της αρχιτεκτονικής διάταξης, την προσεκτική διαστασιολόγηση και στον ορισμό του κατάλληλου οργανωτικού σχήματος με στόχο την αποτελεσματική και αποδοτική διαχείριση της υποδομής. Η επιτυχία είναι συνάρτηση του βαθμού εμπιστοσύνης που θα εδραιωθεί μεταξύ των οντοτήτων που συμμετέχουν στην ΥΔΚ.

Επιβάλλεται η δημιουργία του κατάλληλου οργανωτικού σχήματος και η λεπτομερή αποτύπωση των επιχειρησιακών διαδικασιών που θα καθορίζουν τη λειτουργία της ΥΔΚ. Θα πρέπει να διαθέτει όλες τις απαραίτητες πιστοποιήσεις, να συμμορφώνεται με τα διεθνή ελεγκτικά πρότυπα και κανονισμούς και να εφαρμόζει αυστηρές πολιτικές και αντίμετρα ασφάλειας.

Το αρχιτεκτονικό μοντέλο που επιλέγεται συνήθως είναι το ιεραρχικό με την υλοποίηση μίας ριζικής ΑΠ, ορισμένων υποκείμενων ΑΠ και ενός ικανού αριθμού ΑΕ για την εξυπηρέτηση όλων των τελικών χρηστών. Η διαλειτουργικότητα μεταξύ υφιστάμενων ΠΥΠ, με σκοπό τη δημιουργία μίας ΥΔΚ ευρείας κλίμακας, μπορεί να επιτευχθεί με την δια-πιστοποίηση όλων των επιμέρους ριζικών ΑΠ ή εναλλακτικά με την ανάπτυξη μίας ΑΠ έμπιστου διαμεσολαβητή η οποία να επικοινωνεί με όλες τις ριζικές ΑΠ.

Επιπλέον, θα πρέπει να περιγραφούν αναλυτικά τα στάδια εγγραφής και ταυτοποίησης των χρηστών, καθώς και οι διαδικασίες έκδοσης και ανάκλησης των πιστοποιητικών. Θα πρέπει να καθορισθούν οι ρόλοι και οι αρμοδιότητες του προσωπικού αναφορικά με τη διαχείριση των κρυπτογραφικών κλειδιών και να αποτυπωθεί με κάθε λεπτομέρεια η τελετή δημιουργίας του ιδιωτικού κλειδιού του παρόχου (root key generation ceremony). Επίσης, θα πρέπει να ορισθούν οι υπεύθυνοι για κάθε υποσύστημα της ΥΔΚ σύμφωνα με το οργανωτικό σχήμα που προβλέπει το σχέδιο ασφάλειας και το σχέδιο επιχειρησιακής συνέχειας του ΠΥΠ.

Η τεχνική υλοποίηση της ΥΔΚ απαιτεί αναλυτική σχεδίαση και λεπτομερή αξιολόγηση όλων των παραμέτρων που επηρεάζουν την απόδοση, την επεκτασιμότητα, την ευελιξία και τη διαλειτουργικότητα του συστήματος. Θα πρέπει να ληφθούν υπόψη όλες οι απαιτήσεις ασφάλειας και ιδιωτικότητας των υπηρεσιών που θα παρέχονται από την ΥΔΚ.

Επιπλέον, θα πρέπει να γίνει προσεκτική διαστασιολόγηση της κίνησης και του αριθμού των τελικών οντοτήτων που θα πρέπει να εξυπηρετεί. Η επιλογή για παράδειγμα, μεταξύ ενός συστήματος κλειστής αρχιτεκτονικής ή μίας υλοποίησης ανοιχτού κώδικα ενδέχεται να επηρεάσει δραστικά στο μέλλον το βαθμό ευελιξίας, διαλειτουργικότητας, καθώς και το συνολικό κόστος συντήρησης της υποδομής.

Εξαιρετικά σημαντικός παράγοντας επιτυχίας μίας ΥΔΚ είναι το επίπεδο τεχνογνωσίας που χαρακτηρίζει το προσωπικό του ΠΥΠ. Ο βαθμός πολυπλοκότητας και οι αναγκαίες τεχνολογικές προσαρμογές απαιτούν την προσέλκυση στελεχών με υψηλό επίπεδο εκπαίδευσης και επιστημονικής επάρκειας. Ο ΠΥΠ θα πρέπει να φροντίζει για τη συνεχή εκπαίδευση και συμμετοχή τους σε επιστημονικά δίκτυα, μέσα από τα οποία να αποκτούν νέες γνώσεις και εμπειρίες για τα αντικείμενα της αρμοδιότητάς τους.

4. ΤΕΧΝΙΚΗ ΥΛΟΠΟΙΗΣΗ

Η Κοινωνία της Πληροφορίας χαρακτηρίζεται από την εφαρμογή των Τεχνολογιών Πληροφορικής και Επικοινωνιών σε όλα τα επίπεδα δραστηριότητας με στόχο την ενεργή συμμετοχή των πολιτών, των επιχειρήσεων και των κυβερνητικών οργανισμών σε διαδικτυακές συναλλαγές χρησιμοποιώντας προηγμένες ηλεκτρονικές υπηρεσίες. Συνεπώς, η ασφάλεια της πληροφορίας και η προστασία της ιδιωτικότητας αποκτούν, ολοένα και περισσότερο, σημαντικό ρόλο στην ανάπτυξη της οικονομίας και στη διατήρηση της ευημερίας μιας πολιτείας. Ωστόσο, η προστασία των ψηφιακών αγαθών προϋποθέτει επίγνωση των απειλών και των αδυναμιών που πηγάζουν από το διαδίκτυο, καθώς και ικανότητα εφαρμογής βασικών αντιμέτρων ασφάλειας.

Σύμφωνα με τα αποτελέσματα μίας πρόσφατης σημαντικής επιστημονικής έρευνας [36] αποδεικνύεται ότι η πλειοψηφία των ατόμων νεαρής ηλικίας και έμπειροι χρήστες εφαρμογών του διαδικτύου, δεν είναι εξοικειωμένοι με τις βασικές έννοιες της κρυπτογραφίας και δεν είναι ικανοί να διαχειριστούν και να χρησιμοποιήσουν αποτελεσματικά τα ψηφιακά πιστοποιητικά. Συνεπώς, παρατηρείται μία βασική έλλειψη επιμόρφωσης και ουσιαστικής κατανόησης των θεμάτων που άπτονται του γνωστικού αντικείμενου των ΥΔΚ, η οποία θα πρέπει να αντιμετωπιστεί με το κατάλληλο συνδυασμό θεωρητικής και πρακτικής εκπαίδευσης.

Τα πανεπιστημιακά τμήματα και σχολές πληροφορικής αποτελούν τον ιδανικό χώρο για τη δημιουργία της απαραίτητης επιστημονικής επάρκειας και τεχνογνωσίας σε ζητήματα ΥΔΚ. Προτείνεται η υιοθέτηση μίας τεχνικής μάθησης που να στηρίζεται στην εκπόνηση εργασιών οι οποίες θα περιγράφουν ένα σενάριο παροχής μίας νέας ηλεκτρονικής υπηρεσίας. Οι φοιτητές σε κάθε εργασία θα πρέπει να εκπονήσουν μία μελέτη περίπτωσης η οποία θα περιλαμβάνει την ανάλυση των απαιτήσεων ασφάλειας, τον προσδιορισμό και τεκμηρίωση των κατάλληλων πολιτικών πιστοποιητικών, τη σχεδίαση, καθώς και την πρακτική υλοποίηση της ΥΔΚ η οποία θα υποστηρίζει την παροχή της υπηρεσίας.

Η προτεινόμενη εκπαιδευτική προσέγγιση έχει το πλεονέκτημα ότι επιτρέπει την αφομοίωση και την εφαρμογή της θεωρίας στην πράξη, παρέχοντας τη δυνατότητα στους σπουδαστές να εξοικειωθούν με τις έννοιες της εφαρμοσμένης ασύμμετρης κρυπτογραφίας. Οι λειτουργικές απαιτήσεις της παραπάνω εκπαιδευτικής πρότασης περιλαμβάνουν την ανάπτυξη ενός γραφικού περιβάλλοντος προσομοίωσης ΥΔΚ αρκετά φιλικό, εύχρηστο και ταυτόχρονα ολοκληρωμένο, το οποίο να δίνει τη δυνατότητα σχεδίασης και υλοποίησης μίας αξιόπιστης, ευέλικτης, επεκτάσιμης και σταθερής ΥΔΚ παρέχοντας τη δυνατότητα διαχείρισης ολόκληρου του κύκλου ζωής των ψηφιακών πιστοποιητικών.

Η παρούσα ενότητα εξετάζει την υλοποίηση μιας ΥΔΚ για εκπαιδευτικούς σκοπούς, χρησιμοποιώντας λογισμικό ανοιχτού κώδικα, στοχεύοντας στην κατανόηση των εφαρμογών της κρυπτογραφίας δημόσιου κλειδιού, στη διαχείριση των ψηφιακών πιστοποιητικών και ειδικότερα στην αξιοποίηση και πρακτική χρήση των ψηφιακών υπογραφών και της χρονοσήμανσης.

Αναλυτικότερα, χρησιμοποιώντας ένα ευέλικτο γραφικό εργαστηριακό περιβάλλον υποδομής Oracle VM VirtualBox έκδοση 4.2.12 και λειτουργικού συστήματος Linux Ubuntu έκδοση 12.04.2 – desktop – amd64, θα εγκατασταθεί το λογισμικό EJBCA σε μία αρχιτεκτονική διάταξη που θα παρέχει τη δυνατότητα διεξαγωγής ολοκληρωμένων εκπαιδευτικών ασκήσεων και σεναρίων σχεδίασης και ανάπτυξης μίας Υποδομής Δημόσιου Κλειδιού, διαχείρισης του κύκλου ζωής των ψηφιακών πιστοποιητικών, καθώς και της αξιοποίησης των ψηφιακών υπογραφών για την ηλεκτρονική διακίνηση εγγράφων, εξασφαλίζοντας τη συμμόρφωση με τις απαιτήσεις ασφάλειας για αυθεντικοποίηση, ακεραιότητα, και μη αποποίηση της ευθύνης.

4.1. Υποδομή Δημόσιου Κλειδιού

Η εφαρμογή της κρυπτογραφίας δημόσιου κλειδιού στηρίζεται στη χρήση ψηφιακών πιστοποιητικών για την αυθεντικοποίηση των οντοτήτων που συμμετέχουν στην επικοινωνία. Ωστόσο, η πολυπλοκότητα των διαδικασιών έκδοσης και διαχείρισης του κύκλου ζωής των ψηφιακών πιστοποιητικών σε υλοποιήσεις ευρείας κλίμακας, με μεγάλο αριθμό χρηστών σε επίπεδο επιχείρησης, οργανισμού ή Δημόσιας Διοίκησης, οδηγεί στην ανάγκη ανάπτυξης, σχεδίασης και εγκατάστασης εφαρμογών λογισμικού Αρχής Πιστοποίησης.

Η εφαρμογή EJBCA (Enterprise Java Beans Certification Authority) αποτελεί ένα λογισμικό ανοιχτού κώδικα Αρχής Πιστοποίησης για την υλοποίηση μιας Υποδομής Δημόσιου Κλειδιού σε μεγάλη κλίμακα [37],[38]. Είναι σχεδιασμένη σε τεχνολογία Java Enterprise Edition (JEE) και κατά συνέπεια, μπορεί να εγκατασταθεί σε οποιαδήποτε πλατφόρμα λειτουργικού συστήματος. Επιτρέπει την έκδοση και διαχείριση ολόκληρου του κύκλου ζωής των ψηφιακών πιστοποιητικών για χρήστες, εξυπηρετητές και συσκευές, σύμφωνα με τα πρότυπα X509 έκδοση 3 και CVC BSI TR-03110 [39],[40],[41],[42],[43]. Επίσης, υποστηρίζει την ανάπτυξη και την παροχή της υπηρεσίας πρωτοκόλλου OCSP για την επαλήθευση της κατάστασης των ψηφιακών πιστοποιητικών που εκδίδει.

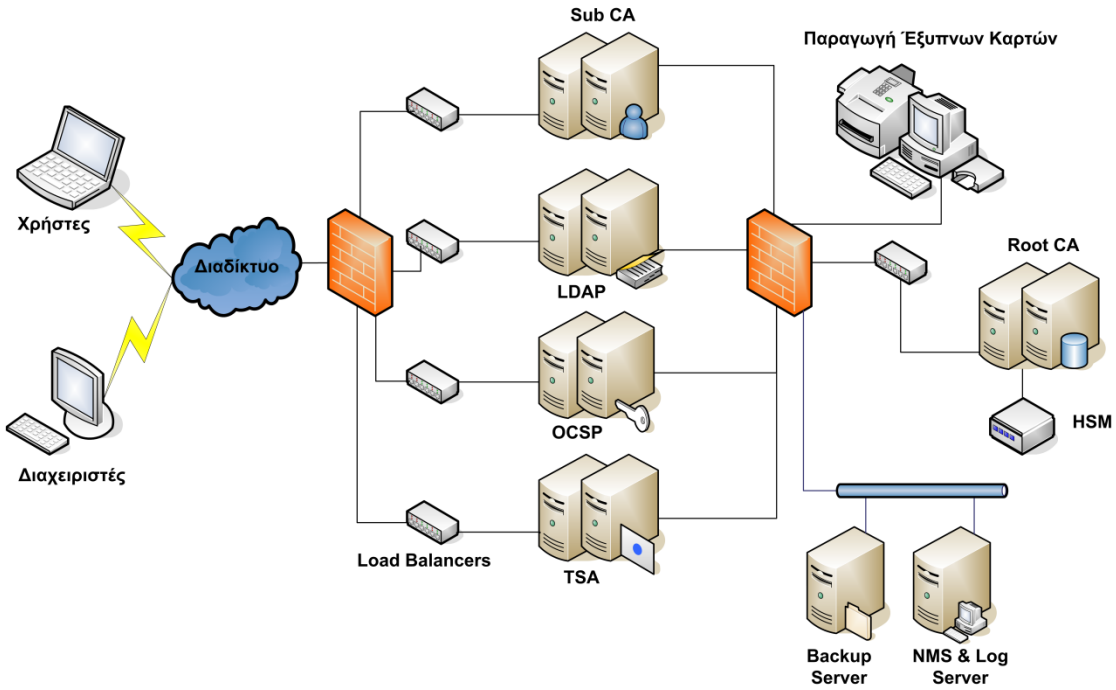
Η EJBCA έχει αναπτυχθεί και υποστηρίζεται από τη Σουηδική εταιρία πληροφορικής PrimeKey Solutions AB, η οποία εξειδικεύεται σε πληροφοριακά συστήματα ασφάλειας και υποδομές δημόσιου κλειδιού. Το έργο ξεκίνησε το Δεκέμβριο του 2001 και σήμερα περιέχει περίπου 260.000 γραμμές κώδικα. Η εφαρμογή υπάγεται στην Ελάσσονα Γενική Άδεια Δημόσιας Χρήσης GNU (GNU Lesser General Public License – LGPL) όπου περιγράφονται αναλυτικά οι όροι διανομής του λογισμικού.

