Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ασφάλεια Πληροφοριών σε Περιβάλλοντα η-Μάθησης – SWBES: Μελέτη Περίπτωσης η-Εξετάσεων μέσω Ιστού**
Ονοματεπώνυμο	**Δημήτριος Παράς του Γερασίμου**
Αριθμός Μητρώου	**ΜΠΣΠ/ 09045**
Κατεύθυνση	**Δικτυοκεντρικά Πληροφοριακά Συστήματα**
Επιβλέπουσα	**Δέσποινα Πολέμη, Επίκουρος Καθηγήτρια**

Ημερομηνία Παράδοσης **Οκτώβριος 2012**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Δέσποινα Πολέμη Επίκουρος Καθηγήτρια	Μαρία Βίρβου Καθηγήτρια	Παναγιώτης Κοτζανικολάου Λέκτορας

Ευχαριστιες

Θα ήθελα να εκφράσω τις θερμότερες ευχαριστίες μου στην Επίκουρη Καθηγήτρια Κα Δέσποινα Πολέμη, για την πολύτιμη επιστημονική καθοδήγηση, την υπομονή και το ενδιαφέρον που επέδειξε καθ'όλη τη διάρκεια της εκπόνησης της εργασίας και θα ήθελα να της εκφράσω την ευγνωμοσύνη μου για τη βοήθεια που μου προσέφερε αφιερώνοντας πολλές ώρες από τον προσωπικό της χρόνο.

Επίσης θα ήθελα να εκφράσω την ευγνωμοσύνη μου και να πω ένα μεγάλο ευχαριστώ στους γονείς μου, τον αδερφό μου και την Άντρεα για την υπομονή και την καθημερινή στήριξη που μου προσέφεραν απλόχερα όλο αυτό τον καιρό.

Περιληψη

Η ανάγκη για απεριόριστη πρόσβαση στη πληροφορία και τη γνώση μέσω Διαδικτύου, έχει οδηγήσει το παραδοσιακό σύστημα ανταλλαγής γνώσης να υποστηρίζεται από ένα σύστημα βασισμένο σε τεχνολογίες πληροφοριών και επικοινωνιών. Αυτό έχει ως αποτέλεσμα, ο παραδοσιακός τρόπος μάθησης να αλληλοσυμπληρώνεται με την ηλεκτρονική μάθηση (η-μάθηση) σύμφωνα με την οποία τα μαθησιακά αντικείμενα διανέμονται σε απομακρυσμένους εκπαιδευόμενους μέσω των δικτύων υπολογιστών. Το τεχνολογικό μέσο της απομακρυσμένης πρόσβασης στη μάθηση αποτελούν τα Συστήματα η-Μάθησης και πιο συγκεκριμένα τα Σύστημα Διαχείρισης Ηλεκτρονικής Μάθησης (ΣΔΗΜ).

Λαμβάνοντας υπόψη ότι ένα ΣΔΗΜ βασίζεται στις τεχνολογίες πληροφοριών και επικοινωνιών, οι απειλές ασφάλειας πολλαπλασιάζονται με αποτέλεσμα το σύστημα να γίνεται ευάλωτο και ο κίνδυνος ασφάλειας να οδηγεί στην ανάγκη λήψης αντιμέτρων με στόχο την αποτελεσματική άμυνα του συστήματος απέναντι στις απειλές αυτές. Σε αντίθεση με την ευρεία αποδοχή των ΣΔΗΜ, οι απαιτήσεις ασφάλειας και ιδιωτικότητας δε λαμβάνονται σοβαρά υπόψη, με τις περισσότερες καινοτομίες να επικεντρώνονται στην ανάπτυξη και διανομή του περιεχομένου.

Μελετώντας την πολυδιάστατη φύση των συστημάτων η-μάθησης, στο πλαίσιο της διατριβής, θα παρουσιαστούν τα λειτουργικά χαρακτηριστικά των ΣΔΗΜ και θα αναλυθεί η δραστηριότητα των διαφορετικών χρηστών του συστήματος (Διαχειριστής, Εκπαιδευτής, Εκπαιδευόμενος) εστιάζοντας στις απειλές ασφάλειας που αντιμετωπίζουν. Το Moodle (Modular Object-Oriented Dynamic Learning Environment) θα αποτελέσει μέρος της έρευνας ως ένα χαρακτηριστικό παράδειγμα ΣΔΗΜ ανοιχτού κώδικα. Τα περισσότερα ΣΔΗΜ της αγοράς υλοποιούν διάφορους μηχανισμούς ασφάλειας χωρίς όμως να ακολουθούν κάποιο πρότυπο ασφάλειας πληροφοριών. Στο πλαίσιο της διατριβής προτείνεται ένα **Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών**, βασισμένο στο πρότυπο του Διεθνούς Οργανισμού Προτυποποίησης (ISO) 27002, το οποίο αποτελεί έναν οδηγό υλοποίησης ασφάλειας σε Περιβάλλοντα η-Μάθησης.

Η ασφάλεια κατά τη διαδικασία αξιολόγησης ενός εκπαιδευόμενου σε ένα περιβάλλον η-μάθησης χρίζει ολοκληρωμένου σχεδίου αντιμετώπισης καθώς πρόκειται για την πιο κρίσιμη υπηρεσία που προσφέρεται σε ένα σύστημα η-μάθησης. Για τους σκοπούς της διατριβής προτείνεται μια **Αρχιτεκτονική Ασφαλών Ηλεκτρονικών Εξετάσεων** (η-Εξετάσεων), μια υπηρεσία ασφαλών ηλεκτρονικών εξετάσεων μέσω ιστού προσβάσιμη μέσα από ένα ΣΔΗΜ όπως το Moodle, με στόχο ένα ολιστικό, ευέλικτο και επεκτάσιμο μοντέλο ασφαλούς αξιολόγησης εκπαιδευόμενων το οποίο μπορεί να εφαρμοστεί σε οποιοδήποτε ΣΔΗΜ.

Το **SWBES (Secure Web-Based Exam System)** αποτελεί τον πυρήνα της Αρχιτεκτονικής Ασφαλών η-Εξετάσεων το οποίο υλοποιεί τη διαδικασία ασφαλούς αξιολόγησης εκπαιδευόμενου υιοθετώντας προτεινόμενα αντίμετρα ασφάλειας του Σχεδίου Πολιτικής Ασφάλειας. Επίσης αποτελεί τη διεπαφή εξέτασης στην οποία η πρόσβαση γίνεται μέσα από ένα ΣΔΗΜ όπως το Moodle.

Στο τέλος γίνεται αξιολόγηση της ασφάλειας της Αρχιτεκτονικής Ασφαλών η-Εξετάσεων και του SWBES εφαρμόζοντας το Σχέδιο Πολιτικής Ασφάλειας και συγκρίνοντας τους μηχανισμούς ασφάλειας της Αρχιτεκτονικής με τους εξ'ορισμού μηχανισμούς του Moodle.

Περιεχομενα

Περιεχομενα Σχηματων

Περιεχομενα Εικονων

Περιεχομενα Πινακων

Εισαγωγή

Η ανάγκη για απεριόριστη πρόσβαση στη πληροφορία και τη γνώση μέσω Διαδικτύου, έχει οδηγήσει το παραδοσιακό σύστημα ανταλλαγής γνώσης να υποστηρίζεται από ένα σύστημα βασισμένο σε τεχνολογίες πληροφοριών και επικοινωνιών. Αυτό έχει ως αποτέλεσμα, ο παραδοσιακός τρόπος μάθησης να αλληλοσυμπληρώνεται με την ηλεκτρονική μάθηση (η-μάθηση) σύμφωνα με την οποία τα μαθησιακά αντικείμενα διανέμονται σε απομακρυσμένους εκπαιδευόμενους μέσω των δικτύων υπολογιστών. Το τεχνολογικό μέσο της απομακρυσμένης πρόσβασης στη μάθηση αποτελούν τα Συστήματα η-Μάθησης, Σύστημα Διαχείρισης Ηλεκτρονικής Μάθησης (ΣΔΗΜ) και Σύστημα Διαχείρισης Περιεχομένου Ηλεκτρονικής Μάθησης (ΣΔΠΗΜ). Τα ΣΔΠΗΜ τείνουν να αποτελούν υποσύνολο των ΣΔΗΜ καθώς λειτουργικά χαρακτηριστικά των ΣΔΠΗΜ υιοθετούνται στα ΣΔΗΜ. Επομένως, για τις ανάγκες της διατριβής, η έννοια των συστημάτων η-μάθησης αντιστοιχίζεται καθολικά με τα ΣΔΗΜ. Ένα περιβάλλον η-μάθησης είναι ένα υπερσύνολο το οποίο περιλαμβάνει εκτός από το ΣΔΗΜ, τους χρήστες και τη συνεργατικότητα που αναπτύσσεται μεταξύ τους σε ένα τέτοιο σύστημα.

Λαμβάνοντας υπόψη ότι ένα ΣΔΗΜ βασίζεται στις τεχνολογίες πληροφοριών και επικοινωνιών, οι απειλές ασφάλειας πολλαπλασιάζονται με αποτέλεσμα το σύστημα να γίνεται ευάλωτο και ο κίνδυνος ασφάλειας να οδηγεί στην ανάγκη λήψης αντιμέτρων με στόχο την αποτελεσματική άμυνα του συστήματος απέναντι στις απειλές αυτές. Τα περισσότερα ΣΔΗΜ της αγοράς υλοποιούν διάφορους μηχανισμούς ασφάλειας χωρίς όμως να αντιμετωπίζουν τα κρίσιμα θέματα ασφάλειας.