Η αρχιτεκτονική δομή της EJBCA αποτελείται από τέσσερα συγκεκριμένα επίπεδα: χρήστη, διαδικτύου, EJB και δεδομένων, όπως παρουσιάζονται στην Εικόνα 5.

Εικόνα 5. Αρχιτεκτονική EJBCA

Υπάρχουν δύο βασικές εκδόσεις του EJBCA PKI λογισμικού: η EJBCA Community Edition και η πιστοποιημένη EJBCA Enterprise Edition. Η EJBCA Community έκδοση (EJBCA 4) παρέχεται δωρεάν και είναι κατάλληλη για μη πιστοποιημένες υλοποιήσεις υποδομής δημόσιου κλειδιού. Η EJBCA PKI Enterprise έκδοση (EJBCA 5) έχει πιστοποιηθεί σύμφωνα με τα Common Criteria EAL4+, συμμορφώνεται με πρότυπα όπως το CWA/ETSI Qualified Certificates και το WebTrust και διαθέτει επιπλέον λειτουργικά χαρακτηριστικά ασφάλειας. Είναι διαθέσιμη δωρεάν μόνο στους πελάτες τεχνικής υποστήριξης της εταιρίας PrimeKey ή σε επίσημους συνεργάτες. Οι αναβαθμίσεις και η δυνατότητα λήψεων λογισμικού περιλαμβάνονται δωρεάν [44].

Η δικτυακή αρχιτεκτονική διάταξη υλοποίησης μίας ΥΔΚ διαφέρει ανάλογα με τις απαιτήσεις ασφάλειας και τις επιχειρησιακές ανάγκες που καλείται να εξυπηρετήσει. Στην Εικόνα 6 παρουσιάζεται μία προτεινόμενη αρχιτεκτονική υλοποίηση μίας ΥΔΚ η οποία απευθύνεται σε οργανισμούς των οποίων τα πληροφοριακά συστήματα και οι εγκαταστάσεις πρέπει να διαθέτουν υψηλά επίπεδα ασφάλειας και διαθεσιμότητας.



Εικόνα 6. ΥΔΚ – προτεινόμενη αρχιτεκτονική διάταξη

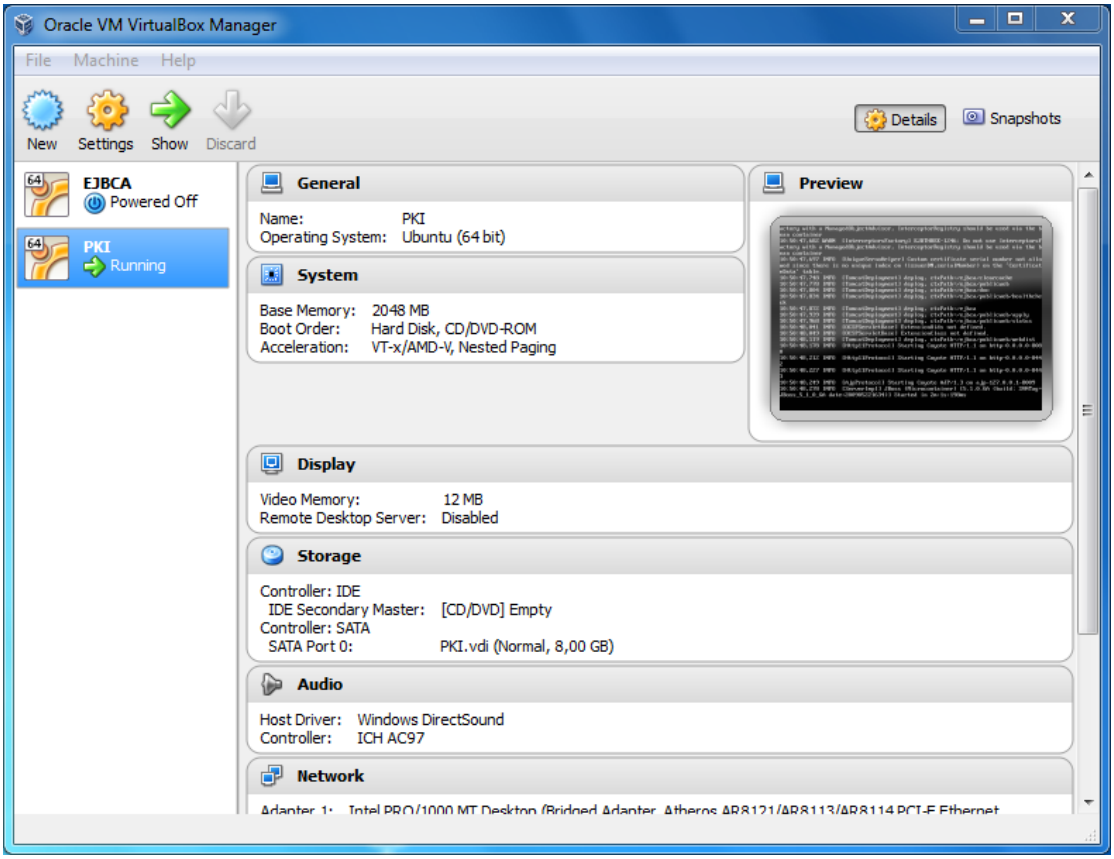
Στη συγκεκριμένη υλοποίηση οι χρήστες και οι διαχειριστές μπορούν να προσπελάσουν με ασφάλεια τις υπηρεσίες δημόσιου κλειδιού μέσω του διαδικτύου χρησιμοποιώντας το πρωτόκολλο SSL. Τα πληροφοριακά συστήματα της υποδομής προστατεύονται από firewalls σε διάταξη εφεδρείας failover και η δικτυακή κίνηση μοιράζεται, με την εγκατάσταση load balancers, στους εξυπηρετητές οι οποίοι βρίσκονται σε συστοιχίες διάταξης υψηλής διαθεσιμότητας.

Επίσης, προβλέπονται εξυπηρετητές λήψης αντιγράφων ασφάλειας, διαχείρισης και επίβλεψης του εξοπλισμού, καθώς και καταγραφής των ενεργειών και συμβάντων. Η συστοιχία εξυπηρετητών που φιλοξενούν την Πρωτεύουσα Αρχή Πιστοποίησης (Root CA) προστατεύεται από ένα δεύτερο επιπλέον επίπεδο firewalls (ασφάλεια σε βάθος). Τα κλειδιά της Πρωτεύουσας Αρχή Πιστοποίησης φυλάσσονται για λόγους ασφάλειας σε κατάλληλο Hardware Secure Module (HSM) συμβατό με την εφαρμογή EJBCA.

4.2. Ανάπτυξη Εργαστηρίου

Ολόκληρη η υποδομή θα αναπτυχθεί χρησιμοποιώντας εργαλεία και λογισμικό ανοιχτού κώδικα. Αρχικά, θα εγκατασταθεί η εφαρμογή Oracle VM VirtualBox η οποία θα επιτρέψει τη δημιουργία μιας εικονικής μηχανής που θα αποτελέσει τον κεντρικό εξυπηρετητή. Το Oracle VM VirtualBox έκδοση 4.2.12 (Εικόνα 7) είναι ένα δωρεάν λογισμικό το οποίο παρέχει τη δυνατότητα εκτέλεσης ενός ή περισσότερων λειτουργικών συστημάτων μέσα από μία εικονική μηχανή, χρησιμοποιώντας παράλληλα το ήδη εγκατεστημένο λειτουργικό του υπολογιστή.

Το πρόγραμμα διαθέτει ένα εύχρηστο μενού και οδηγούς που κατευθύνουν το χρήστη, βήμα προς βήμα, στην εγκατάσταση μίας εικονικής μηχανής και αναπτύσσεται συνεχώς με νέες αναβαθμισμένες εκδόσεις [45].

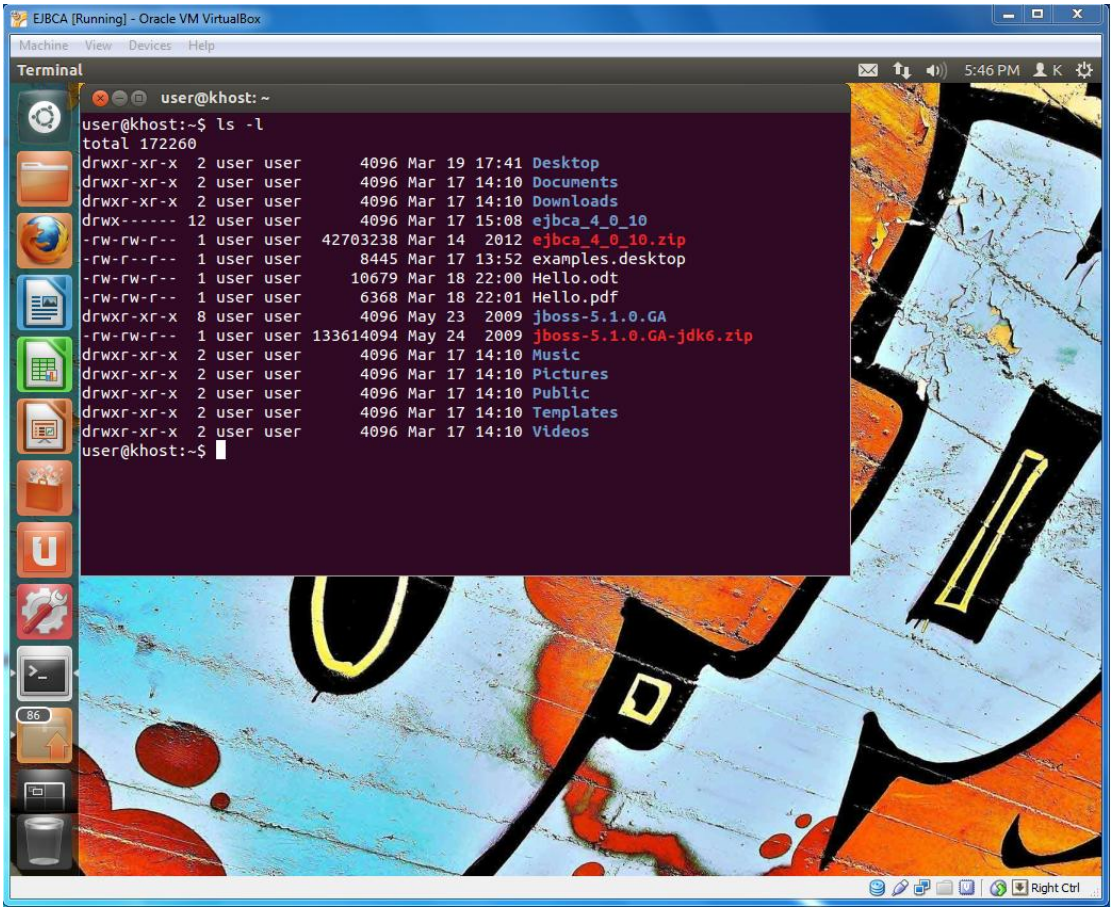


Εικόνα 7. Η εφαρμογή Oracle VM VirtualBox

Το εργαστήριο θα υλοποιηθεί σε περιβάλλον Linux Ubuntu διότι είναι ένα λειτουργικό σύστημα ανοιχτού κώδικα ικανοποιητικά σταθερό και φιλικό προς τους χρήστες.

Μετά από την επιτυχημένη εγκατάσταση του Oracle VM VirtualBox, δημιουργείται μία εικονική μηχανή με 2GB μνήμης η οποία θα φιλοξενήσει τον εικονικό εξυπηρετητή με λειτουργικό σύστημα Linux Ubuntu έκδοση 12.04.2 – desktop – amd64 [46].

Εκτελείται η λήψη και η εγκατάσταση του λειτουργικού συστήματος και ορίζονται οι επιθυμητές παράμετροι λειτουργίας, όπως παρουσιάζεται στην Εικόνα 8.