Στόχος του κεφαλαίου είναι να περιγραφεί η ανάγκη δημιουργίας ενός πλαισίου ασφάλειας πληροφοριών προσανατολισμένο στην ηλεκτρονική μάθηση και πιο συγκεκριμένα στα Συστήματα Διαχείρισης Ηλεκτρονικής Μάθησης (ΣΔΗΜ). Στην επόμενη ενότητα πραγματοποιείται μια βιβλιογραφική ανασκόπηση προκειμένου να οριοθετήσουμε το πρόβλημα και να οδηγηθούμε στο αντικείμενο έρευνας.

1.1 Βιβλιογραφική Ανασκόπηση

Κάνοντας μια ανασκόπηση στη βιβλιογραφία, γίνεται εύκολα αντιληπτή η πληθώρα βιβλιογραφίας που επικεντρώνεται στη γενική θεωρία πίσω από τα ΣΔΗΜ, αναδεικνύοντας και εξετάζοντας την εννοιολογική πλευρά τους όπως επίσης και τις διάφορες χρήσεις των συστημάτων σε διάφορους τομείς [8], [9] .

Τα θέματα ασφάλειας των ΣΔΗΜ αποτελούν πεδίο έρευνας το οποίο δεν έχει αναλυθεί σε βάθος αφού σε αντίθεση με την ευρεία αποδοχή των συστημάτων η-μάθησης, οι απαιτήσεις ασφάλειας και ιδιωτικότητας δε λαμβάνονται σοβαρά υπόψη, με τις περισσότερες καινοτομίες να επικεντρώνονται στην ανάπτυξη και διανομή του περιεχομένου [14] .

Στα [1], [2], [7], [12], [13], [14], [18], [19], [26], [30], [35], [40], [51], [52], [56], επισημαίνεται η ανάγκη ασφάλειας στα ΣΔΗΜ και προτείνονται διάφορες τεχνολογίες ως πιθανές λύσεις των προβλημάτων ασφάλειας με στόχο την προστασία της πληροφορίας και

τη συνολική ακεραιότητα των δεδομένων αφού τα πολυάριθμα λειτουργικά χαρακτηριστικά και το είδος της πληροφορίας την οποία διαχειρίζονται, εκθέτουν το σύστημα σε απειλές ασφάλειας που θα πρέπει να αντιμετωπιστούν.

Στα [20], [21], [31], [35], [47], οι ερευνητές αντιμετωπίζουν καθολικά το πρόβλημα ασφάλειας στα περιβάλλοντα η-μάθησης προτείνοντας ο καθένας ένα διαφορετικό μοντέλο ασφάλειας όπου το καθένα έχει διαφορετική προσέγγιση. Πιο συγκεκριμένα, οι συγγραφείς των [20] [21] πρότειναν την ευέλικτη και επεκτάσιμη υπηρεσία ασφάλειας AICA (Integrity, Non-Repudiation, Confidentiality και Authenticity) η οποία βασίζεται στις υπηρεσίες ιστού. Χαρακτηριστική ιδιότητα της υπηρεσίας είναι η δυνατότητα χρήσης της από οποιοδήποτε σύστημα η-μάθησης ανεξάρτητα από τη γλώσσα προγραμματισμού και την αρχιτεκτονική με την οποία είναι υλοποιημένο. Στο [31] προτείνεται ένα μοντέλο ασφαλούς συστήματος η-μάθησης το οποίο βασίζεται σε τεχνολογίες όπως τείχος προστασίας[1], εικονικά ιδιωτικά δίκτυα[2] και πακέτο λογισμικού PGP[3] για την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων. Οι συγγραφείς του [35] ανέπτυξαν ένα εννοιολογικό πλαίσιο απειλών ασφάλειας το οποίο ονομάζεται AICA (Availability, Integrity, Confidentiality and Authentication) Μοντέλο Απειλών, το οποίο μπορεί να χρησιμοποιηθεί από τους προγραμματιστές των συστημάτων η-μάθησης ως οδηγός για τη μείωση των ευπαθειών ενός τέτοιου συστήματος κατά τη φάση της σχεδίασης. Τέλος, στο [47], οι ερευνητές επισημαίνουν την ανάγκη ασφάλειας σε ένα προσωποποιημένο περιβάλλον η-μάθησης (Web F-SMILE) και χρησιμοποιούν Υποδομή Δημόσιου Κλειδιού και Ασφάλεια Υπηρεσιών Ιστού για την ασφαλή λειτουργία του συστήματος.

Στα [27] [50], οι ερευνητές εισάγουν την έννοια της διοίκησης ασφάλειας πληροφοριών σε ένα περιβάλλον η-μάθησης. Πρόκειται για ένα ολιστικό τρόπο αντιμετώπισης της ασφάλειας το οποίο απευθύνεται στις διοικητικές δομές ενός οργανισμού που διατηρεί και χρησιμοποιεί ένα σύστημα ηλεκτρονικής μάθησης και περιλαμβάνει μη τεχνικές προδιαγραφές εστιάζοντας περισσότερο στη διοίκηση ασφάλειας.

Αναμφισβήτητα η διαδικασία αξιολόγησης του εκπαιδευόμενου σε ένα σύστημα η-μάθησης αποτελεί μια κρίσιμη διαδικασία η οποία αποτελεί αντικείμενο μελέτης ασφάλειας. Στα [16] και [42] παρουσιάζονται αντίμετρα ασφάλειας για την αντιμετώπιση απειλών ασφάλειας κατά τη διενέργεια ηλεκτρονικών εξετάσεων (η-εξετάσεων) μέσω ιστού.

1.2 Περιγραφή Προβλήματος/Αντικειμένου Έρευνας

Συνοψίζοντας από την παραπάνω βιβλιογραφία, γίνεται αντιληπτό ότι η ασφάλεια στα συστήματα η-μάθησης απαιτεί μεγάλη προσοχή και επιπλέον έρευνα. Χαρακτηριστική είναι η έλλειψη ενός σχεδίου πολιτικής ασφάλειας πληροφοριών προσανατολισμένο στα συστήματα η-μάθησης, το οποίο να μπορεί να χρησιμοποιηθεί ως οδηγός υλοποίησης ασφάλειας σε ένα

[1] Firewall

[2] VPN – Virtual Private Network

[3] Pretty Good Privacy

περιβάλλον η-μάθησης. Βασικό εργαλείο για τη δημιουργία αυτού του σχεδίου θα μπορούσε να αποτελέσει το διεθνές πρότυπο ISO 27002 το οποίο περιλαμβάνει καλές πρακτικές διαχείρισης ασφάλειας πληροφοριών [23]. Επιπλέον, η ασφάλεια κατά τη διαδικασία αξιολόγησης ενός εκπαιδευόμενου σε ένα περιβάλλον η-μάθησης χρίζει ολοκληρωμένου σχεδίου αντιμετώπισης καθώς πρόκειται για την πιο κρίσιμη υπηρεσία που προσφέρεται σε ένα σύστημα η-μάθησης. Κρίσιμα ζητήματα ασφάλειας κατά την αξιολόγηση αποτελούν η ακεραιότητα και η εμπιστευτικότητα των ερωτήσεων εξέτασης κατά τη μεταφορά τους και την αποθήκευση τους, η εξουσιοδοτημένη προβολή των ερωτήσεων εξέτασης, η ταυτοποίηση και αυθεντικοποίηση του εκπαιδευόμενου κατά την εξέταση, η εμπιστευτικότητα των απαντήσεων του εκπαιδευόμενου και η μη άρνηση της ευθύνης κατά την υποβολή των απαντήσεων, η διαθεσιμότητα της υπηρεσίας εξετάσεων, η ακεραιότητα και η εμπιστευτικότητα των βαθμολογιών.

1.3 Στόχοι και Αναμενόμενα Αποτελέσματα Διατριβής

Βασικοί στόχοι και κατ'επέκταση τα επιθυμητά αποτελέσματα της διατριβής είναι τα παρακάτω:

1. **Σχέδιο Πολιτικής Ασφάλειας σε Περιβάλλοντα η-Μάθησης** βασισμένο σε καλές πρακτικές ασφάλειας που προτείνονται από το πρότυπο ISO 27002 και το οποίο αποτελείται από τεχνικές και μη τεχνικές συνιστώσες. Το Σχέδιο θα μπορεί να χρησιμοποιηθεί ως
   - Οδηγός υλοποίησης ασφάλειας πληροφοριών σε ένα περιβάλλον η-μάθησης.
   - Μέσο αξιολόγησης ασφάλειας πληροφοριών ενός περιβάλλοντος η-μάθησης.
2. **Αρχιτεκτονική Ασφαλών η-Εξετάσεων** μέσω Ιστού το οποίο θα αποτελέσει ένα ολιστικό, ευέλικτο και επεκτάσιμο μοντέλο ασφαλούς αξιολόγησης εκπαιδευόμενων το οποίο μπορεί να εφαρμοστεί σε οποιοδήποτε ΣΔΗΜ.
3. **SWBES - Σύστημα Ασφαλών η-Εξετάσεων μέσω Ιστού** το οποίο υλοποιεί τα απαραίτητα αντίμετρα ασφάλειας.
4. Εφαρμογή του Σχεδίου Πολιτικής Ασφάλειας στην Αρχιτεκτονική Ασφαλών η-Εξετάσεων και στο SWBES.

Πιο συγκεκριμένα, για την επίτευξη των στόχων θα εφαρμοστεί η παρακάτω βηματική διαδικασία ανάλυσης:

1. Μελέτη Συστημάτων Διαχείρισης η-Μάθησης – Ανάλυση λειτουργικών χαρακτηριστικών.
2. Μελέτη Ασφάλειας Πληροφοριών στα ΣΔΗΜ βάσει της δραστηριότητας των χρηστών.
3. Πρόταση Σχεδίου Πολιτικής Ασφάλειας Πληροφοριών σε Περιβάλλοντα η-Μάθησης (ΣΔΗΜ).
4. Υλοποίηση Υπηρεσίας Ηλεκτρονικών Εξετάσεων.
   4.1. Αρχιτεκτονική Ασφαλών η-Εξετάσεων μέσω Ιστού
   4.2. Υλοποίηση του Συστήματος Ασφαλών Εξετάσεων μέσω Ιστού SWBES
   4.3. Ενσωμάτωση υπηρεσίας ασφαλών εξετάσεων μέσα σε ένα ΣΔΗΜ ανοιχτού κώδικα όπως το Moodle.

5. Εφαρμογή του Σχεδίου Πολιτικής Ασφάλειας στην Υπηρεσία Ασφαλών Εξετάσεων.
6. Σύγκριση της υλοποιημένης υπηρεσίας εξετάσεων με την ενσωματωμένη διαδικασία αξιολόγησης του Moodle.

1.4 Δομή Περιεχομένου Διατριβής

Στην παρούσα ενότητα θα γίνει παρουσίαση της οργάνωσης περιεχομένου της διατριβής κάνοντας μια σύντομη ανασκόπηση των κεφαλαίων 2 έως 6.

Στο κεφάλαιο 2 γίνεται σύντομη έρευνα και ανάλυση των συστημάτων διαχείρισης ηλεκτρονικής μάθησης εστιάζοντας στην αρχιτεκτονική υλοποίησής τους και στις λειτουργικές απαιτήσεις τους. Στο πλαίσιο της έρευνας, παρουσιάζεται το Σύστημα Διαχείρισης Ηλεκτρονικής Μάθησης ανοικτού κώδικα Moodle προβάλλοντας τα λειτουργικά χαρακτηριστικά του.

Στο κεφάλαιο 3 γίνεται μελέτη ασφάλειας πληροφοριών των ΣΔΗΜ παρουσιάζοντας τις απειλές ασφάλειας που αντιμετωπίζουν οι διάφορες κατηγορίες χρηστών βάσει της δραστηριότητας τους σε ένα τέτοιο περιβάλλον. Επίσης, γίνεται έρευνα των υλοποιημένων αντιμέτρων ασφάλειας του Moodle βάσει των βασικών απαιτήσεων ασφάλειας: Ταυτοποίηση και Αυθεντικοποίηση, Εξουσιοδότηση, Εμπιστευτικότητα, Ακεραιότητα, Μη Άρνηση της Ευθύνης και Διαθεσιμότητα.

Στο κεφάλαιο 4 προτείνεται και συντάσσεται ένα Σχέδιο Πολιτικής Ασφάλειας στα Περιβάλλοντα η-Μάθησης και αναλύονται όλες οι συνιστώσες που το απαρτίζουν περιγράφοντας κάποιες καλές πρακτικές βάσει του ISO 27002.

Στο κεφάλαιο 5 προτείνεται και παρουσιάζεται η Αρχιτεκτονική Ασφαλών Ηλεκτρονικών Εξετάσεων μέσω Ιστού. Πιο συγκεκριμένα αναλύονται οι λειτουργικές απαιτήσεις και οι απειλές ασφάλειας των η-εξετάσεων μέσω Ιστού, παρουσιάζεται η προτεινόμενη Αρχιτεκτονική και τεκμηριώνεται λεπτομερώς το Σύστημα Ασφαλών η-Εξετάσεων μέσω Ιστού, **SWBES**. Το κεφάλαιο 5 ολοκληρώνεται με την εφαρμογή της τεχνικής συνιστώσας του Σχεδίου Πολιτικής Ασφάλειας στην προτεινόμενη Αρχιτεκτονική μέσω ενός συγκριτικού πίνακα. Στο πίνακα αυτό αντιπαραβάλλονται τα αντίμετρα ασφάλειας της προτεινόμενης Αρχιτεκτονικής με τα ενσωματωμένα αντίμετρα του Moodle

Τέλος, στο κεφάλαιο 6 αναφέρονται συνοπτικά τα ευρήματα της διατριβής και προτάσεις μελλοντικής έρευνας και βελτίωσης.

Συστήματα Ηλεκτρονικής Μάθησης

Στόχος της διατριβής είναι η δημιουργία ενός ασφαλούς περιβάλλοντος ηλεκτρονικής μάθησης βασισμένο σε ένα πλαίσιο ασφάλειας πληροφοριών προσαρμόζοντας το πρότυπο ISO 27002 στις ανάγκες της ηλεκτρονικής μάθησης. Στο κεφάλαιο αυτό θα γίνει περιγραφή βασικών εννοιών της ηλεκτρονικής μάθησης και λεπτομερής ανάλυση της αρχιτεκτονικής και των λειτουργικών χαρακτηριστικών των συστημάτων διαχείρισης ηλεκτρονικής μάθησης.

2.1 Η εξέλιξη της ηλεκτρονικής μάθησης (η-μάθησης)

Με στόχο την περιγραφή της εξέλιξης των μεθόδων διαμοιρασμού γνώσης θα χωρίσουμε την εξέλιξη αυτή σε τρεις διακριτές φάσεις.

Η πρώτη φάση οριοθετείται κατά την περίοδο όπου οι υπολογιστές είτε δεν υπήρχαν είτε δεν είχαν εδραιωθεί λόγω του υψηλού κόστους. Η εκπαίδευση και η πρακτική συνυπήρχαν και διεξάγονταν σε μια αίθουσα βασισμένη σε ένα εκπαιδευτή ο οποίος είχε τον πλήρη έλεγχο της εκπαιδευτικής διαδικασίας. Η πρώτη φάση χαρακτηρίζεται σε μεγάλο βαθμό από τον τόπο και την ώρα της μάθησης όπου η κοινωνική δικτύωση αποτελεί κυρίαρχο ρόλο.

Η δεύτερη φάση τοποθετείται τη δεκαετία του ’80 με την άφιξη και την αυξανόμενη δημοσιότητα των προσωπικών υπολογιστών [46]. Η εφεύρεση και η κοινωνική αποδοχή των προσωπικών υπολογιστών οδήγησαν στην εκπαίδευση και εξάσκηση βασισμένη στους υπολογιστές και αποτέλεσαν την έναρξη της δεύτερης φάσης και την είσοδο στην εποχή Μάθησης βασισμένη στου υπολογιστές. Κατά την εποχή αυτή η μάθηση γίνεται μέσω ψηφιακών δίσκων όπου το μαθησιακό υλικό αποτελείται από πολυμέσα βασισμένα σε ήχο, εικόνα και animation. Η εποχή αυτή χαρακτηρίζεται από την ανεξαρτησία της μάθησης από το χρόνο και τον τόπο.

Η τρίτη φάση ξεκινάει με την έλευση του Διαδικτύου και του ιστού στα τέλη του 1990, τα οποία σηματοδότησαν ένα νεο ξεκίνημα για τη μάθηση βασισμένη στις τεχνολογίες πληροφοριών και επικοινωνιών [46]. Η ανάγκη για απεριόριστη πρόσβαση στην πληροφορία, τη γνώση και τη βελτίωση των νοητικών ικανοτήτων επέβαλε τη δημιουργία και την ενίσχυση της εκπαίδευσης βασισμένης σε τεχνολογίες πληροφοριών και επικοινωνιών η οποία είναι γνωστή και ως ηλεκτρονική μάθηση. Κατά τη διάρκεια αυτής της περιόδου η ηλεκτρονική μάθηση, η εκπαίδευση και η εξάσκηση λαμβάνονται μέσω Διαδικτύου, εσωτερικών δικτύων κοκ. Αυτή η τεχνολογική καινοτομία έχει ως αποτέλεσμα την αλλαγή της εκπαιδευτικής διαδικασίας η οποία είναι αναγκασμένη να ενσωματώσει πρακτικές ηλεκτρονικής μάθησης καθώς οι χρήστες/εκπαιδευόμενοι/μαθητές μπορούν να έχουν πρόσβαση στη μάθηση οποιαδήποτε στιγμή και από οποιοδήποτε σημείο .

Αυτή τη στιγμή βρισκόμαστε στο πιο παραγωγικό στάδιο της τρίτης φάσης όπου η εκπαίδευση αποκτάει συνεχώς διαφορετικές μορφές ενσωματώνοντας τεχνολογίες ηλεκτρονικής μάθησης. Από την άλλη πλευρά η ηλεκτρονική μάθηση δεν μπορεί να αντικαταστήσει πλήρως την κλασική μέθοδο εκπαίδευσης γι’αυτό το λόγο όλα τα ηλεκτρονικά περιβάλλοντα μάθησης υιοθετούν καλές πρακτικές από όλες τις φάσεις εξέλιξης της εκπαίδευσης.

2.2 Άξονες της η-Μάθησης

Η ηλεκτρονική μάθηση ορίζεται ως μάθηση βασισμένη στην τεχνολογία όπου το εκπαιδευτικό υλικό παραδίδεται ηλεκτρονικά στους απομακρυσμένους εκπαιδευόμενους είτε μέσω ψηφιακών μέσων είτε μέσω των δικτύων υπολογιστών [53]. Η ηλεκτρονική μάθηση μπορεί να καλύψει ένα ευρύ φάσμα εφαρμογών, συστημάτων και διαδικασιών όπως τα συστήματα ηλεκτρονικής μάθησης, μάθηση βασισμένη στον ιστό, εικονικές τάξεις, και ηλεκτρονική συνεργασία.

Η μορφή και το ποσοστό συμμετοχής των τεχνολογιών πληροφορίας και επικοινωνιών στην εκπαιδευτική διαδικασία καθορίζουν και το είδος μάθησης που προσφέρεται. Οι διακριτές μορφές μάθησης είναι οι παρακάτω:

2.2.1 Μάθηση βασισμένη στον υπολογιστή[4]

Το εκπαιδευτικό περιβάλλον δομείται με γνώμονα τις τεχνολογικές υποδομές (υπολογιστές) οι οποίες εξυπηρετούν τη διδασκαλία. Οι υπολογιστές αποτελούν βασικό συστατικό της εκπαίδευσης και έχουν ως στόχο τη διευκόλυνση και τον εμπλουτισμό της εκπαιδευτικής διαδικασίας [53].