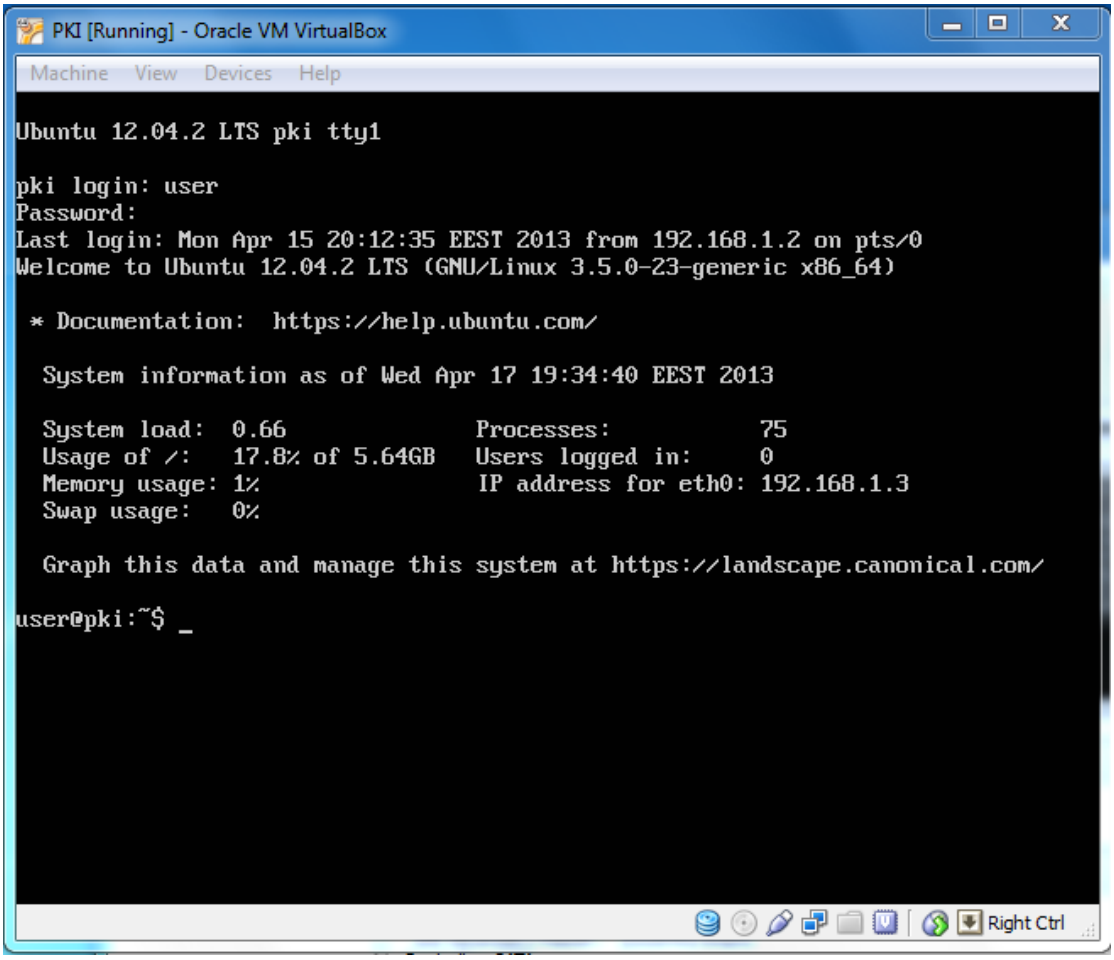


Εικόνα 8. Λειτουργικό Σύστημα Linux Ubuntu 12.04.2 – desktop – amd64

Εναλλακτικά, μετά την εγκατάσταση του Oracle VM VirtualBox και τη δημιουργία μίας εικονικής μηχανής με 2GB μνήμης, μπορεί να εγκατασταθεί το λειτουργικό σύστημα Linux Ubuntu έκδοση 12.04.2 – server – amd64 [47].

Το συγκεκριμένο λειτουργικό είναι κατάλληλο για την εγκατάσταση εξυπηρετητών διότι η απουσία του γραφικού περιβάλλοντος εργασίας μειώνει την επιφάνεια επίθεσης.

Εκτελείται η λήψη και η εγκατάσταση του λειτουργικού συστήματος και ορίζονται οι επιθυμητές παράμετροι λειτουργίας, όπως παρουσιάζεται στην Εικόνα 9.



Εικόνα 9. Λειτουργικό Σύστημα Linux Ubuntu έκδοση 12.04.2 – server – amd64

Εκτελούνται οι ακόλουθες εντολές για τη λήψη και εγκατάσταση των τελευταίων ενημερώσεων.

sudo apt-get update
sudo apt-get install

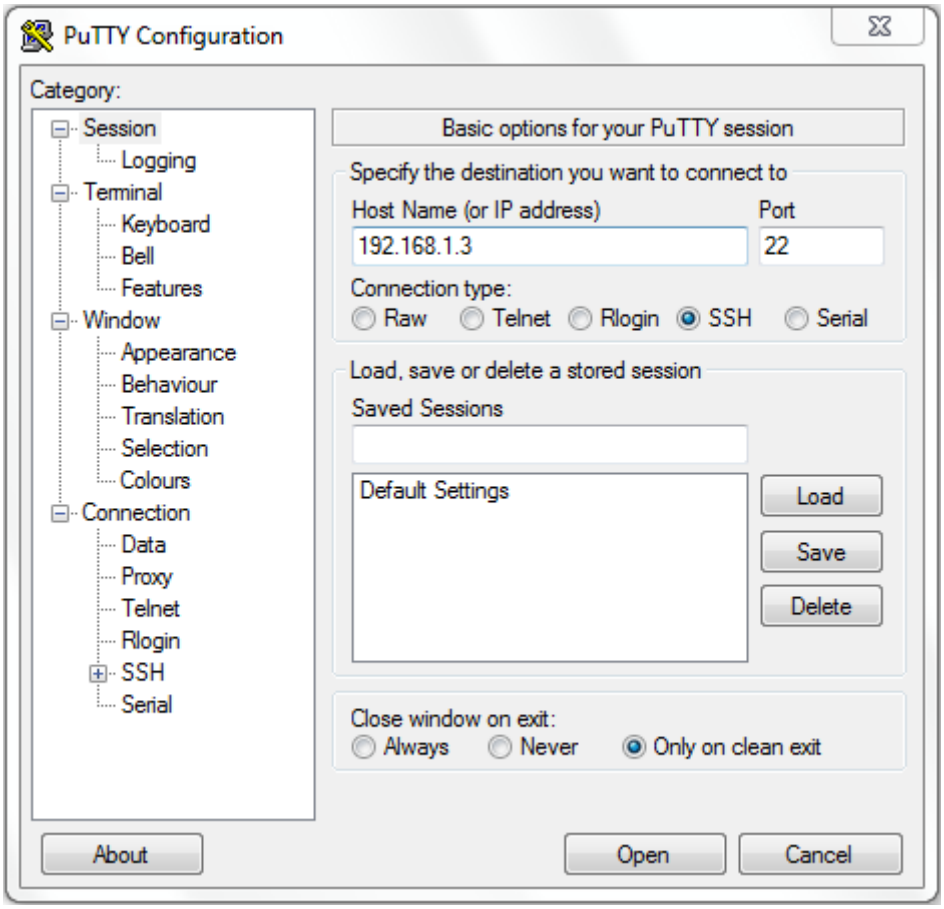
Στη συνέχεια εκτελείται η ακόλουθη εντολή για να υπάρχει η δυνατότητα εγκαθίδρυσης ssh σύνδεσης με τον εξυπηρετητή.

sudo apt-get install openssh-server

Επίσης, είναι απαραίτητη η εγκατάσταση ενός FTP server για να υπάρχει η δυνατότητα μεταφοράς αρχείων από τον εξυπηρετητή. Για το σκοπό αυτό, εγκαθίσταται ο vsftpd (Very Secure FTP Daemon) server εκτελώντας τις ακόλουθες εντολές [48].

sudo apt-get install vsftpd
sudo nano /etc/vsftpd.conf
anonymous_enable=NO
local_enable=YES
write_enable=YES
Ctrl+O (save)
Ctrl+X (exit)
sudo /etc/init.d/vsftpd restart

Η δυνατότητα απομακρυσμένης σύνδεσης επιτυγχάνεται χρησιμοποιώντας το λογισμικό ανοιχτού κώδικα PuTTY, το οποίο είναι ένα SSH και telnet client, όπως παρουσιάζεται στην Εικόνα 10 [49].



Εικόνα 10. PuTTY, SSH και telnet client

Την έναρξη λειτουργίας του εικονικού εξυπηρετητή ακολουθεί η διαδικασία εγκατάστασης του συστήματος EJBCA ανοίγοντας μία κονσόλα τερματικού. Στη συνέχεια, περιγράφεται αναλυτικά, βήμα προς βήμα, ολόκληρη η διαδικασία εγκατάστασης [50],[51].

Θα εγκατασταθεί η EJBCA 4.0.10 και ο application server JBoss 5.1.0.GA. Η εγκατάσταση διαφορετικών εκδόσεων μπορεί να γίνει απλά αντικαθιστώντας τον επιθυμητό αριθμό έκδοσης στις αντίστοιχες εντολές. Η διαδικασία εκτελείται από έναν λογαριασμό χρήστη με το όνομα “user” και παρουσιάζεται αναλυτικά στην επόμενη σελίδα.

Διαδικασία Εγκατάστασης

1. **Εγκατάσταση Linux Ubuntu έκδοση 12.04.2 – desktop – amd64 (εναλλακτικά μπορεί να εγκατασταθεί Ubuntu 12.04 server x64 με την προεπιλεγμένη παραμετροποίηση επιλέγοντας τον OpenSSH server).**

Ορισμός χρήστη με όνομα "user" κατά τη διάρκεια της εγκατάστασης. Ο αρχικός κατάλογος του χρήστη "user" βρίσκεται στη διαδρομή: /home/user.

2. **Άνοιγμα μίας νέας κονσόλας τερματικού "ejbca".**
3. **Εγκατάσταση προαπαιτούμενου λογισμικού από τις πηγές του Ubuntu.**

sudo apt-get install openjdk-6-jdk ant ant-optional unzip ntp

4. **Εγκατάσταση λογισμικού application server JBoss 5.1.0.GA-jdk6 και EJBCA 4.0.10 που δεν περιέχεται στα αποθετήρια του Ubuntu.**

wget http://sourceforge.net/projects/jboss/files/JBoss/JBoss-5.1.0.GA/jboss-5.1.0.GA-jdk6.zip

wget http://sourceforge.net/projects/ejbca/files/ejbca4/ejbca_4_0_10/ejbca_4_0_10.zip

unzip jboss-5.1.0.GA-jdk6.zip

unzip ejbca_4_0_10.zip

5. **Παραμετροποίηση της EJBCA ούτως ώστε να μπορεί να επικοινωνήσει με τον application server (JBoss).**

echo "appserver.home=/home/user/jboss-5.1.0.GA" >> ejbca_4_0_10/conf/ejbca.properties

6. **Ανάπτυξη και υλοποίηση της EJBCA με τον JBoss.**

cd ejbca_4_0_10

ant bootstrap (enter στην περίπτωση εμφάνισης ερωτήσεων)

7. **Άνοιγμα μίας νέας κονσόλας τερματικού "jboss" και εκκίνηση του JBoss.**

jboss-5.1.0.GA/bin/run.sh

8. **Επιστροφή στο τερματικό "ejbca" και εκτέλεση της εντολής "install" για τη δημιουργία της αρχικής CA με ρόλο διαχειριστή.**

ant install (επιλογή όλων των προεπιλεγμένων τιμών)

ant deploy

9. **Επιστροφή στο τερματικό "jboss" και επανεκκίνηση του JBoss.**

ctrl-c

jboss-5.1.0.GA/bin/run.sh

10. **Αντιγραφή του αρχείου: /home/user/ejbca_4_0_10/p12/superadmin.p12 στην επιφάνεια εργασίας του διαχειριστή και εισαγωγή του στο πρόγραμμα περιήγησης ιστού (web browser).**
11. **Σύνδεση στο URL https://server:8443/ejbca, όπου "server" είναι το όνομα του EJBCA εξυπηρετητή ή εναλλακτικά η IP διεύθυνσή του.**

Ολοκλήρωση της διαδικασίας εγκατάστασης!

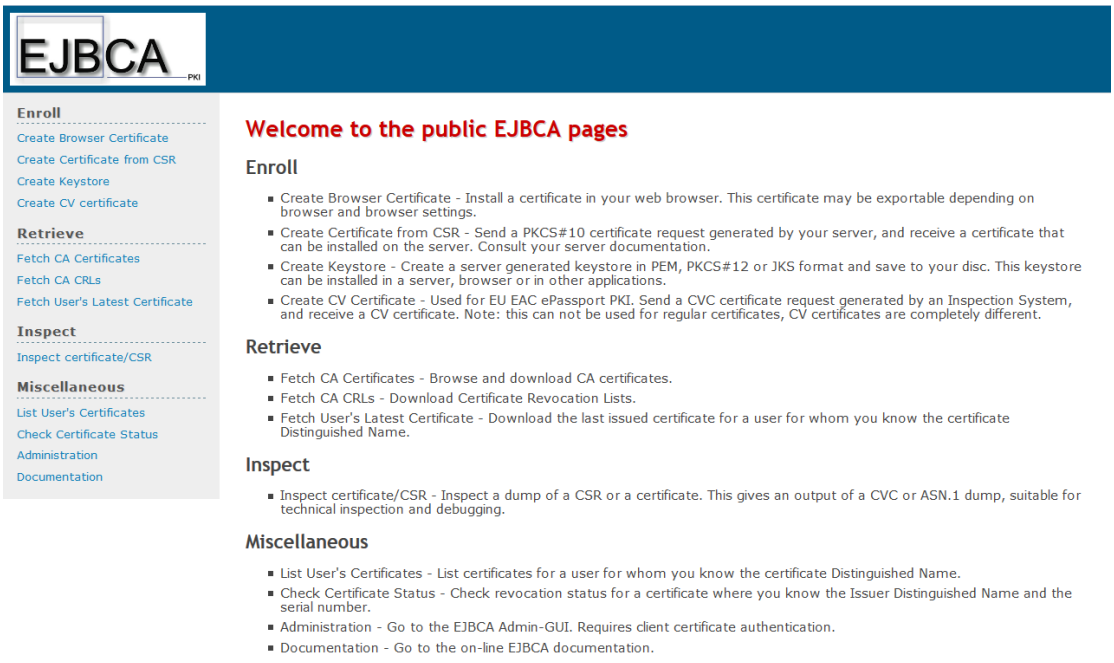
Η εφαρμογή δημιουργεί ένα ψηφιακό πιστοποιητικό χαλαρής αποθήκευσης με χρήση κλειδιού υπογραφής, μη αποποίησης, και κρυπτογράφησης για την αυθεντικοποίηση του διαχειριστή του συστήματος. Το πιστοποιητικό αυτό πρέπει να αντιγραφεί και να εγκατασταθεί στο πρόγραμμα περιήγησης ιστού του υπολογιστή από τον οποίο ο διαχειριστής επιθυμεί να προσπελάσει την ΥΔΚ.