2.2.2 Εξάσκηση βασισμένη στον υπολογιστή[5]

Σε αυτή την περίπτωση η ηλεκτρονική μάθηση έχει τη μορφή εξάσκησης μέσω αυτόνομων μαθησιακών δραστηριοτήτων οι οποίες είναι προσβάσιμες μέσω υπολογιστή (είτε τοπικά είτε μέσω ιστού) [53]. Παρακάτω αναφέρονται τα βασικά χαρακτηριστικά:

- Γραμμική παρουσίαση εκπαιδευτικού περιεχομένου. Χρησιμοποιείται για να εμπλουτίσει στατικά την εκπαιδευτική διαδικασία.
- Δυνατότητα αξιολόγησης του εκπαιδευόμενου μέσω αλληλεπιδραστικών ηλεκτρονικών ασκήσεων οι οποίες βαθμολογούνται αυτόματα και τροφοδοτούν το χρήστη με χρήσιμα σχόλια.
- Εμπλουτισμός της εκπαιδευτικής διαδικασίας. Καλύπτει εκπαιδευτικές ανάγκες και δημιουργεί κίνητρο στον εκπαιδευόμενο μέσω φιλικών προς το χρήστη εφαρμογών οι οποίες οπτικοποιούν το εκπαιδευτικό υλικό και το προσφέρουν με έναν εναλλακτικό τρόπο.

2.2.3 Συνεργατική μάθηση υποστηριζόμενη από υπολογιστές[6]

Βελτίωση της μάθησης και της διδασκαλίας μέσω καινοτόμων διαδικασιών χρησιμοποιώντας συνεργατικά εργαλεία Web 2.0 (e-Learning 2.0) [53]. Η διαφοροποίηση της συγκεκριμένης

[4] Computer-Based Learning (CBL)

[5] Computer-Based Traning (CBT)

[6] Computer-Supportive Collaborative Learning (CSCL)

μορφής μάθησης από τις υπόλοιπες είναι ότι έχει ως στόχο την ενίσχυση της συνεργατικότητας, συμμετοχής και επικοινωνίας μεταξύ των εκπαιδευομένων. Blogs, , Google Docs και εργαλεία κοινωνικής δικτύωσης είναι μερικά από τα Web 2.0 εργαλεία που χρησιμοποιούνται έχοντας υποστηρικτικό ρόλο στη εκπαιδευτική διαδικασία και δίνουν τη δυνατότητα στους εκπαιδευόμενους για συνεργασία, συζητήσεις ιδεών και προώθηση πληροφοριών.

2.3 Συστήματα η-Μάθησης

Τα συστήματα ηλεκτρονικής μάθησης είναι τα πληροφοριακά συστήματα τα οποία χρησιμοποιούν τεχνολογίες δικτύων με στόχο τη διανομή εκπαιδευτικού περιεχομένου στους χρήστες τους. Ένα σύστημα ηλεκτρονικής μάθησης έχει τη δυνατότητα να σχεδιάζει, παραδίδει και διαχειρίζεται την online εκπαιδευτική διαδικασία [50].

Τα συστήματα ηλεκτρονικής μάθησης μπορούν να χρησιμοποιηθούν τόσο σε εταιρικά όσο και σε ακαδημαϊκά περιβάλλοντα. Στην περίπτωση του εταιρικού περιβάλλοντος, ένα τέτοιο σύστημα συμβάλλει στο διαμοιρασμό πληροφοριών και γνώσης μεταξύ των εργαζομένων σχετικών με την πορεία των εργασιών τους όπως επίσης στη δημιουργία εκπαιδευτικών σεμιναρίων προς όφελος της εταιρικής συνέχειας. Σε ένα ακαδημαϊκό περιβάλλον, τα συστήματα ηλεκτρονικής μάθησης μπορούν να χρησιμοποιηθούν σε όλες τις βαθμίδες της εκπαίδευσης με στόχο την ενίσχυση της εκπαιδευτικής διαδικασίας ή ακόμα και τη δημιουργίας ενός ολοκληρωμένου συστήματος ηλεκτρονικής μάθησης αποκλειστικά μέσω δικτύου. Τα συστήματα ηλεκτρονικής μάθησης χωρίζονται στις δύο παρακάτω μεγάλες κατηγορίες:

2.3.1 Σύστημα Διαχείρισης η-Μάθησης (ΣΔΗΜ)[7]

Το ΣΔΗΜ αποτελεί την κύρια κατηγορία συστημάτων η-μάθησης και πρόκειται για μια εφαρμογή λογισμικού η οποία ενσωματώνει τη διαχείριση και τη διανομή εκπαιδευτικού υλικού προς τους εκπαιδευόμενους μέσω τεχνολογιών πληροφοριών και επκοινωνιών. Συγκεκριμένα ένα περιβάλλον διαχείρισης ηλεκτρονικής μάθησης συγκεντρώνει τα παρακάτω χαρακτηριστικά [54]:

- Κεντρικοποιημένη και αυτοματοποιημένη διαχείριση
- Άμεση δόμηση και διανομή εκπαιδευτικού περιεχομένου
- Προσωποποίηση περιεχομένου
- Δυνατότητα επαναχρησιμοποίησης του υλικού
- Υπηρεσίες αυτοεξυπηρέτησης και αυτοκαθοδήγησης των χρηστών
- Υποστήριξη φορητότητας και εδραιωμένων προτύπων τεχνολογίας

[7] e-Learning Management System (e-LMS)

Μερικά παραδείγματα συστημάτων διαχείρισης ηλεκτρονικής μάθησης είναι τα Moodle, Claroline, ILIAS, eFront, Sakai κα.

2.3.2 Σύστημα Διαχείρισης Περιεχομένου η-Μάθησης[8]

Αποτελεί ένα σύστημα προσανατολισμένο στο περιεχόμενο σε αντίθεση με τα σύστημα διαχείρισης η-μάθησης τα οποία είναι προσανατολισμένα στη διοίκηση και τον έλεγχο της μάθησης. Πιο συγκεκριμένα ένα Σύστημα Διαχείρισης Περιεχομένου η-μάθησης έχει ως στόχο τη δημιουργία, διαχείριση και διανομή του εκπαιδευτικού περιεχομένου αλλά κυρίως παρέχει τη δυνατότητα της επεξεργασίας και επαναχρησιμοποίησης των υπαρχόντων εκπαιδευτικών αντικειμένων [54]. Πρόκειται για ένα συμπληρωματικό σύστημα το οποίο καλύπτει την ανάγκη των δημιουργών περιεχομένου (διευθυντές, καθηγητές, εκπαιδευτές) για γρήγορη και προσωποποιημένη δημιουργία περιεχομένου διαμορφώνοντας εκπαιδευτικά αντικείμενα τα οποία βρίσκονται στο αποθετήριο. Μερικά παραδείγματα συστημάτων διαχείρισης περιεχομένου ηλεκτρονικής μάθησης είναι τα aTutor, Kenexa LCMS κα.

Για τις ανάγκες της διατριβής, θα επικεντρωθούμε στα Συστήματα Διαχείρισης η-Μάθησης (ΣΔΗΜ) καθώς αποτελούν μια ολοκληρωμένη λύση περιλαμβάνοντας διαχειριστικά και εκπαιδευτικά εργαλεία σε σύγκριση με τα συστήματα διαχείρισης περιεχομένου η-μάθησης τα οποία έχουν υποστηρικτικό ρόλο και αφορούν συγκεκριμένες κατηγορίες χρηστών. Στη συνέχεια του κεφαλαίου και στο πλαίσιο της έρευνας σχετικά με τα ΣΔΗΜ, μελετάμε την περίπτωση του Moodle, το οποίο αποτελεί το πιο διαδεδομένο ανοιχτού κώδικα ΣΔΗΜ και αποτελεί χαρακτηριστικό παράδειγμα περιβάλλοντος η-μάθησης.

2.4 Πρότυπα η-Μάθησης

Τα ΣΔΗΜ στηρίζονται σε μια ποικιλία από πλατφόρμες ανάπτυξης χρησιμοποιώντας διαφορετικές τεχνολογίες με αποτέλεσμα να παρουσιαστεί η ανάγκη ύπαρξης προτύπων για την περιγραφή του μαθησιακού υλικού, ώστε τα συστήματα αυτά να προσφέρουν μεταφερσιμότητα (portability) των μαθησιακών πόρων, διαλειτουργικότητα (interoperability) μεταξύ τους και εύκολη αναζήτηση . Έτσι, τα κυριότερα πρότυπα που έχουν αναπτυχθεί μέχρι στιγμής είναι [53]:

- Το πρότυπο της AICC (Aviation Industry CBT Committee).
- Το πρότυπο διαλειτουργικότητας μαθησιακών εργαλείων LTI[9] της IMS Global Learning Consortium.
- Το πρότυπο SCORM (Sharable Content Object Reference Model), που αναπτύχθηκε από το Υπουργείο Εθνικής Άμυνας των ΗΠΑ, με σκοπό να συνενώσει τα υπόλοιπα πρότυπα και σήμερα είναι ίσως το πιο δημοφιλές. Τα πακέτα SCORM μπορούν να φορτωθούν σε οποιοδήποτε συμβατό με αυτό Σύστημα Διαχείρισης Μάθησης.

[8] e-Learning Content Management Systems (e-LCMS)

[9] Learning Tools Interoperability

- Το πρότυπο Learning Object Metadata Standard της IEEE (IEEE LOM), που ορίζει τα στοιχεία των μεταδεδομένων που μπορούν να χρησιμοποιηθούν για την περιγραφή μαθησιακών πόρων.

2.5 Επίδραση των ΣΔΗΜ στην εκπαιδευτική διαδικασία

Η εισαγωγή των συστημάτων διαχείρισης η-μάθησης στην εκπαιδευτική διαδικασία είτε σε εταιρικό είτε σε ακαδημαϊκό περιβάλλον αποτέλεσε και εξακολουθεί να αποτελεί καινοτομία. Αξιολογώντας τις υπηρεσίες που μπορεί να προσφέρει ένα τέτοιο σύστημα, στον παρακάτω πίνακα παρατίθενται συγκεντρωτικά μερικά από τα πλεονεκτήματα και μειονεκτήματα που παρουσιάζονται κατά τη χρήση τους [10].

Πλεονεκτήματα	
Ευελιξία	Ο κάθε εκπαιδευόμενος κάνει το δικό του χρονοπρογραμματισμό εργασιών ακολουθώντας τους δικούς του ρυθμούς εκμάθησης.
Ανεξαρτησία τόπου και χρόνου	Ο εκπαιδευόμενος και ο εκπαιδευτής συμμετέχουν στη μάθηση (ο καθένας ανάλογα με το ρόλο του) χωρίς να περιορίζονται τοπικά και χρονικά.
Μείωση συνολικού κόστους	Η μάθηση προσφέρεται μέσω δικτύου με αποτέλεσμα να μην υπάρχουν έξοδα μεταφοράς, κόστος χαρτιού κοκ.
Μάθηση χωρίς χρονικές καθυστερήσεις	Αποτελεσματική μεταφορά και διαχείριση της μάθησης ειδικά σε ένα ανταγωνιστικό εταιρικό περιβάλλον όπου ο προγραμματισμός είναι αρκετά αυστηρός.
Προσαρμοστική Μάθηση	Κάθε εκπαιδευόμενος αντιμετωπίζεται από το σύστημα ως μοναδική οντότητα με αποτέλεσμα να μπορεί να προσαρμόζεται στις ανάγκες του και να μην είναι προσανατολισμένο στο περιεχόμενο.
Συνέπεια περιεχομένου	Λόγω της κεντρικοποιημένης απόθεσης του εκπαιδευτικού υλικού, κάθε εκπαιδευόμενος έχει το ίδιο δικαίωμα πρόσβασης στο εκπαιδευτικό υλικό του.
Άμεση διάδοση πληροφοριών	Κάθε ενημέρωση ή αλλαγή σε ένα μάθημα είναι άμεσα διαθέσιμη στον εκπαιδευόμενο με τη μορφή ηλεκτρονικής ανακοίνωσης
Χρήση μοναδικών λειτουργικών χαρακτηριστικών	Οι εκπαιδευόμενοι και οι εκπαιδευτές μπορούν να χρησιμοποιήσουν πλήθος δυνατοτήτων οι οποίες δεν είναι διαθέσιμες στην παραδοσιακή μορφή εκπαίδευσης. Τέτοιες δυνατότητες είναι η χρήση πολυμέσων όπως videos, διαδραστικά quiz, παιχνίδια, εικονικά δωμάτια συνομιλίας, δημιουργία κοινότητας (forum) κ.α.
Αύξηση συμμετοχής/	Σε ένα περιβάλλον ηλεκτρονικής μάθησης, τα Web 2.0 εργαλεία μπορούν να συμβάλλουν στη επίτευξη συνεργασίας μεταξύ των

συνεργασίας των εκπαιδευομένων	εκπαιδευομένων μέσω της αυξημένης συμμετοχής προς όφελος της εκπαιδευτικής διαδικασίας.
Κίνητρο	Η χρήση τεχνολογιών πληροφορίας και επικοινωνιών στη μάθηση επιδρά θετικά στον εκπαιδευόμενο δίνοντας του κίνητρο να συμμετέχει και να επιτύχει τους στόχους του.
Καταγραφή εξέλιξης εκπαιδευόμενου	Ο εκπαιδευτής έχει τη δυνατότητα να παρακολουθεί την εξέλιξη ενός εκπαιδευόμενου μέσω δεδομένων σχετικών με τη δραστηριότητα του μέσα στο σύστημα. Συνεπώς η αξιολόγηση για τον εκπαιδευτή γίνεται με πιο αντικειμενικό τρόπο καθώς έχει ανα πάσα στιγμή την εξέλιξη κάθε εκπαιδευόμενου.

Πίνακας 1. Πλεονεκτήματα χρήσης ΣΔΗΜ στην εκπαιδευτική διαδικασία

Μειονεκτήματα	
Έλλειψη άμεσης επαφής	Η εκπαιδευτική διαδικασία χάνει το χαρακτηριστικό γνώρισμα της αμεσότητας και μετατρέπεται σε απρόσωπη διαδικασία κατά την οποία ο εκπαιδευόμενος οφείλει να αντιμετωπίσει μόνος του τα όποια προβλήματα συναντήσει.
Απαίτηση υποδομών πληροφορικής	Οι εκπαιδευόμενοι είναι υποχρεωμένοι να έχουν πρόσβαση σε προσωπικό υπολογιστή, στο διαδίκτυο και σε λογισμικό. Τα παραπάνω αποτελούν τις ελάχιστες απαιτήσεις για τη χρήση ενός συτήματος η-μάθησης
Κόστος αγοράς συστήματος η-μάθησης	Στην περίπτωση που το σύστημα είναι κάποια εμπορική λύση, τότε το κόστος απόκτησης και συντήρησης είναι αρκετά υψηλό. Εκτός από τις εμπορικές λύσεις, υπάρχουν και συστήματα η-μάθησης ανοικτού κώδικα τα οποία διατίθενται δωρεάν και παρέχουν τις ίδιες λειτουργικότητες.
Μάθηση μέσω υπολογιστή	Η χρήση υπολογιστή είναι αναγκαία με αποτέλεσμα οι εκπαιδευόμενοι να είναι αναγκασμένοι να δουλεύουν για μεγάλα χρονικά διαστήματα μπροστά σε κάποια οθόνη.

Απαίτηση πρότερης γνώσης σχετικά με συστήματα η-μάθησης	Οι χρήστες ενός συστήματος η-μάθησης θα πρέπει να εκπαιδευτούν στη χρήση ενός τέτοιου συστήματος έτσι ώστε να αντιληφθούν και να χρησιμοποιήσουν σωστά όλα τα λειτουργικά χαρακτηριστικά του. Οι χρήστες με λίγες γνώσεις υπολογιστών αντιμετωπίζουν προβλήματα στην προσαρμογή τους σε ένα τέτοιο περιβάλλον.
Ασφάλεια	Η ασφάλεια σε ένα σύστημα η-μάθησης αποτελεί ίσως τη μεγαλύτερη πρόκληση καθώς οι προγραμματιστές και οι διαχειριστές του δεν λαμβάνουν υπόψη τη κρισιμότητα των υπηρεσιών που προσφέρει με αποτέλεσμα το σύστημα να είναι πολλές φορές ευάλωτο σε επιθέσεις. Τα περισσότερα συστήματα η-μάθησης δεν ικανοποιούν τις απαραίτητες απαιτήσεις ασφάλειας.

Πίνακας 2. Μειονεκτήματα χρήσης ΣΔΗΜ στην εκπαιδευτική διαδικασία

2.6 Αρχιτεκτονική ΣΔΗΜ

Η βασική αρχιτεκτονική των συστημάτων διαχείρισης η-μάθησης είναι παρόμοια για τα περισσότερα συστήματα που κυκλοφορούν στην αγορά σύμφωνα με την οποία αποτελούνται από ένα κεντρικοποιημένο αποθετήριο για την αποθήκευση των απαραίτητων πληροφοριών/περιεχομένου και μια οργανωμένη σχεδίαση για την εύκολη πλοήγηση μέσα στο εκπαιδευτικό και μη περιεχόμενο . Πιο συγκεκριμένα τα περισσότερα συστήματα έχουν υιοθετήσει την αρχιτεκτονική 3 επιπέδων :

1. **Επίπεδο αποθήκευσης**: Σε αυτό το επίπεδο βρίσκονται αποθηκευμένα όλα τα απαραίτητα δεδομένα του συστήματος.
2. **Επίπεδο εφαρμογής**: Πρόκειται για τη γέφυρα μεταξύ του επιπέδου αποθήκευσης και του επιπέδου ιστού η οποία είναι υπεύθυνη για τη μεταφορά των αιτήσεων προς το επίπεδο αποθήκευσης και την αποστολή των αποτελεσμάτων προς το επίπεδο ιστού.
3. **Επίπεδο ιστού**: Αποτελεί τη διεπαφή χρήσης του συστήματος και είναι το περιβάλλον με το οποίο οι χρήστες αλληλεπιδρούν και στο οποίο χρησιμοποιούν το σύνολο των λειτουργιών του συστήματος.

2.7 Λειτουργικές Απαιτήσεις ΣΔΗΜ

Οι λειτουργικές απαιτήσεις ενός αξιόπιστου ΣΔΗΜ συνοψίζονται παρακάτω [33]:

- **Υψηλή διαθεσιμότητα (High availability)**: Ικανότητα ταυτόχρονης κάλυψης διαφορετικών και εξελισσόμενων αναγκών των χρηστών του.
- **Επεκτασιμότητα (Scalability)**: Δυνατότητα προσαρμογής και επέκτασης στις ανάγκες των χρηστών και στο μεγάλο όγκο διδακτικών πακέτων.