Ως πρόγραμμα περιήγησης προτείνεται να χρησιμοποιηθεί το λογισμικό ανοιχτού κώδικα Firefox του μη κερδοσκοπικού οργανισμού Mozilla [52].

Ο τελικός χρήστης μπορεί να προσπελάσει την ΥΔΚ μέσω διαδικτυακής σύνδεσης στο παρακάτω URL, όπου “server” είναι το όνομα του EJBCA εξυπηρετητή ή εναλλακτικά η IP διεύθυνσή του.

http://server:8080/ejbca

Η δημόσια ιστοσελίδα της εφαρμογής EJBCA παρουσιάζεται στην Εικόνα 11.



Εικόνα 11. Η δημόσια ιστοσελίδα της EJBCA

Ο διαχειριστής της εφαρμογής συνδέεται στην ΥΔΚ μέσω ασφαλούς διαδικτυακής σύνδεσης στο παρακάτω URL, όπου “server” είναι το όνομα του EJBCA εξυπηρετητή ή εναλλακτικά η IP διεύθυνσή του.

https://server:8443/ejbca

Μετά τον έλεγχο της εγκυρότητας του πιστοποιητικού αυθεντικοποίησης η εφαρμογή επιτρέπει την πρόσβαση στον διαχειριστή, όπως παρουσιάζεται στην Εικόνα 12.

Εικόνα 12. Το περιβάλλον διαχείρισης της EJBCA

Το γραφικό περιβάλλον διαχείρισης της εφαρμογής επιτρέπει την ανάπτυξη μίας ολοκληρωμένης ΥΔΚ, με τον ορισμό και την ενεργοποίηση ριζικής ΑΠ, υποκείμενης ΑΠ, προφίλ πιστοποιητικών, υπηρεσίες καταλόγου και έγκριση πιστοποιητικών.

4.3. Μελέτη Περίπτωσης

Η αξία μίας ΥΔΚ είναι ανάλογη των ηλεκτρονικών υπηρεσιών που παρέχει στους τελικούς χρήστες. Η αξιολόγηση και ο έλεγχος του εργαστηριακού περιβάλλοντος εκπαίδευσης και εργασίας της παραγράφου 4.2, θα πραγματοποιηθεί με την εκπόνηση μίας μελέτης περίπτωσης. Στόχος είναι η επικύρωση της πλήρης συμμόρφωσης του συστήματος με τις αρχικές λειτουργικές απαιτήσεις της ΥΔΚ. Επίσης, η μελέτη περίπτωσης θα επιβεβαιώσει την ορθότητα των συμπερασμάτων της επιχειρησιακής ανάλυσης του κεφαλαίου 3. Τέλος, θα δοκιμασθούν και θα προταθούν διάφορες εφαρμογές αυτοματισμού γραφείου ανοιχτού λογισμικού για την πρακτική αξιοποίηση και χρήση των ψηφιακών πιστοποιητικών.

Η μελέτη περίπτωσης αφορά την ανάπτυξη μίας ιεραρχικής ΥΔΚ με στόχο τη διαχείριση του κύκλου ζωής των ψηφιακών πιστοποιητικών, τα οποία θα διατίθενται στα μέλη ΔΕΠ και στους φοιτητές ενός πανεπιστημίου για την υποστήριξη της ηλεκτρονικής υπηρεσίας υποβολής των εργασιών στο πλαίσιο των μαθημάτων. Αρχικά, θα εξεταστούν οι απαιτήσεις ασφάλειας και στη συνέχεια θα αναλυθούν οι διαδικασίες εγγραφής και χρήσης της ηλεκτρονικής υπηρεσίας.

Το ζητούμενο είναι να μπορεί ένας καθηγητής να κοινοποιεί στους φοιτητές του το κείμενο της εργασίας εξασφαλίζοντας την εγκυρότητα του ηλεκτρονικού εγγράφου. Επίσης, ο καθηγητής μετά από τη διόρθωση των εργασιών, θα πρέπει να έχει τη δυνατότητα να αποστείλει στους σπουδαστές εξατομικευμένες παρατηρήσεις και σχόλια, καθώς και την τελική βαθμολογία της εργασίας, εξασφαλίζοντας το απόρρητο της επικοινωνίας. Συνεπώς, οι απαιτήσεις ασφάλειας της υπηρεσίας είναι η αυθεντικοποίηση του συντάκτη, η ακεραιότητα του κειμένου και η εμπιστευτικότητα.

Στην περίπτωση αποστολής της εργασίας με ηλεκτρονικό ταχυδρομείο, η επιπρόσθετη ψηφιακή υπογραφή του μηνύματος αυθεντικοποιηθεί τον αποστολέα και εξασφαλίζει

την ακεραιότητα του περιεχομένου. Επιπλέον, το μήνυμα μπορεί να κρυπτογραφηθεί με το δημόσιο κλειδί του παραλήπτη. Οι συγκεκριμένες απαιτήσεις ασφάλειας ικανοποιούνται, σύμφωνα με τον Πίνακα 1, με τη χρήση πιστοποιητικών ψηφιακής υπογραφής και κρυπτογράφησης.

Οι φοιτητές με τη σειρά τους, θα πρέπει να παραδώσουν την εργασία τους στον καθηγητή εντός καθορισμένης προθεσμίας, αποδεικνύοντας την εγκυρότητα του ηλεκτρονικού εγγράφου, τον χρόνο και την ημερομηνία υπογραφής και επιπλέον εξασφαλίζοντας το απόρρητο της επικοινωνίας. Κατά συνέπεια, οι απαιτήσεις ασφάλειας της υπηρεσίας είναι η αυθεντικοποίηση του συντάκτη, η ακεραιότητα του κειμένου και η μη αποποίηση της ευθύνης αναφορικά με το χρόνο ολοκλήρωσης της εργασίας. Επιπλέον, υπάρχει η απαίτηση της εμπιστευτικότητας του περιεχομένου της επικοινωνίας. Όλες αυτές οι απαιτήσεις ασφάλειας ικανοποιούνται, σύμφωνα με τον Πίνακα 1, με τη χρήση ψηφιακής υπογραφής, χρονοσήμανσης και κρυπτογράφησης.

Οι καθηγητές και οι φοιτητές αποτελούν τους τελικούς χρήστες της ηλεκτρονικής υπηρεσίας υποβολής εργασιών. Συνεπώς, υπάρχει η απαίτηση ταυτοποίησης και εξουσιοδότησης των χρηστών ούτως ώστε να μπορούν να συμμετέχουν στην επικοινωνία. Η συγκεκριμένη απαίτηση μπορεί να ικανοποιηθεί, πάντοτε σύμφωνα με τον Πίνακα 1, με την εγγραφή των χρηστών, την έγκριση και έκδοση των ψηφιακών πιστοποιητικών τους και τις παρεχόμενες υπηρεσίες καταλόγου της ΥΔΚ.

Το συμπέρασμα είναι ότι η ΥΔΚ καλύπτει πλήρως τις απαιτήσεις ασφάλειας της υπηρεσίας ηλεκτρονικής υποβολής εργασιών. Ο καθηγητής συντάσσει το θέμα της εργασίας σε ηλεκτρονικό έγγραφο, το υπογράφει ψηφιακά και στη συνέχεια το αναρτά σε προσυμφωνημένη ιστοσελίδα ή το αποστέλλει στους φοιτητές του επισυναπτόμενο σε μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο υπογράφει επίσης ψηφιακά. Οι φοιτητές επαληθεύουν το γνήσιο της ψηφιακής υπογραφής του καθηγητή και επιβεβαιώνουν την αυθεντικότητα και την ακεραιότητα του εγγράφου της εργασίας.

Οι σπουδαστές, ολοκληρώνοντας την εργασίας τους την υπογράφουν ψηφιακά με χρονοσήμανση, πετυχαίνοντας την αυθεντικοποίηση, την ακεραιότητα και την μη αποποίηση της ευθύνης για το χρόνο ολοκλήρωσης του εγγράφου. Στη συνέχεια την επισυνάπτουν σε μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο υπογράφουν ψηφιακά με το ιδιωτικό τους κλειδί και κρυπτογραφούν με το δημόσιο κλειδί του καθηγητή τους, το οποίο έχουν ανακτήσει διαδικτυακά από την υπηρεσία καταλόγου της ΥΔΚ.

Ο καθηγητής, μοναδικός κάτοχος του ιδιωτικού κλειδιού, είναι ο μόνος που μπορεί να αποκρυπτογραφήσει τα μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνει από τους φοιτητές του. Στη συνέχεια, επαληθεύει το γνήσιο της ψηφιακής υπογραφής κάθε φοιτητή, επιβεβαιώνοντας την αυθεντικότητα και την ακεραιότητα των εργασιών. Τέλος, ελέγχει την ώρα και την ημερομηνία δημιουργίας της υπογραφής από τη σχετική χρονοσήμανση και αποδέχεται ή απορρίπτει την εργασία ως εκπρόθεσμη.

Ο καθηγητής, διορθώνει και βαθμολογεί τις εργασίες συντάσσοντας ένα κείμενο αξιολόγησης για κάθε ένα φοιτητή, το οποίο περιέχει παρατηρήσεις, σχόλια, καθώς και την τελική αξιολόγηση. Υπογράφει ψηφιακά το κάθε έγγραφο ξεχωριστά και το επισυνάπτει σε μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο υπογράφει επίσης ψηφιακά και το κρυπτογραφεί με το δημόσιο κλειδί του αντίστοιχου σπουδαστή στον οποίο απευθύνεται. Ο φοιτητής αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί και επαληθεύει το γνήσιο της υπογραφής του καθηγητή, επιβεβαιώνοντας την αυθεντικότητα και την ακεραιότητα του εγγράφου αξιολόγησης της εργασίας.

Αναφορικά με την επιχειρησιακή διαδικασία διαχείρισης του κύκλου ζωής των ψηφιακών πιστοποιητικών, ως ΑΕ θα ορισθεί η γραμματεία του εκπαιδευτικού ιδρύματος. Τα μέλη ΔΕΠ και οι φοιτητές προσέρχονται στον αρμόδιο υπάλληλο της γραμματείας έχοντας συμπληρώσει και υπογράψει την αίτηση χορήγησης ψηφιακού

πιστοποιητικού. Ταυτόχρονα με την υποβολή και την πρωτοκόλληση της αίτησης, ο υπάλληλος κάνει την ταυτοποίηση του χρήστη, ελέγχοντας τα στοιχεία της αστυνομικής του ταυτότητας ή του διαβατηρίου. Τέλος, αρχειοθετεί την αίτηση έκδοσης πιστοποιητικού μαζί με ένα επικυρωμένο φωτοαντίγραφο της ταυτότητας.

Οι διαχειριστές της εφαρμογής ΑΠ θα εγκρίνουν ή θα απορρίψουν την αίτηση, ανάλογα με το αν ο χρήστης πληροί ή όχι τα κριτήρια της πολιτικής του πιστοποιητικού. Στην περίπτωση έγκρισης του αιτήματος, θα δημιουργήσουν το λογαριασμό του χρήστη και θα του αποστείλουν ενημερωτικό μήνυμα, με το ηλεκτρονικό ταχυδρομείο, το οποίο θα περιέχει τα συνθηματικά έκδοσης του πιστοποιητικού.

Εάν, κάποια στιγμή στο μέλλον, ο χρήστης αποφασίσει να ανακαλέσει το πιστοποιητικό του, εξαιτίας ενδεχόμενης απώλειας ή αποκάλυψης του ιδιωτικού του κλειδιού, θα απευθύνεται με αίτησή του στην ΑΕ ζητώντας την ανάκληση του πιστοποιητικού αναφέροντας το λόγο της απόφασής του.

Εικόνα 13. Κύκλος Ζωής Ψηφιακών Πιστοποιητικών

Η διαδικασία ανανέωσης του πιστοποιητικού ξεκινά με την έγκαιρη αποστολή ενημερωτικού μηνύματος ηλεκτρονικού ταχυδρομείου από την ΑΕ ότι το πιστοποιητικό του τελικού χρήστη πρόκειται να λήξει. Επίσης, η ΑΕ θα πρέπει να ελέγχει και να ενημερώνει το χρήστη για το εάν έχει το δικαίωμα ανανέωσης ή όχι του πιστοποιητικού του βάσει του κανονισμού πιστοποίησης. Εάν ο χρήστης συνεχίζει να πληροί τους όρους της πολιτικής θα μπορεί να αιτείται την ανανέωση του πιστοποιητικού του η οποία γίνεται παρόμοια με την αρχική έκδοση.

Η ανανέωση περιλαμβάνει την έκδοση ενός νέου πιστοποιητικού, δηλαδή με καινούργιο σειριακό αριθμό, περιέχοντας το ίδιο δημόσιο κλειδί του χρήστη, το οποίο είναι γνωστό στην ΑΠ και φυσικά τις νέες ημερομηνίες έκδοσης και λήξης. Στο διάγραμμα της Εικόνας 13 παρουσιάζονται τα βασικά στάδια του κύκλου ζωής των ψηφιακών πιστοποιητικών.

Η επικύρωση των ψηφιακών πιστοποιητικών πραγματοποιείται είτε μέσα από το γραφικό περιβάλλον του χρήστη με την επιλογή "Check Certificate Status", είτε με τις διάφορες εφαρμογές λογισμικού χρησιμοποιώντας το πρωτόκολλο OCSP και τους ΚΑΠ.

Κρίσιμος παράγοντας επιτυχίας της ΥΔΚ είναι καταρχήν η δέσμευση της Διοίκησης του ακαδημαϊκού ιδρύματος, έχοντας σκοπό την εξασφάλιση των απαραίτητων πόρων για την υλοποίηση της υποδομής και την εφαρμογή της υπηρεσίας από τα μέλη ΔΕΠ και τους φοιτητές του πανεπιστημίου. Απαραίτητη προϋπόθεση για τη λειτουργία της ΥΔΚ είναι επίσης, η έγκριση του κανονισμού πιστοποίησης, ο οποίος θα περιέχει την πολιτική πιστοποιητικών και τη δήλωσης πρακτικής. Επιπρόσθετα, θα πρέπει να διεξαχθεί ένας κύκλος εκπαίδευσης και ενημέρωσης των συμμετεχόντων στην ΥΔΚ αναφορικά με τις διαδικασίες, την τεχνολογία, τα δικαιώματα, τις υποχρεώσεις και τον τρόπο χρήσης των πιστοποιητικών, διαφορετικά υπάρχει μεγάλος κίνδυνος η υπηρεσία να απορριφτεί από τους ίδιους τους χρήστες.