- **Χρηστικότητα (Usability):** Ευκολία με την οποία οι χρήστες μπορούν να εκμεταλλευτούν τις δυνατότητες της πλατφόρμας.
- **Διαλειτουργικότητα (Interoperability)**: Επικοινωνία με συστήματα διαφορετικής τεχνολογίας.
- **Σταθερότητα (Stability)**: Δυνατότητα διαχείρισης μεγάλου όγκου πληροφοριών και χρηστών με αξιοπιστία και αποτελεσματικότητα.
- **Ασφάλεια (Security)**: Ισχυρή ταυτοποίηση και αυθεντικοποίηση χρηστών, εξουσιοδότηση, εμπιστευτικότητα, ακεραιότητα δεδομένων, μη-άρνηση ευθύνης και διαθεσιμότητα υπηρεσιών.

Στη συνέχεια γίνεται περιγραφή των λειτουργικών μερών που συναντάμε στο σύνολο των συστημάτων η-μάθησης [33]:

Πύλη

Είναι ο προσωπικός ιστοχώρος στον οποίο ο κάθε χρήστης έχει πρόσβαση και έχει τη δυνατότητα να διαχειριστεί τα προσωπικά του δεδομένα όπως πληροφορίες λογαριασμού χρήστη, μαθήματα στα οποία είναι εγγεγραμμένος είτε ως εκπαιδευόμενος είτε ως εκπαιδευτής κα. Όπως γίνεται αντιληπτό οι δυνατότητες που προσφέρει ένα σύστημα η-μάθησης είναι διαθέσιμες στους χρήστες ανάλογα με το ρόλο τον οποίο διαθέτουν. Συνεπώς ο προσωπικός ιστοχώρος στον οποίο εισέρχονται όπως επίσης και τα εργαλεία τα οποία είναι διαθέσιμα διαφοροποιούνται ανά ρόλο (εκπαιδευτής, εκπαιδευόμενος, διαχειριστής)

Αναζήτηση

Η λειτουργία της αναζήτησης αποτελεί βασικό στοιχείο του συστήματος η-μάθησης. Οι χρήστες έχουν τη δυνατότητα να αναζητήσουν περιεχόμενο (έγγραφα, εκπαιδευτικό υλικό κα.) σχετικό με κάποια κριτήρια που εκείνοι προσδιορίζουν.

Κατάλογος Μαθημάτων

Στον κατάλογο μαθημάτων είναι διαθέσιμη η κατηγοριοποίηση βάσει των θεματικών τους όπως επίσης και βασικές πληροφορίες σχετικές με την εγγραφή στο μάθημα (π.χ. προαπαιτούμενες γνώσεις), χρονοδιαγράμματα, όρους και κανόνες διδασκαλίας του μαθήματος κα.

Αξιολόγηση

Η αξιολόγηση αποτελεί βασικό λειτουργικό μέρος ενός συστήματος η-μάθησης καθώς παίζει καθοριστικό ρόλο στη βαθμολόγηση και στην ολοκλήρωση του μαθήματος για ένα εκπαιδευόμενο. Συγκεκριμένα η αξιολόγηση έχει τις παρακάτω λειτουργικές απαιτήσεις:

- Μηχανισμός διαχείρισης εργασιών των εκπαιδευομένων. Συγκεκριμένα ο εκπαιδευόμενος θα πρέπει να καταχωρήσει την εργασία του μέσα ένα καθορισμένο χρονικό διάστημα, η εργασία αποστέλλεται στον εκπαιδευτή και στη συνέχεια ο εκπαιδευτής αξιολογεί την εργασία κοινοποιώντας στον εκπαιδευόμενο τη βαθμολογία του.
- Online Εξετάσεις με τη μορφή ερωτήσεων πολλαπλής επιλογής, ερωτήσεων σωστού/λάθους, ερωτήσεων ανοικτού κειμένου κα. Ο μηχανισμός αυτός βοηθάει τον

εκπαιδευτή στην αντικειμενική αξιολόγηση του εκπαιδευόμενου μέσω αυτόματης διόρθωσης των κλειστών ερωτήσεων.

Αναφορά προόδου

Στην αναφορά προόδου καταγράφεται η συνολική δραστηριότητα και απόδοση του εκπαιδευόμενου σε ένα μάθημα, η οποία συνδέεται λειτουργικά με τον κατάλογο μαθημάτων και την αξιολόγηση.

Εργαλεία επικοινωνίας

Η επικοινωνία σε ένα σύστημα η-μάθησης μπορεί να επιτευχθεί είτε με σύγχρονο τρόπο (μέσω δωματίων συνομιλίας ή εργαλείων τηλεδιάσκεψης ενσωματωμένων στο περιβάλλον του συστήματος) είτε με ασύγχρονο τρόπο (ηλεκτρονική αλληλογραφία, προσωπικός πίνακας πληροφοριών, forums κα). Εκτός από την ευκολία που προσφέρουν στην επικοινωνία, τα συγκεκριμένα εργαλεία βελτιώνουν τη συμμετοχή των εκπαιδευομένων στην εκπαιδευτική διαδικασία και μετατρέπουν ένα απρόσωπο σύστημα σε μια ζωντανή και αλληλεπιδραστική κοινότητα.

2.8 Modular Object-Oriented Dynamic Learning Environment (Moodle)

Το **Moodle** είναι ένα σύστημα διαχείρισης ηλεκτρονικής μάθησης που προσφέρει ολοκληρωμένες υπηρεσίες Ασύγχρονης Τηλεκπαίδευσης. Δημιουργήθηκε το 1999 από τον Αυστραλό Martin Dougiamas ως τμήμα του PhD του. Το όνομα Moodle είναι το ακρώνυμο του Modular Object-Oriented Dynamic Learning Environment [33].

Το Moodle παρέχεται δωρεάν ως λογισμικό ανοικτού κώδικα (κάτω από την GNU Public License) και μπορεί να τρέξει σε οποιοδήποτε σύστημα υποστηρίζει PHP, ενώ έχει τη δυνατότητα να συνδυάζεται με πολλούς τύπους βάσεων δεδομένων (ιδιαίτερα MySQL).

Το Moodle είναι ένα πακέτο λογισμικού για τη δημιουργία διαδικτυακών μαθημάτων, το οποίο προσφέρει ολοκληρωμένες υπηρεσίες διαδικτυακής εκπαίδευσης. Οι δυνατότητές του δεν περιορίζονται στην εξ'αποστάσεως εκπαίδευση αλλά μπορεί να λειτουργήσει συμπληρωματικά και στην κλασσική εκπαίδευση με διαφόρους τρόπους. Μέσα από το γραφικό περιβάλλον του Moodle, το οποίο δεν απαιτεί εξειδικευμένες γνώσεις για τη δημιουργία μαθήματος και την παρακολούθησή του, ο εκπαιδευτικός μπορεί να παρουσιάσει το μάθημα με τρόπο που προκαλεί ενδιαφέρον με την εισαγωγή εκπαιδευτικού υλικού σε διάφορες μορφές, την ανάθεση εργασιών στους εκπαιδευόμενους, την επικοινωνία μαζί τους μέσω εργαλείων ασύγχρονης ή σύγχρονης επικοινωνίας και την αξιολόγηση της επίδοσης των εκπαιδευομένων. Κατ' αυτόν τον τρόπο, οι εκπαιδευόμενοι μαθαίνουν να αναλύουν, να ερευνούν και κυρίως να συνεργάζονται τόσο με τους εκπαιδευτικούς όσο και μεταξύ τους.

Όπως κάθε πλατφόρμα εκμάθησης, έτσι και η πλατφόρμα Moodle δίνει πρόσβαση σε έναν προσωπικό δικτυακό χώρο όπου οι εκπαιδευτές μπορούν να αποθηκεύσουν τα μαθήματα και τα επιτεύγματά τους, και κάθε εκπαιδευόμενος έχει πρόσβαση σε διδακτικό υλικό και σε εργαλεία που υποστηρίζουν τον προγραμματισμό και την ανταλλαγή πληροφοριών.

Η εφαρμογή υποστηρίζει την «εξατομικευμένη μάθηση», επιτρέποντας στους εκπαιδευτές να προσαρμόσουν το πρόγραμμα σπουδών βάσει των μεμονωμένων αναγκών των εκπαιδευομένων τους. Κύρια χαρακτηριστικά είναι η επικοινωνία και η συνεργασία και ο εντοπισμός της δραστηριότητας του εκπαιδευόμενου στην πλατφόρμα.

2.8.1 Αρχιτεκτονική του Moodle

Μελετώντας την αρχιτεκτονική του Moodle, τα επίπεδα τα οποία απαρτίζουν τη δομή του είναι τα εξής: Κατάλογος εφαρμογής, Κατάλογος δεδομένων και Βάση Δεδομένων. Πιο συγκεκριμένα,

Κατάλογος Εφαρμογής

Το Moodle είναι ένα αρθρωτό σύστημα αποτελούμενο από το πυρήνα της εφαρμογής και τα πολυάριθμα αρθρώματα τα οποία προσδίδουν συγκεκριμένη λειτουργικότητα στον πυρήνα. Η συγκεκριμένη δομή συντελεί στην μεγάλη ευελιξία και ευκολία παραμετροποίησης χωρίς την τροποποίηση βιβλιοθηκών του πυρήνα καθώς και στην προσθήκη πολυάριθμων αρθρωμάτων καλύπτωντας με αυτό τον τρόπο διαφορετικές ανάγκες του ηλεκτρονικού μαθήματος . Χαρακτηριστικά παραδείγματα αρθρωμάτων είναι οι δραστηριότητες μαθημάτων (quiz, έρευνα κ.α.), ταυτοποίηση χρήστη κ.α.

Στον κατάλογο της εφαρμογής βρίσκεται ο πυρήνας και τα αρθρώματα του Moodle με το καθένα από αυτά να έχει τους δικούς του υποκαταλόγους.

Κατάλογος Δεδομένων

Το αποθετήριο των αρχείων που ανεβάζουν οι χρήστες του Moodle στον εξυπηρετητή. Εργασίες εκπαιδευόμενων, πολυμεσικό εκπαιδευτικό υλικό, κ.α. είναι μερικά παραδείγματα των αρχείων που περιέχει το αποθετήριο.

Βάση Δεδομένων

Αντικείμενα που δημιουργούνται από τα αρθρώματα του Moodle όπως τα quiz, οι βαθμολογίες, τα στοιχεία χρηστών, κ.α. Επίσης στη βάση δεδομένων αποθηκεύονται τα φυσικά μονοπάτια προς τα αρχεία του αποθετηρίου.

2.8.2 Λειτουργικά Χαρακτηριστικά του Moodle

Το Moodle βρίσκεται υπό συνεχή ανάπτυξη από το 1999 ξεκινώντας από την έκδοση 1.0. Η τρέχουσα έκδοση της πλατφόρμας είναι η 2.3 βάσει της οποίας θα περιγραφούν τα παρακάτω λειτουργικά χαρακτηριστικά [33].

Ως πλατφόρμα ασύγχρονης τηλεκπαίδευσης υποστηρίζει τις ακόλουθες κατηγορίες χρηστών:

- **Διαχειριστές:** Ελέγχουν το σύνολο των ρυθμίσεων του περιβάλλοντος και καθορίζουν τους χρήστες με δικαίωμα δημιουργίας μαθημάτων.
- **Δημιουργοί μαθημάτωνΕκπαιδευτές** : Έχουν δικαίωμα να δημιουργούν δικά τους μαθήματα και να προσθέτουν υλικό σε υπάρχοντα.
- **Μαθητές**: Μπορούν να εγγράφονται και να συμμετέχουν στα μαθήματα.

- **Επισκέπτες:** Συνήθως δεν μπορούν να συμμετάσχουν στις εκπαιδευτικές δραστηριότητες των μαθημάτων, αλλά μπορεί να έχουν τη δυνατότητα να προσπελάσουν το εκπαιδευτικό υλικό συγκεκριμένου μαθήματος, ανάλογα με τις ρυθμίσεις του δημιουργού-εκπαιδευτή.

Η λειτουργία της πλατφόρμας βασίζεται στα μαθήματα, τα οποία ταξινομούνται σε κατηγορίες. Κάθε μάθημα σχεδιάζεται σε διακριτές ενότητες και διατηρεί μια στοιχειώδη οργάνωση, είτε θεματική (όταν οι δραστηριότητες και το εκπαιδευτικό υλικό δομούνται σε θέματα) είτε ημερολογιακή (όταν η αντίστοιχη οργάνωση γίνεται στο χρόνο). Το περιεχόμενο κατασκευάζεται στο σύστημα από τον εκπαιδευτή, αλλά μπορεί να επηρεάζεται και από το μαθητή, διαμορφώνεται σε μικρές ενότητες και στοχεύει σε συγκεκριμένους κάθε φορά μαθησιακούς στόχους. Αποδέχεται εγγραφή του μαθητή, κρατάει στοιχεία της συμμετοχής του στο μάθημα καθώς και βαθμολογίες στις δοκιμασίες που καταχωρούνται, δίνει τη δυνατότητα συζητήσεων των συμμετεχόντων, αξιολόγηση από τους συμμετέχοντες της προσπάθειας που γίνεται στο μάθημα αυτό, κ.ο.κ.

Στις δυνατότητες οργάνωσης του εκπαιδευτικού περιεχομένου του περιβάλλοντος περιλαμβάνεται η σύνθεση κειμένου ή ιστοσελίδας, η δημιουργία συνδέσμων προς άλλους ιστοτόπους, η προβολή όλων των αρχείων ενός φακέλου καθώς και η χρήση εγγράφων πολυμεσικού περιεχομένου όπως είναι τα pdf και τα flash αρχεία. Στις αλληλεπιδραστικές δραστηριότητές του περιλαμβάνονται η υποβολή εργασίας, η ζωντανή συνομιλία (chat), οι ψηφοφορίες/δημοσκοπήσεις, οι ομάδες συζήτησης, το γλωσσάριο ορολογιών μαθήματος, τα κουίζ, η συλλογική συγγραφή κειμένων, οι έρευνες και τα παιχνίδια. Συγκεκριμένα, δραστηριότητες που μπορεί να ενσωματώσει ο εκπαιδευτής μέσα στο μάθημά του είναι:

- **Συζήτηση (Chat)**, για επικοινωνία σύγχρονη, με δυνατότητα δημιουργίας πολλών «δωματίων συζήτησης» για ξεχωριστά θέματα.
- **Ομάδα συζήτησης (Forum)**, για ασύγχρονες συζητήσεις μεταξύ των συμμετεχόντων.
- **Λεξικό (Glossary)**, για δημιουργία καταλόγου λημμάτων ορισμών λέξεων που χρησιμοποιούνται στο μάθημα.
- **Κουίζ (Quiz)**, δηλαδή τεστ με ερωτήσεις διαφόρων τύπων (πολλαπλής επιλογής, ουργούνται από τους εκπαιδευτές, καταχωρούνται σε μια κατηγοριοποιημένη βάση δεδομένων και μπορούν να ξαναχρησιμοποιηθούν.
- **Ημερολόγιο (Journal)**, για τη χρονική οργάνωση των εργασιών.
- **Εργαστήριο (Workshop)**, ένα είδος αξιολόγησης με πολλές επιλογές.
- **Εργασία (Assignment)**, δραστηριότητες με μορφή δοκιμίων, εκθέσεων ή ασκήσεων, που οφείλουν να ετοιμάσουν οι εκπαιδευόμενοι και να αποστείλουν στον εκπαιδευτή και μπορούν να βαθμολογηθούν.
- **Δημοσκόπηση (Choice)**, για την εξακρίβωση της γνώμης των εκπαιδευομένων πάνω σε συγκεκριμένο ερώτημα που αφορά το μάθημα.

- **Ενότητα (Lesson)**, με σκοπό να κάνει την παρουσίαση του μαθήματος ευέλικτη και ενδιαφέρουσα μέσα από πολυσέλιδο περιεχόμενο στο οποίο περιλαμβάνονται κείμενο, γραφικά κλπ.
- **Διάλογος (Dialogue)**, δηλαδή μια κλειστή συζήτηση μεταξύ δυο συμμετεχόντων στο μάθημα.
- **Έρευνα (Survey),** σύνολο τυποποιημένων ερευνών, όπου οι εκπαιδευόμενοι εκφράζουν τις απόψεις τους για το μάθημα και τις διαδικασίες του, με σκοπό να βοηθηθεί ο εκπαιδευτής στο να διαπιστώσει πόσο αποτελεσματικό είναι το μάθημα του και να εντοπίσει πιθανά προβλήματα.
- **Wiki,** εργαλείο που επιτρέπει τη συλλογική συγγραφή αρχείων σε απλή γλώσσα προγραμματισμού, χρησιμοποιώντας web browser.
- **SCORM**, που βοηθά στην εύκολη φόρτωση ενός πακέτου SCORM με ιστοσελίδες, γραφικά, προγράμματα Javascript, παρουσιάσεις κλπ., ώστε να καταστεί τμήμα των μαθημάτων.
- **Απουσιολόγιο (Attendance)**, για την παρακολούθηση της παρουσίας των εκπαι-δευομένων σε ένα μάθημα ή μια δραστηριότητα.
- **Αποθετήριο (Repository)**, όπου μπορούν να καταχωρηθούν διάφορες πληροφορίες, δεδομένα και αρχεία από τον εκπαιδευτή ή τους εκπαιδευόμενους.
- **Εξωτερικό Εργαλείο (External Tool)**, ενσωμάτωση εξωτερικού μαθησιακού εργαλείου μέσα στο περιβάλλον του Moodle, με δυνατότητα ανταλλαγής δεδομένων μέσω του προτύπου διαλειτουργικότητας μαθησιακών εργαλείων LTI. Παράδειγμα ενσωμάτωσης εξωτερικού εργαλείου είναι η χρήση εξωτερικής υπηρεσίας εξετάσεων με δυνατότητα μεταφοράς των βαθμολογιών προς το Moodle.

Τέλος, στο περιβάλλον του Moodle είναι ενσωματωμένα διάφορα προγράμματα εφαρμογών, όπως επεξεργαστής κειμένου, ημερολόγιο γεγονότων, μηχανή αναζήτησης, καταγραφικό σύστημα δραστηριότητας χρηστών καθώς και γενικού τύπου διαχειριστικές δυνατότητες όπως δυνατότητα δημιουργίας αντιγράφων ασφαλείας, δυνατό σύστημα βοήθειας, δυνατότητα ομαδοποίησης χρηστών καθώς και δυνατότητα ορισμού δικαιωμάτων σε επίπεδο χρήστη ή ομάδας.

Ασφάλεια Πληροφοριών στα ΣΔΗΜ

Ένα σύστημα διαχείρισης ηλεκτρονικής μάθησης έχει αποθηκευμένα ευαίσθητα δεδομένα τα οποία διακινούνται μεταξύ των χρηστών με στόχο την εκπαίδευση και την ενημέρωση. Επίσης, προσφέρει υπηρεσίες οι οποίες θα πρέπει να βασίζονται σε απόλυτα ασφαλείς διαδικασίες. Για παράδειγμα, η διαχείριση προσωπικών στοιχείων χρηστών, η διαδικασία εξετάσεων σε ένα περιβάλλον η-μάθησης, η διακίνηση εσωτερικών εταιρικών εγγράφων αποτελούν κρίσιμες διαδικασίες ενός τέτοιου πληροφοριακού συστήματος οι οποίες θα πρέπει να εκτελούνται με απόλυτα ασφαλή τρόπο. Όπως γίνεται αντιληπτό η ανάγκη που προκύπτει για ασφάλεια πληροφοριών σε ένα σύστημα διαχείρισης η-μάθησης εξαρτάται από το είδος της πληροφορίας την οποία διαχειρίζεται. Επίσης η αρχιτεκτονική σχεδίασης και η ανάγκη για διαλειτουργικότητα ενός τέτοιου συστήματος αυξάνουν τον κίνδυνο ασφάλειας καθώς το περιβάλλον η-μάθησης γίνεται πιο ευάλωτο σε απειλές.