Ο σημαντικότερος παράγοντας για την επιτυχία και τη βιωσιμότητα της όλης προσπάθειας είναι το ίδιο το περιεχόμενο της ηλεκτρονικής υπηρεσίας. Δηλαδή, η αντιλαμβανόμενη από τους τελικούς χρήστες προστιθέμενη αξία, η ποιότητα και η ευχρηστία της υπηρεσίας. Επίσης, ο τρόπος οργάνωσης, αναφορικά με την εγγραφή των χρηστών και τις διαδικασίες έγκρισης, έκδοσης, ανάκλησης και γενικότερα τη διαχείριση του κύκλου ζωής των ψηφιακών πιστοποιητικών, θα συμβάλει ουσιαστικά στην αποδοτική και αποτελεσματική λειτουργία της ΥΔΚ.

Η τεχνική υλοποίηση είναι επίσης πολύ σημαντική διότι εξασφαλίζει την εύρυθμη και αδιάλειπτη παροχή της υπηρεσίας. Το λογισμικό EJBCA επιλέχθηκε διότι είναι μία εφαρμογή ανοιχτού κώδικα, η οποία χαρακτηρίζεται από ευχρηστία, επεκτασιμότητα, διαλειτουργικότητα και ευελιξία. Τέλος, κρίσιμος παράγοντας επιτυχίας είναι η εμπειρογνωμοσύνη, η ικανότητα και η επιστημονική κατάρτιση του προσωπικού που θα αναλάβει την ευθύνη οργάνωσης, λειτουργίας και υποστήριξης της ΥΔΚ, καθώς και την επίλυση όλων των επιχειρησιακών, οργανωτικών και τεχνικών προβλημάτων που θα προκύψουν.

4.4. Διαχείριση & Λειτουργία

Η ΥΔΚ που απαιτείται για την παροχή της ηλεκτρονικής υπηρεσίας υποβολής εργασιών περιλαμβάνει την ανάπτυξη και ενεργοποίηση μίας ριζικής και μίας υποκείμενης ΑΠ, καθώς και τη δημιουργία των κατάλληλων προφίλ ψηφιακών πιστοποιητικών και τελικών χρηστών.

Η διαχείριση της EJBCA μπορεί να γίνει είτε μέσα από το γραφικό περιβάλλον της εφαρμογής (Εικόνα 12), είτε μέσα από περιβάλλον γραμμής εντολών:

cd ejbca_4_0_10/bin

./ejbca.sh

Η παραπάνω εντολή επιστρέφει όλες τις διαθέσιμες παραμέτρους και δυνατότητες. Ωστόσο, ο ευκολότερος τρόπος διαχείρισης της εφαρμογής είναι μέσα από το γραφικό

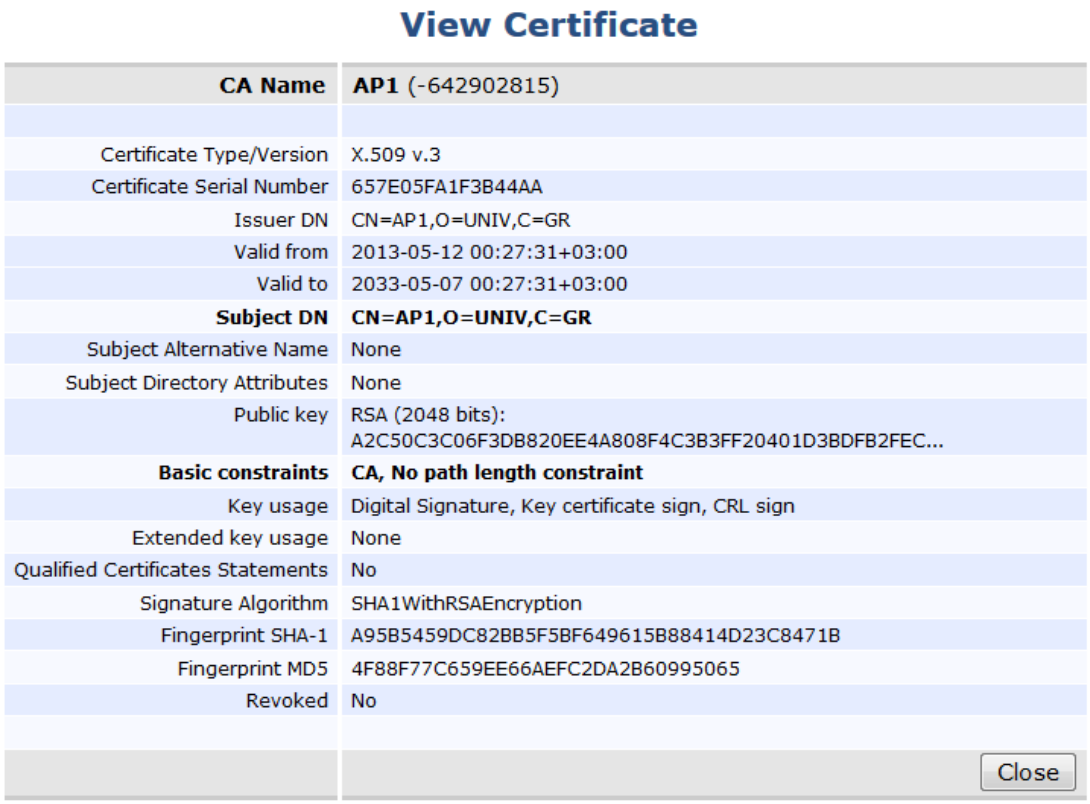
περιβάλλον. Μετά την επιτυχημένη εγκατάσταση του λογισμικού, η οποία δημιουργεί εξορισμού μία αρχική ριζική ΑΠ (AdminCA1), μπορεί να ξεκινήσει η ανάπτυξη και η παραμετροποίηση νέων ΑΠ. Μία νέα ΑΠ μπορεί να ορισθεί εναλλακτικά ως ριζική ΑΠ, ως υποκείμενη ΑΠ μίας άλλης ΑΠ της EJBCA ή ως υποκείμενη ΑΠ σε μία εξωτερική ΑΠ.

Η δημιουργία μίας νέας ΑΠ υλοποιείται μέσα από το γραφικό διαχειριστικό περιβάλλον με την επιλογή "Edit Certificate Authorities", τον ορισμό του ονόματος της ΑΠ και την εκτέλεση της εντολής "Create". Η νέα ριζική ΑΠ, που ορίζεται για τις ανάγκες υλοποίησης της ηλεκτρονικής υπηρεσίας υποβολής των εργασιών, ονομάζεται "AP1". Στη συνέχεια ορίζονται οι βασικές τιμές των παραμέτρων στα αντίστοιχα πεδία όπως παρουσιάζονται στον Πίνακα 2.

Πίνακας 2. Βασικές τιμές παραμέτρων ριζικής ΑΠ

ΠΑΡΑΜΕΤΡΟΙ	ΤΙΜΕΣ
Τύπος ΑΠ	X509
Τύπος πιστοποιητικού ΑΠ	Soft
Αλγόριθμος υπογραφής	SHA1WithRSA
Μήκος κλειδιού RSA	2048
Διάρκεια ισχύος πιστοποιητικού	7300d (20 χρόνια)
Subject DN (Διακριτικό Όνομα Υποκειμένου)	CN=AP1,O=UNIV,C=GR
Υπογράφεται από	Self Signed

Το πιστοποιητικό της νέας ριζικής ΑΠ με το όνομα AP1 παρουσιάζεται στην Εικόνα 14.



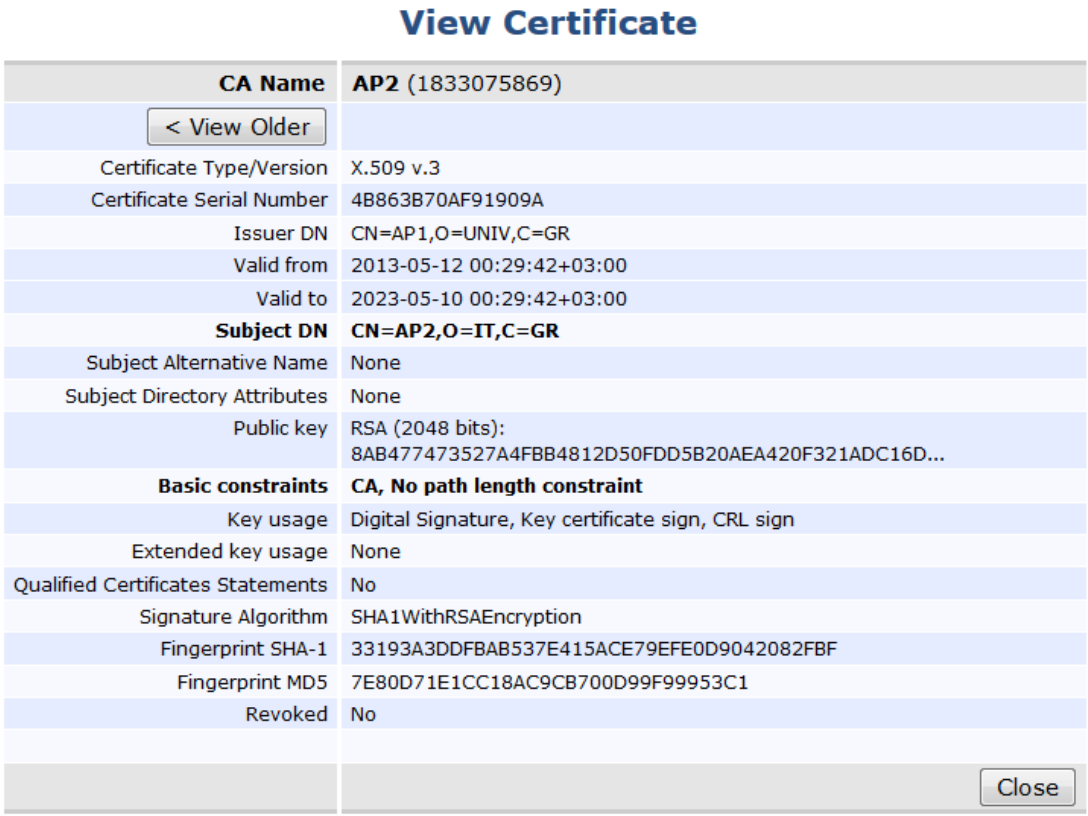
Εικόνα 14. Το ψηφιακό πιστοποιητικό της AP1

Με ανάλογο τρόπο, μέσα από το γραφικό διαχειριστικό περιβάλλον, δημιουργείται η υποκείμενη ΑΠ με το όνομα “AP2” και ορίζονται οι βασικές τιμές των παραμέτρων στα αντίστοιχα πεδία όπως παρουσιάζονται στον Πίνακα 3.

Πίνακας 3. Βασικές τιμές παραμέτρων υποκείμενης ΑΠ

ΠΑΡΑΜΕΤΡΟΙ	ΤΙΜΕΣ
Τύπος ΑΠ	X509
Τύπος πιστοποιητικού ΑΠ	Soft
Αλγόριθμος υπογραφής	SHA1WithRSA
Μήκος κλειδιού RSA	2048
Διάρκεια ισχύος πιστοποιητικού	3650d (10 χρόνια)
Subject DN (Διακριτικό Όνομα Υποκειμένου)	CN=AP2,O=IT,C=GR
Υπογράφεται από	CN=AP1,O=UNIV,C=GR

Το πιστοποιητικό της υποκείμενης ΑΠ με όνομα AP2 παρουσιάζεται στην Εικόνα 15.



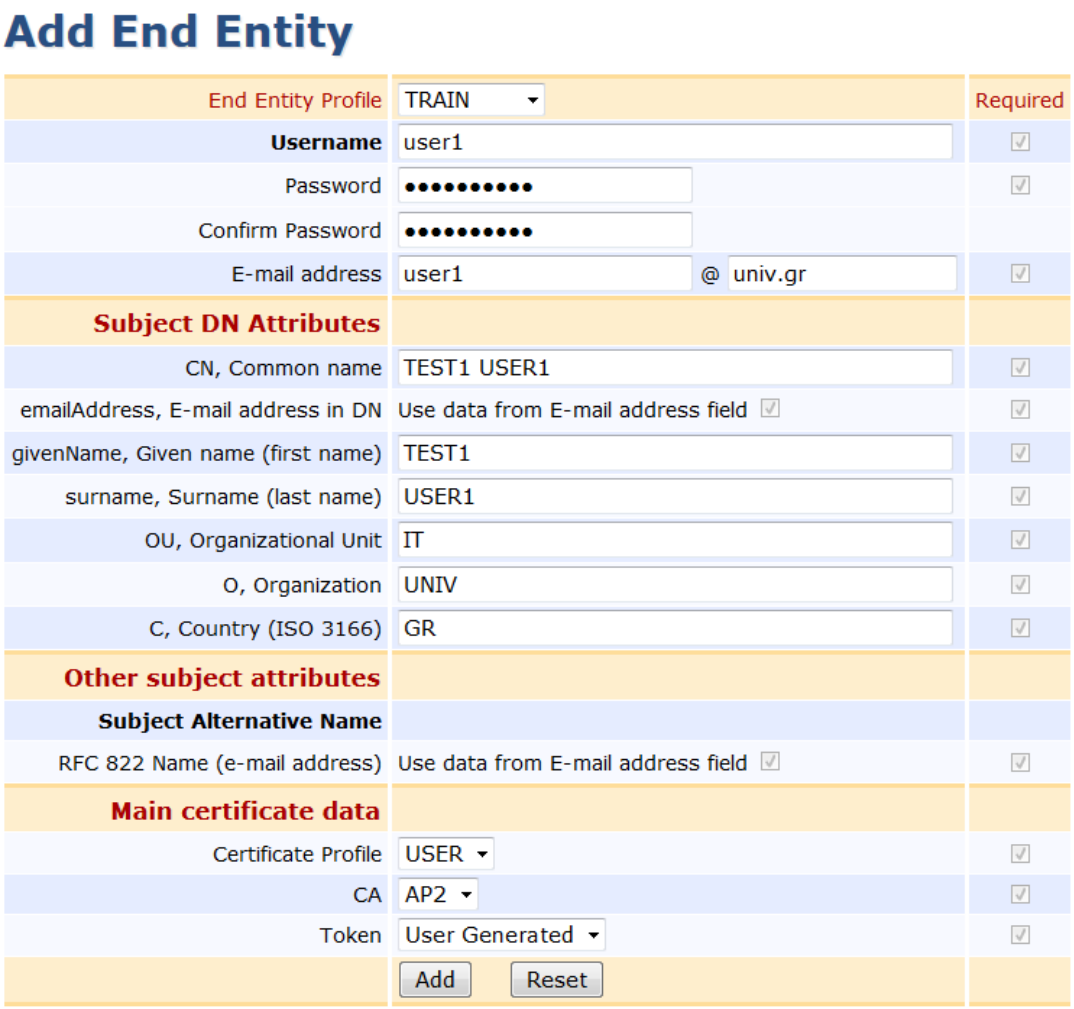
Εικόνα 15. Το ψηφιακό πιστοποιητικό της AP2

Μετά την ενεργοποίηση των αρχών πιστοποίησης, για τις ανάγκες υλοποίησης της ηλεκτρονικής υπηρεσίας υποβολής των εργασιών, θα πρέπει να ακολουθήσει η δημιουργία των προφίλ των ψηφιακών πιστοποιητικών τα οποία θα εκδίδονται από την υποκείμενη ΑΠ.

Η δημιουργία ενός νέου προφίλ πιστοποιητικού πραγματοποιείται μέσα από το γραφικό διαχειριστικό περιβάλλον με την επιλογή “Edit Certificate Profiles ”, τον ορισμό του ονόματος του προφίλ και την εκτέλεση της εντολής “Add” ή “Use selected as template” στην περίπτωση επιλογής ενός υφιστάμενου τύπου προφίλ. Το νέο προφίλ ονομάζεται “USER”.

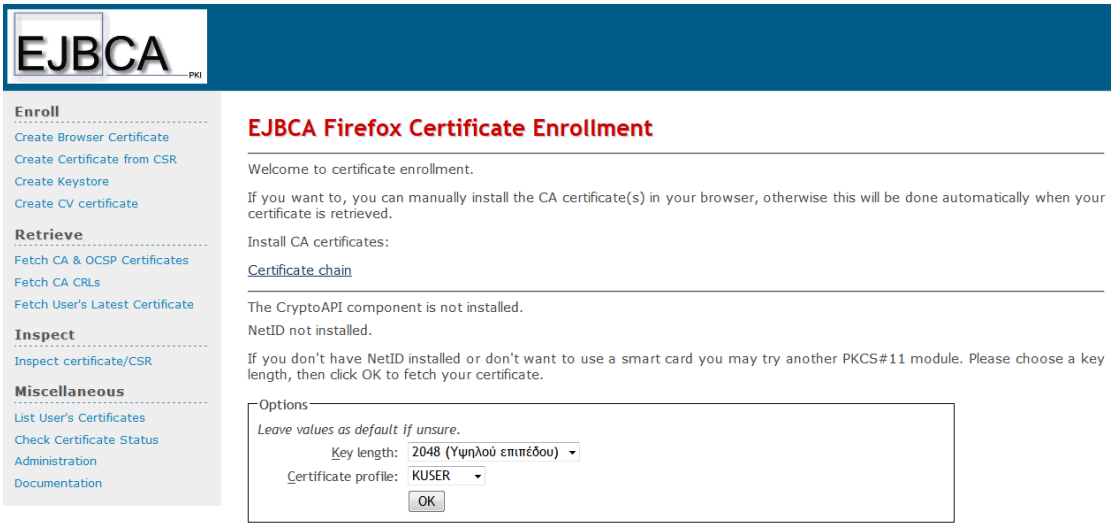
Επιπλέον, υπάρχει η δυνατότητα ορισμού προφίλ τελικών οντοτήτων με στόχο την ομαδοποίηση των χρηστών οι οποίοι χαρακτηρίζονται από κοινές ιδιότητες. Η δημιουργία ενός νέου προφίλ τελικής οντότητας υλοποιείται μέσα από το γραφικό διαχειριστικό περιβάλλον με την επιλογή “Edit End Entity Profiles”, τον ορισμό του ονόματος του προφίλ και την εκτέλεση της εντολής “Add” ή “Use selected as template” για την ενδεχόμενη επιλογή ενός υφιστάμενου τύπου προφίλ. Στην προκειμένη περίπτωση δημιουργείται το προφίλ με όνομα “TRAIN”.

Οι χρήστες δημιουργούνται μέσα από το γραφικό περιβάλλον διαχείρισης της εφαρμογής με την επιλογή “Add End Entity ”. Στη συνέχεια επιλέγεται το προφίλ τελικού χρήστη, το οποίο στη συγκεκριμένη περίπτωση είναι το “TRAIN” και συμπληρώνονται τα διαθέσιμα πεδία με τις κατάλληλες τιμές, όπως παρουσιάζεται στην Εικόνα 16.



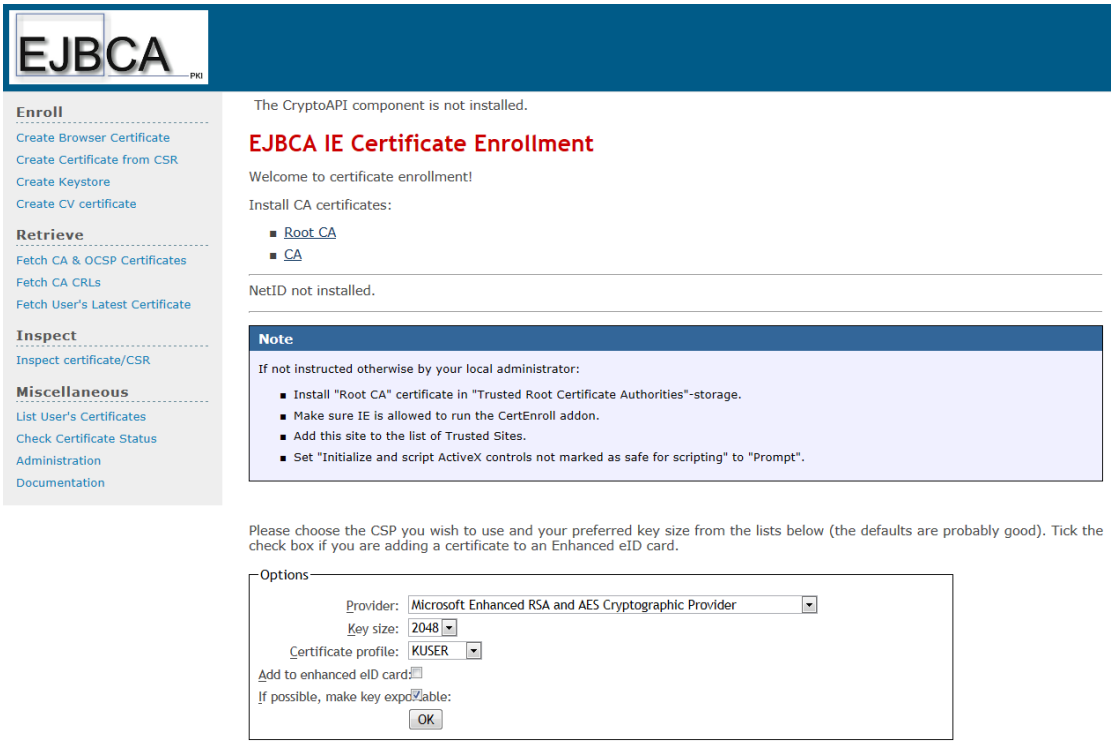
Εικόνα 16. Δημιουργία τελικού χρήστη

Ο τελικός χρήστης από τη δημόσια ιστοσελίδα της εφαρμογής EJBCA (Εικόνα 11) επιλέγει “Create Browser Certificate”, όπου του ζητείται να εισάγει όνομα χρήστη και κωδικό πρόσβασης. Μετά από την επιτυχημένη εξακρίβωση των στοιχείων, το πιστοποιητικό του μπορεί να εγκατασταθεί στον υπολογιστή. Στην Εικόνα 17 παρουσιάζεται η εγκατάσταση πιστοποιητικού σε Firefox.



Εικόνα 17. Εγκατάσταση πιστοποιητικού τελικού χρήστη σε Firefox

Στην Εικόνα 18 παρουσιάζεται η εγκατάσταση πιστοποιητικού σε Internet Explorer.



Εικόνα 18. Εγκατάσταση πιστοποιητικού τελικού χρήστη σε Internet Explorer

Ο τελικός χρήστης έχοντας εγκαταστήσει το ψηφιακό πιστοποιητικό στον υπολογιστή του είναι σε θέση να υπογράφει ψηφιακά και να κρυπτογραφεί ηλεκτρονικά έγγραφα.

Η ανάκληση ενός ψηφιακού πιστοποιητικού πραγματοποιείται μέσα από το γραφικό διαχειριστικό περιβάλλον με την επιλογή “Search End Entities”, αναζητώντας και επιλέγοντας τον χρήστη του οποίου το πιστοποιητικό θα πρέπει να ανακληθεί. Στη συνέχεια εκτελείται η εντολή “Revoke Selected” προσδιορίζοντας την αιτία ανάκλησης του πιστοποιητικού. Όταν εκδοθεί ο νέος ΚΑΠ θα περιέχει το σειριακό αριθμό του ανακληθέντος πιστοποιητικού.

Οι εφαρμογές λογισμικού προκειμένου να επικυρώσουν την εγκυρότητα των πιστοποιητικών, μπορούν να προσπελάσουν την υπηρεσία του OCSP πρωτοκόλλου μέσω διαδικτυακής σύνδεσης στο παρακάτω URL, όπου “server” είναι το όνομα του EJBCA εξυπηρετητή ή εναλλακτικά η IP διεύθυνσή του.

http://server:8080/ejbca/publicweb/status/ocsp

Επίσης, οι εφαρμογές που χρησιμοποιούν τους ΚΑΠ για τον έλεγχο εγκυρότητας των πιστοποιητικών, μπορούν να προσπελάσουν το σημείο διανομής των ΚΑΠ μέσω διαδικτυακής σύνδεσης στο παρακάτω URL, όπου “server” είναι το όνομα του EJBCA εξυπηρετητή ή εναλλακτικά η IP διεύθυνσή του.

http://server:8080/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=AP2,O=IT,C=GR

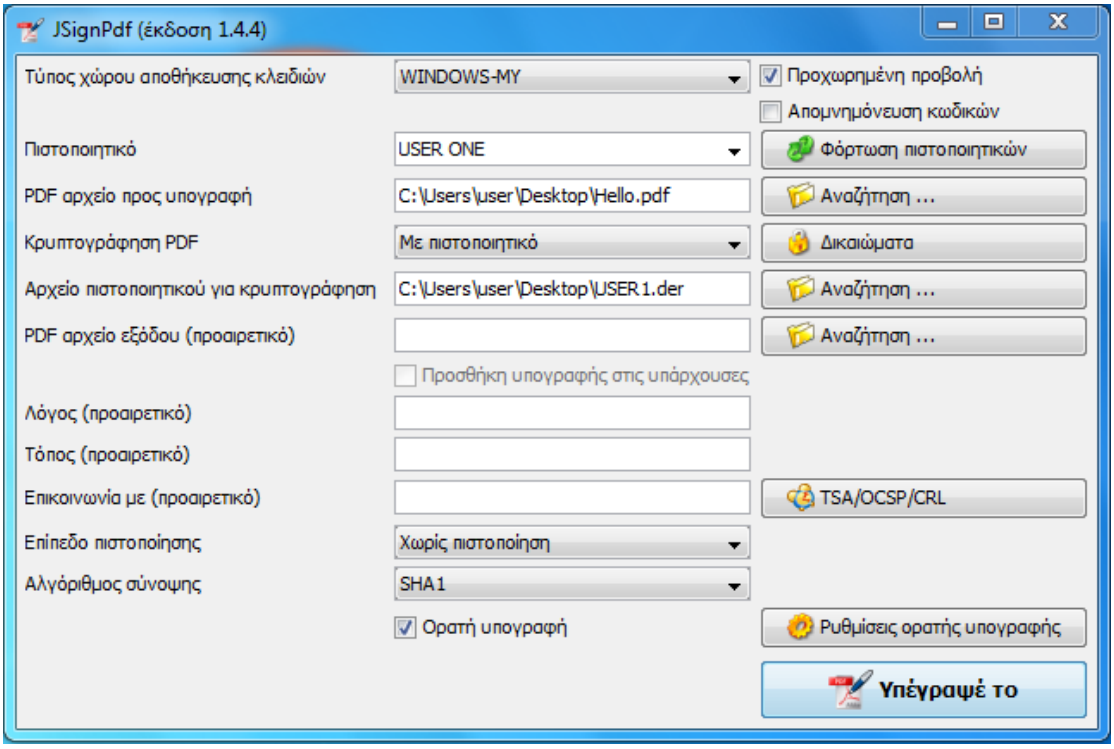
Η δημιουργία και η εγκατάσταση SSL ψηφιακών πιστοποιητικών για εξυπηρετητές είναι παρόμοια με τη δημιουργία πιστοποιητικών για τελικούς χρήστες.

4.5. Πρακτική Εφαρμογή

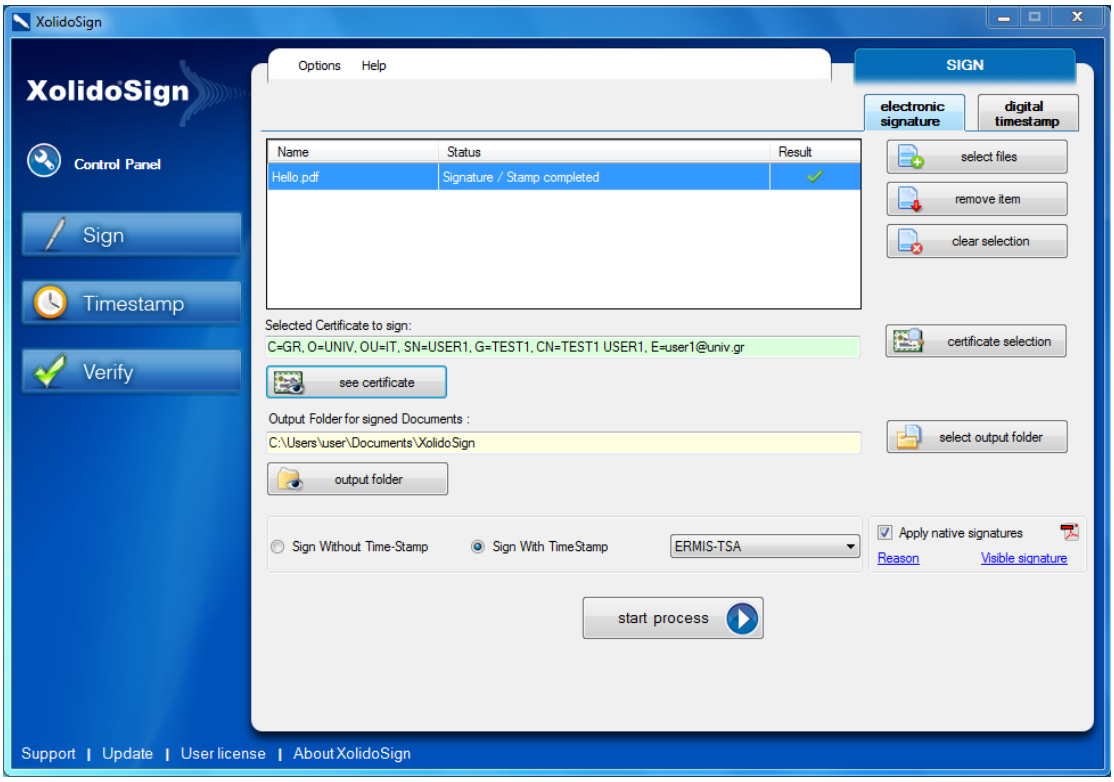
Οι δυνατότητες που έχει στη διάθεσή του ο τελικός χρήστης εξαρτώνται από εκείνες που του παρέχει η εκάστοτε εφαρμογή που χρησιμοποιεί. Αναλυτικότερα, η πρακτική αξιοποίηση και χρήση της ψηφιακής υπογραφής υποστηρίζεται από τις εφαρμογές αυτοματισμού γραφείου Microsoft Office [53], LibreOfice [54]και OpenOffice [55].

Η εφαρμογή επεξεργασίας pdf τύπου αρχείων Adobe Acrobat Pro [56] υποστηρίζει ψηφιακή υπογραφή και χρονοσήμανση. Η δωρεάν έκδοση Adobe Acrobat Reader υποστηρίζει την ανάγνωση ψηφιακά υπογεγραμμένων αρχείων με χρονοσήμανση. Αρχικά, θα πρέπει να γίνει η ρύθμιση “Ενοποίηση με Windows” (Windows Integration) μέσα από το μενού της εφαρμογής Adobe Acrobat.

Στην περίπτωση που ο χρήστης διαθέτει μόνο το λογισμικό Adobe Acrobat Reader, θα πρέπει να χρησιμοποιήσει μία επιπλέον εφαρμογή ανοιχτού κώδικα όπως για παράδειγμα τις JSignPDF [57], XolidoSign [58] και Sinadura [59], οι οποίες επιτρέπουν την προσθήκη ψηφιακής υπογραφής και χρονοσήμανσης σε pdf τύπου αρχεία. Η εφαρμογή JSignPdf για την ψηφιακή υπογραφή, χρονοσήμανση και κρυπτογράφηση ενός αρχείου τύπου pdf παρουσιάζεται στην Εικόνα 19. Η εφαρμογή XolidoSign για χρήση ψηφιακής υπογραφής και χρονοσήμανσης παρουσιάζεται στην Εικόνα 20.



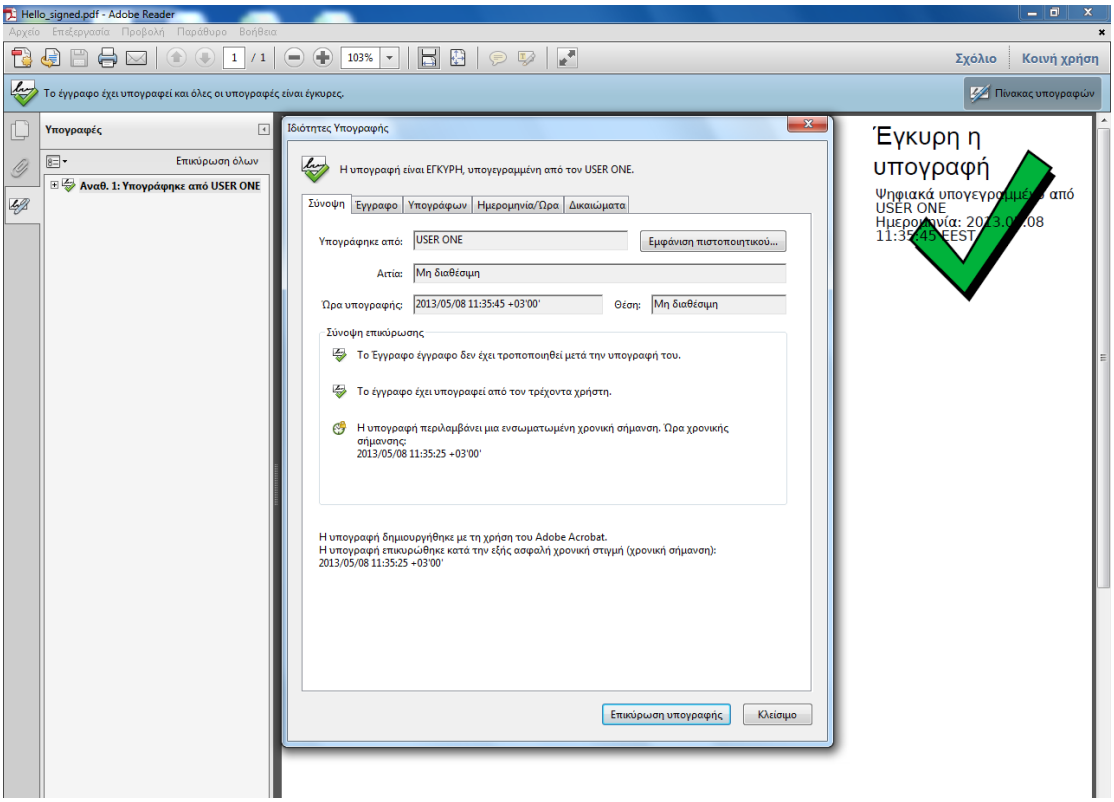
Εικόνα 19. Η εφαρμογή JSignPdf



Εικόνα 20. Η εφαρμογή XolidoSign

Η χρήση των ψηφιακών πιστοποιητικών στο ηλεκτρονικό ταχυδρομείο εξαρτάται από τις δυνατότητες που παρέχει η εκάστοτε εφαρμογή. Για παράδειγμα το λογισμικό Microsoft Outlook υποστηρίζει τη χρήση ψηφιακής υπογραφής και κρυπτογράφησης. Προϋπόθεση για την επίτευξη εμπιστευτικότητας στα απεσταλμένα μηνύματα, είναι η εγκατάσταση στις "Επαφές" του δημόσιου κλειδιού κρυπτογράφησης του παραλήπτη.

Η ψηφιακή υπογραφή μπορεί να γίνει ορατή με την επιλογή της κατάλληλης ρύθμισης. Η εφαρμογή Adobe Acrobat Reader μπορεί να χρησιμοποιηθεί για την προβολή ενός αρχείου τύπου pdf ψηφιακά υπογεγραμμένο με χρονοσήμανση, από την εφαρμογή JSignPdf έχοντας επιλέξει τη δυνατότητα ρύθμισης ορατής υπογραφής και την επιλογή θέσης εμφάνισης πάνω στο έγγραφο, όπως παρουσιάζεται στην Εικόνα 20.



Εικόνα 20. Η εφαρμογή Adobe Acrobat Reader

Αναφορικά με την απαίτηση ασφάλειας περί μη αποποίησης, θα πρέπει να επιλεγεί μία Αρχή Χρονοσήμανσης η οποία να αντιστοιχίζει ένα ηλεκτρονικό αρχείο με μια συγκεκριμένη χρονική στιγμή και να εγγυάται την ακρίβεια της χρονικής στιγμής και της αντιστοίχισης. Αναλυτικότερα, ο Πάροχος Υπηρεσιών Χρονοσήμανσης (ΠΥΧ) θα πρέπει να διασφαλίζει τη χρήση αξιόπιστης πηγής ώρας και την κατάλληλη διαχείριση των συστημάτων χρονοσήμανσης.

Επίσης θα πρέπει να εγγυάται την οργάνωση της υποδομής και την έκδοση χρονοσημάνσεων. Η διαδικασία χρονοσήμανσης θα πρέπει να χρησιμοποιεί το Συντονισμένο Παγκόσμιο Χρόνο (Coordinated Universal Time – UTC), δηλαδή τη χρονική κλίμακα με βάση το δευτερόλεπτο όπως ορίζεται αναλυτικά στη σύσταση ITU-R TF.460-5. Η μέγιστη απόκλιση από το ρολόι της πηγής θα πρέπει να είναι ένα (1) δευτερόλεπτο και η παρεχόμενη προς τους χρήστες χρονοσήμανση να περιλαμβάνει την απαραίτητη προσαύξηση κατά 2 ώρες έτσι ώστε να είναι σύμφωνα με τη χρονική ζώνη της Ελλάδας.

Η Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ) παρέχει υπηρεσίες χρονοσήμανσης με σκοπό τη δημιουργία των απαραίτητων τεκμηρίων για την ύπαρξη ενός συνόλου ψηφιακών δεδομένων σε μία συγκεκριμένη χρονική στιγμή [60]. Το κλειδί επαλήθευσης της υπογεγραμμένης χρονοσήμανσης παρέχεται μέσω ψηφιακού πιστοποιητικού. Τα πιστοποιητικά των συστημάτων της χρονοσήμανσης είναι δημοσιευμένα από την ΑΠΕΔ στον σχετικό κατάλογο και μπορεί να επαληθευτεί η εγκυρότητα τους σε σχέση με την παραχθείσα χρονοσήμανση του ηλεκτρονικού εγγράφου [60]. Το πιστοποιητικό παράγεται σύμφωνα με το πρότυπο X.509 v3. Οι χρονοσημάνσεις παράγονται από την ΥΔΚ της ΑΠΕΔ μέσω του συνδέσμου TSA URL http://timestamp.ermis.gov.gr/TSS/HttpTspServer και με Προσδιοριστή Αντικειμένου OID Policy: (1.3.6.1.4.1.601.10.3.1).

Το Ελληνικό Ινστιτούτο Μετρολογίας (ΕΙΜ) παρέχει επίσης παρέχει υπηρεσίες χρονοσήμανσης ηλεκτρονικών εγγράφων με βάση τον Εθνικό Χρόνο [62]. Οι χρονοσημάνσεις παράγονται μέσω του συνδέσμου TSA URL http://79.129.72.249/tsa από εξυπηρετητές χρονοσήμανσης που φιλοξενούνται στην υποδομή του ΕΔΕΤ [63], εξασφαλίζοντας υψηλή απόδοση και διαθεσιμότητα.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η παρούσα διπλωματική εργασία αποτελεί μία ολοκληρωμένη ανάλυση του αντικειμένου Υποδομές Δημόσιου Κλειδιού (Public Key Infrastructures) σε επιστημονικό, επιχειρησιακό και τεχνικό επίπεδο. Επιτεύχθηκε μία κριτική ανασκόπηση της επιστημονικής βιβλιογραφίας και αποτυπώθηκαν οι σύγχρονες συναφείς τεχνικές προδιαγραφές και πρότυπα.

Η διεξοδική επιχειρησιακή ανάλυση του αρχιτεκτονικού μοντέλου PKIX οδήγησε στο να προσδιορισθούν τα πλεονεκτήματα, τα μειονεκτήματα, οι ευκαιρίες και οι απειλές, καθώς και οι κρίσιμοι παράγοντες επιτυχίας των ΥΔΚ ευρείας κλίμακας για την παροχή προηγμένων ηλεκτρονικών υπηρεσιών προστιθέμενης αξίας. Συγκεκριμένα, οι κρίσιμοι παράγοντες επιτυχίας μίας ΥΔΚ είναι η δέσμευση της ηγεσίας, το ισχυρό νομικό πλαίσιο, η επίγνωση των χρηστών, το επιχειρησιακό μοντέλο, η οργανωτική δομή, η τεχνική υλοποίηση και η τεχνογνωσία των εμπειρογνωμόνων που θα κληθούν να αναπτύξουν και να λειτουργήσουν την υποδομή.

Η αξία μίας ΥΔΚ είναι ανάλογη των ηλεκτρονικών υπηρεσιών που παρέχει στους τελικούς χρήστες. Το σημαντικό όφελος μίας ΥΔΚ βρίσκεται στην προστιθέμενη αξία της ηλεκτρονικής υπηρεσίας που αντιλαμβάνεται ο τελικός χρήστης και όχι στο ίδιο το ψηφιακό πιστοποιητικό. Γενικότερα, οι όποιες δυσκολίες παρουσιάζονται από την πλευρά της ΥΔΚ είναι πάντοτε εφικτό να επιλυθούν, εφόσον τα πληροφοριακά συστήματα υποστηρίζουν τα αναγνωρισμένα διεθνή τεχνικά πρότυπα και ακολουθηθούν οι ορθές διαδικασίες εγκατάστασης, παραμετροποίησης και διαχείρισης των εφαρμογών. Τα αληθινά προβλήματα εμφανίζονται από την πλευρά του τελικού χρήστη. Η ασφάλεια δεν αποτελεί συνήθως πρώτη προτεραιότητα για την ανάπτυξη του λογισμικού, με αποτέλεσμα οι περισσότερες εφαρμογές να χαρακτηρίζονται από ελλιπή υλοποίηση των κρυπτογραφικών μηχανισμών και να μην υποστηρίζουν πλήρως το μοντέλο PKIX.

Επιπλέον, οι χρήστες δεν έχουν πλήρη επίγνωση της ασφάλειας, δυσκολεύονται να κατανοήσουν τις μεθόδους προστασίας και δεν τους παρέχεται η κατάλληλη φιλική καθοδήγηση από το γραφικό περιβάλλον των εφαρμογών. Συνεπώς, η μελλοντική επιτυχία των ΥΔΚ εξαρτάται από το βαθμό ενσωμάτωσής τους στις εφαρμογές λογισμικού, την ευαισθητοποίηση των χρηστών στα θέματα ασφάλειας της πληροφορίας, καθώς και από την πληρότητα και ποιότητα των προγραμμάτων εκπαίδευσης και επιμόρφωσης στα οποία θα συμμετέχουν. Άλλωστε, θα πρέπει να σημειωθεί ότι έως σήμερα δεν υπάρχει κάποια καλύτερη εναλλακτική λύση των ΥΔΚ. Η τεχνική υλοποίηση μίας ολοκληρωμένης ΥΔΚ και η εκπόνηση της μελέτης περίπτωσης, επιβεβαιώνουν την ορθότητα των ανωτέρω συμπερασμάτων.

Προτάθηκε μία τεχνική μάθησης η οποία προβλέπει την εκπόνηση εργασιών βασισμένες σε σενάρια παροχής ηλεκτρονικών υπηρεσιών που περιλαμβάνουν την ανάλυση των απαιτήσεων ασφάλειας, τον προσδιορισμό και τεκμηρίωση των κατάλληλων πολιτικών πιστοποιητικών, τη σχεδίαση, καθώς και την πρακτική υλοποίηση της ΥΔΚ που θα υποστηρίζει την παροχή της υπηρεσίας.

Η υλοποίηση της εκπαιδευτικής πρότασης επιτεύχθηκε με την εγκατάσταση ενός ολοκληρωμένου εργαστηριακού περιβάλλοντος εκπαίδευσης και εργασίας για τη σχεδίαση, ανάπτυξη, διαχείριση και λειτουργία μίας ΥΔΚ μέσω ενός γραφικού περιβάλλοντος προσομοίωσης. Η προτεινόμενη εκπαιδευτική προσέγγιση έχει το πλεονέκτημα ότι επιτρέπει την αφομοίωση και την εφαρμογή της θεωρίας στην πράξη, παρέχοντας τη δυνατότητα στους σπουδαστές να εξοικειωθούν με τις έννοιες της εφαρμοσμένης ασύμμετρης κρυπτογραφίας. Η ανάπτυξη της ΥΔΚ για εκπαιδευτικούς σκοπούς ολοκληρώθηκε χρησιμοποιώντας λογισμικό ανοιχτού κώδικα, στοχεύοντας στην κατανόηση του αρχιτεκτονικού μοντέλου PKIX, των εφαρμογών της

κρυπτογραφίας δημόσιου κλειδιού, στη διαχείριση των ψηφιακών πιστοποιητικών και ειδικότερα στην πρακτική χρήση των ψηφιακών υπογραφών και της χρονοσήμανσης.

Εκπονήθηκε μία μελέτη περίπτωσης η οποία αφορά την ανάπτυξη μίας ιεραρχικής ΥΔΚ με στόχο τη διαχείριση του κύκλου ζωής των ψηφιακών πιστοποιητικών, τα οποία θα διατίθενται στα μέλη ΔΕΠ και στους φοιτητές ενός πανεπιστημίου για την υποστήριξη της ηλεκτρονικής υπηρεσίας υποβολής των εργασιών στο πλαίσιο των μαθημάτων. Εξετάσθηκαν οι απαιτήσεις ασφάλειας και αναλύθηκαν οι διαδικασίες εγγραφής και χρήσης της ηλεκτρονικής υπηρεσίας.

Η μελέτη περίπτωσης αποτέλεσε την αξιολόγηση και έλεγχο του εργαστηριακού περιβάλλοντος εκπαίδευσης και εργασίας, επικυρώνοντας την πλήρη συμμόρφωση του συστήματος με τις αρχικές λειτουργικές απαιτήσεις της ΥΔΚ. Επίσης, η μελέτη περίπτωσης επιβεβαίωσε την ορθότητα των συμπερασμάτων της επιχειρησιακής ανάλυσης. Τέλος, δοκιμάσθηκαν και προτάθηκαν διάφορες εφαρμογές αυτοματισμού γραφείου ανοιχτού λογισμικού για την πρακτική αξιοποίηση και χρήση των ψηφιακών πιστοποιητικών.

6. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Diffie W. and Hellman M.E., "New Directions in Cryptography". IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp. 644-654, November 1976.

[2] Kohnfelder L. M.," Towards a Practical Public Key Cryptosystem". Bachelor's thesis, Dept. Electrical Engineering, MIT, Cambridge, Mass., May 1978.

[3] ITU-T, "The Directory - overview of concepts, models and service". International Telecommunications Union, X.500 series of Recommendations, 1993.

[4] Rivest R.L., Shamir A., and Adleman L., "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120-126, February 1978.

[5] William Stallings, "Network Security Essentials: Applications and Standards" Fourth Edition, Prentice Hall, 2011.

[6] Cooper D. et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". IETF RFC 5280, May 2008. www.ietf.org/rfc/rfc5280.txt

[7] Stephen Farrell, "Not Reinventing PKI until We Have Something Better" IEEE Internet Computer, Volume 15, Issue 5, pp. 95 – 98, Sept. – Oct. 2011.

[8] Shirey R., "Internet Security Glossary, Version 2". IETF RFC 4949, August 2007. http://www.ietf.org/rfc/rfc4949.txt

[9] Andrew S. Tanenbaum, "Δίκτυα Υπολογιστών" Τέταρτη Αμερικανική Έκδοση, Κλειδάριθμος, 2003.

[10] Άρης Αλεξόπουλος και Γιώργος Λαγογιάννης, "Τηλεπικοινωνίες και Δίκτυα Υπολογιστών" Έκτη Έκδοση, 2003.

[11] Adams C., Farrell S., Kause T. and Mononen T., "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)". IETF RFC 4210, September 2005. http://www.ietf.org/rfc/rfc4210.txt

[12] Schaad J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)". IETF RFC 4211, September 2005. http://www.ietf.org/rfc/rfc4211.txt

[13] Schaad J. and Myers M., "Certificate Management over CMS (CMC)". IETF RFC 5272, June 2008. http://www.ietf.org/rfc/rfc5272.txt

[14] Housley R., "Cryptographic Message Syntax (CMS)". IETF RFC 5652, September 2009. http://www.ietf.org/rfc/rfc5652.txt

[15] Myers M., Ankney R., Malpani A. and Adams C., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP". IETF PKIX WG, RFC 2560, June 1999. http://www.ietf.org/rfc/rfc2560.txt

[16] Chokhani S., Ford W., Sabett R., Merrill C. and Wu S., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". IETF RFC 3647, November 2003. http://www.ietf.org/rfc/rfc3647.txt

[17] Τεχνική προδιαγραφή ETSI TS 101 456 V1.4.3 (2007-05), "Electronic Signatures and Infrastructures (ESI), Policy requirements for certification authorities issuing qualified certificates".

[18] Τεχνική προδιαγραφή ETSI TS 101 862 V1.3.3 (2006-01), "Qualified Certificate profile".

[19] Τεχνική προδιαγραφή ETSI TS 102 023 V1.2.2 (2008-10), "Electronic Signatures and Infrastructures (ESI), Policy requirements for time-stamping authorities".

[20] Pinkas D., et al., "Policy Requirements for Time-Stamping Authorities (TSAs)". IETF PKIX WG, RFC 3628, November 2003.

[21] Τεχνική προδιαγραφή ETSI TS 101 861 V1.4.1 (2011-07) "Electronic Signatures and Infrastructures (ESI), Time stamping profile".

[22] Adams, C., et al., "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)". IETF PKIX WG, RFC 3161, August 2001. http://www.ietf.org/rfc/rfc3161.txt

[23] Shimaoka, et al., "Memorandum for Multi-Domain Public Key Infrastructure Interoperability". IETF RFC 5217, July 2008. http://www.ietf.org/rfc/rfc5217.txt

[24] Lekkas D., "Establishing and managing trust within the public key infrastructure". Elsevier, Computer Communications, Volume 26, Issue 16, pp. 1815–1825, October 2003.

[25] Lancaster S., Yena D.C. and Huang S.-M., "Public key infrastructure: a micro and macro analysis". Elsevier, Computer Standards & Interfaces, Volume 25, Issue 5, pp. 437–446, September 2003.

[26] Gutmann P., "PKI: It's Not Dead, Just Resting". IEEE Computer, August 2002.

[27] Ellison C. and Schneier B., "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure". Computer Security Journal, Volume XVI, No. 1, 2000.

[28] Adams, C., and S. Lloyd, "Understanding PKI: Concepts, Standards and Deployment Considerations, 2nd ed., Addison-Wesley, 2005.

[29] Lambrinoudakis C., Gritzalis S., Dridi F., Pernul G., "Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy". Elsevier, Computer Communications, Volume 26, Issue 16, pp. 1873–1883, October 2003.

[30] Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές. Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων, 19. 1. 2000.

[31] Patsos D., Ciechanowicz C., Piper F.," The status of National PKIs – A European overview". Elsevier, Information Security Technical Report, Volume 15, Issue 1, pp. 13–20, February 2010.

[32] Gritzalis S., "A good-practice guidance on the use of PKI services in the public sector of the European Union member states". Information Management & Computer Security, Vol. 13 Issue. 5, pp. 379 – 398, 2005.

[33] Lopez J., Oppliger R. and Pernul G., "Why have Public Key Infrastructures failed so far?". Internet Research, Vol. 15, Issue 5, pp. 544-556, 2005. Emerald, Bradford, England.

[34] Lioy A., Marian M., Moltchanova N. and Pala M., "PKI past, present and future". International Journal of Information Security, Springer-Verlag, Volume 5, Issue 1, pp. 18-29, January 2006.

[35] Camenisch J. and Lambrinoudakis C. (Eds.), "Public Key Infrastructures, Services and Applications". Springer, 7th European Workshop, EuroPKI 2010, Athens, Greece, September 23-24, 2010.

[36] Zissis, D., Lekkas, D. & Koutsabasis, P. "Cryptographic Dysfunctionality-A Survey on User Perceptions of Digital Certificates", In the 7th ICGS3 / 4th e-Democracy Joint Conferences 2011, Thessaloniki, Greece, August 2011.

[37] Η εφαρμογή EJBCA PKI. http://www.ejbca.org/

[38] Zhang, L., Liu, Q., Xu, M., 2007, in IFIP International Federation for Information Processing, Volume 251, Integration and Innovation Orient to E-Society Volume 1, Wang, W. (Eds), (Boston: Springer), pp. 337-345.

[39] Πρότυπο ITU-T X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. http://www.itu.int/rec/T-REC-X.509-200508-I/en

[40] Τεχνική Οδηγία BSI TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI).

[41] Έγγραφο RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP. http://tools.ietf.org/pdf/rfc2560.pdf

[42] Το πρωτόκολλο OCSP. The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments. http://tools.ietf.org/pdf/rfc5019.pdf

[43] Έγγραφο RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. http://tools.ietf.org/pdf/rfc5280.pdf

[44] Επίσημη ιστοσελίδα της εταιρίας PrimeKey. http://www.primekey.se/

[45] Oracle Data Sheet, "ORACLE VM VIRTUALBOX". Διαθέσιμο (1/4/2013) στο: http://www.oracle.com/us/technologies/virtualization/oraclevm/oracle-vm-virtualbox-ds-1655169.pdf

[46] Λειτουργικό σύστημα Linux Ubuntu έκδοση 12.04.2 – desktop – amd64. http://www.ubuntu.com/download/desktop

[47] Λειτουργικό σύστημα Linux Ubuntu έκδοση 12.04.2 – server – amd64. http://www.ubuntu.com/download/server

[48] FTP server. Very Secure FTP Daemon. https://security.appspot.com/vsftpd.html

[49] Λογισμικό ανοιχτού κώδικα PuTTY, SSH και telnet client. http://www.putty.org/

[50] EJBCA Enterprise PKI CA. http://ejbca.sourceforge.net/

[51] Wiki – EJBCA Open Source Enterprise PKI. http://wiki.ejbca.org/start

[52] Mozilla Firefox. Πρόγραμμα περιήγησης ιστού σε λογισμικό ανοιχτού κώδικα. http://www.mozilla.org/el/firefox/fx/

[53] Εφαρμογή αυτοματισμού γραφείου Microsoft Office. http://www.microsoft.com

[54] Εφαρμογή αυτοματισμού γραφείου LibreOffice. https://el.libreoffice.org/

[55] Εφαρμογή αυτοματισμού γραφείου OpenOffive. http://www.openoffice.org/el/

[56] Εφαρμογή Adobe Acrobat. http://www.adobe.com/products/acrobat.html

[57] Εφαρμογή ψηφιακής υπογραφής JSignPdf. http://jsignpdf.sourceforge.net/

[58] Εφαρμογή ψηφιακής υπογραφής XolidoSign. http://www.en.xolido.com/

[59] Εφαρμογή ψηφιακής υπογραφής Sinadura. http://www.sinadura.net/en/inicio

[60] Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ). http://www.yap.gov.gr/

[61] Χώρος Αποθήκευσης Υποδομής Δημοσίου Κλειδιού ΕΡΜΗΣ (Repository). https://pki.ermis.gov.gr/repository.html

[62] Εθνικός Χρόνος από το Ελληνικό Ινστιτούτο Μετρολογίας. http://time.eim.gr/

[63] Εθνικό Δίκτυο Έρευνας & Τεχνολογίας. http://www.grnet.gr/