Ένας κίνδυνος ασφάλειας πληροφοριών ορίζεται ως η αλλαγή από μια γνωστή σε μια άγνωστη και αβέβαιη κατάσταση συστήματος κατά την οποία η ομαλή λειτουργία των υπηρεσιών του συστήματος κινδυνεύει σε μεγάλο βαθμό [55].

Ενας πιο ακριβής ορισμός είναι ο εξής:

> *Ένας κίνδυνος ασφάλειας πληροφοριών εξαρτάται από την πιθανότητα μιας απειλής[10] να εκμεταλλευτεί μια δυνητική ευπάθεια[11] ενός πόρου[12] του συστήματος.* [55]

Η υιοθέτηση αντιμέτρων ασφάλειας σε ένα περιβάλλον ηλεκτρονικής μάθησης κρίνεται απαραίτητη καθώς η αρχιτεκτονική τέτοιων συστημάτων και η κεντρικοποιημένη αποθεση δεδομένων δημιουργεί πολλαπλές ευπάθειες οι οποίες πρέπει να αντιμετωπιστούν.

Αρχικά θα μελετηθούν οι περιπτώσεις χρήσης ενός συστήματος διαχείρισης ηλεκτρονικής μάθησης βάσει των κατηγοριών χρηστών που διαθέτει. Είναι κατανοητό ότι κάθε χρήστης, ανάλογα με την κατηγορία στην οποία ανήκει, έχει συγκεκριμένα δικαιώματα το οποίο συνεπάγεται ότι η πλοηγητική δραστηριότητα μέσα σε ένα περιβάλλον η-μάθησης διαφέρει ανά κατηγορία. Συνεπώς οι απειλές ασφάλειας που δημιουργούνται είναι διαφορετικές για κάθε είδος χρήστη και με διαφορετικό βαθμό επικινδυνότητας.

3.1 Δραστηριότητα Χρηστών και Απειλές Ασφάλειας Πληροφοριών

Οι χρήστες ενός συστήματος διαχείρισης ηλεκτρονικής μάθησης κατατάσσονται στις εξής τρεις διακριτές κατηγορίες: Εκπαιδευτής, Εκπαιδευόμενος, Διαχειριστής. Οι κατηγορίες αυτές

---

[10] Κάθε κακόβουλη δραστηριότητα η οποία έχει ως στόχο να εκμεταλλευτεί κάποια ευπάθεια. Για παράδειγμα μη εξουσιοδοτημένη υποκλοπή, διακοπή λειτουργίας, τροποποίηση ή διαγραφή δεδομένων, πλαστογράφηση είναι μερικές από τις απειλές που πρέπει να αντιμετωπιστούν σε ένα πλαίσιο ασφάλειας το οποίο διέπει ένα πληροφοριακό σύστημα.

[11] Αδυναμίες ασφάλειας πληροφοριών οι οποίες είναι ικανές να προκαλέσουν δυσλειτουργία ή ζημιά σε ένα πληροφοριακό σύστημα. Για παράδειγμα η επιλογή αδύναμου κωδικού πρόσβασης ή οι αδύναμες μέθοδοι αυθεντικοποίησης χρήστη.

[12] Πόρος συστήματος είναι κάθε στοιχείο από το οποίο απαρτίζεται ένα πληροφοριακό σύστημα (υποσύστημα το οποίο υλοποιεί μια συγκεκριμένη λειτουργικότητα ή υπηρεσία, προσωπικά δεδομένα χρήστη, εκπαιδευτικό περιεχόμενο κα)

ορίζουν αυτόματα τα δικαιώματα και τις δυνατότητες που έχει κάθε χρήστης στα διάφορα υποσυστήματα που απαρτίζουν ένα περιβάλλον η-μάθησης. Για παράδειγμα, στο υποσύστημα των ηλεκτρονικών εξετάσεων, ένας εκπαιδευτής έχει δικαίωμα να δημιουργήσει ένα ηλεκτρονικό τεστ ενώ ο εκπαιδευόμενος οφείλει να το λύσει και να το αποστείλει ηλεκτρονικά. Πρόκειται για δύο οπτικές γωνίες του ίδιου υποσυστήματος. Πιο συγκεκριμένα [51],

Εκπαιδευτής

Ένας εκπαιδευτής έχει ως κύρια αρμοδιότητα τη διδασκαλία, την καθοδήγηση και την παρακολούθηση της απόδοσης των εκπαιδευομένων που είναι εγγεγραμμένοι στα μαθήματα τους. Πια αναλυτικά,

- Διαχείριση προσωπικού προφίλ: δημιουργία λογαριασμού, αλλαγή κωδικού πρόσβασης, επικαιροποίηση προσωπικών στοιχείων.
- Διαχείριση ηλεκτρονικού μαθήματος
    1. Δημιουργία μαθήματος περιλαμβάνοντας βασικές πληροφορίες σχετικά με την εγγραφή (ημερομηνίες, προαπαιτούμενες γνώσεις), κανόνες και πολιτικές παρακολούθησης του μαθήματος.
    2. Δημιουργία ηλεκτρονικού εκπαιδευτικού υλικού και προσάρτησή του με δομημένο τρόπο σε μάθημα.
    3. Δημιουργία ηλεκτρονικού υλικού αξιολόγησης και προσάρτηση του με δομημένο τρόπο σε μάθημα.
    4. Ανάθεση εργασιών με δυνατότητα μεταφόρτωση τους από τους εκπαιδευόμενους.
    5. Δημιουργία κλίμακας βαθμολόγησης για κάθε μάθημα ξεχωριστά.
    6. Αξιολόγηση/βαθμολόγηση των μεταφορτωμένων εργασιών και αυτοματοποιημένη ενημέρωση τους με τα αποτελέσματα.
    7. Δημιουργία ηλεκτρονικών εξετάσεων και αυτόματη βαθμολόγηση των εκπαιδευομένων.
    8. Ενεργοποίηση και χρήση υπηρεσίας αυτόματης ενημέρωσης για πιθανές αλλαγές στη δομή και το περιεχόμενο του μαθήματος.
    9. Ενεργοποίηση και χρήση σύγχρονων (chat) και ασύγχρονων (forums) μεθόδων επικοινωνίας για τον εμπλουτισμό της εκπαιδευτικής διαδικασίας μέσω της ενισχυμένης συνεργατικότητας.
    10. Εγγραφή μαθητών σε μάθημα το οποίο είναι υπεύθυνος/η.

Απειλές ασφάλειας για τον εκπαιδευτή

Οι δραστηριότητες ενός εκπαιδευτή μέσα σε ένα περιβάλλον ηλεκτρονικής μάθησης μπορούν να εκθέσουν το σύστημα σε κινδύνους ασφάλειας καθώς μια κακόβουλη πρόθεση μπορεί να οδηγήσει στην αλλοίωση δεδομένων και κρίσιμων πληροφοριών των εκπαιδευτών. Πιο συγκεκριμένα:

- Πρόσβαση και τροποποίηση των προσωπικών πληροφοριών του εκπαιδευτή από μη εξουσιοδοτημένο χρήστη
- Δημιουργία ψεύτικου εκπαιδευτικού περιεχομένου και προσθήκη του στη δομή του μαθήματος
- Προβολή, τροποποίηση και διαγραφή εκπαιδευτικού υλικού από ένα μάθημα από μη εξουσιοδοτημένο άτομο
- Αλλοίωση ηλεκτρονικών εξετάσεων: πρόσβαση στα θέματα πριν από την έναρξη των εξετάσεων, τροποποίηση ερωτήσεων εξέτασης, διαγραφή της ενεργής ηλεκτρονικής εξέτασης, συμμετοχή σε εξετάσεις από μη εξουσιοδοτημένο άτομο ή κακόβουλο εκπαιδευόμενο.
- Τροποποίηση κλίμακας βαθμολόγησης εργασιών και ηλεκτρονικών εξετάσεων
- Πρόσβαση, τροποποίηση και διαγραφή αποτελεσμάτων και βαθμών ηλεκτρονικών εξετάσεων και εργασιών από μη εξουσιοδοτημένο χρήστη.
- Συμμετοχή στα εργαλεία επικοινωνίας (chat, forums) από μη εξουσιοδοτημένα άτομα.

Εκπαιδευόμενος

Όσοι ανήκουν σε αυτή την κατηγορία χρηστών έχουν τη δυνατότητα να παρακολουθήσουν και να συμμετέχουν σε ένα ηλεκτρονικό μάθημα. Μερικές από τις δυνατότητες που προσφέρει ένα σύστημα διαχείρισης ηλεκτρονικής μάθησης στους εκπαιδευόμενου είναι οι εξής:

- Διαχείριση προσωπικού προφίλ: δημιουργία λογαριασμού, αλλαγή κωδικού πρόσβασης, επικαιροποίηση προσωπικών στοιχείων.
- Συμμετοχή σε ηλεκτρονικά μαθήματα
    1. Πρόσβαση στο εκπαιδευτικό περιεχόμενο
    2. Δυνατότητα μεταφόρτωσης εργασιών αξιολόγησης που έχει αναθέσει ο εκπαιδευτής.
    3. Συμμετοχή στις ηλεκτρονικές εξετάσεις αξιολόγησης
    4. Πρόσβαση στα αποτελέσματα εργασιών και εξετάσεων.
    5. Χρήση υπηρεσίας αυτόματης ενημέρωσης για πιθανές αλλαγές του εκπαιδευτικού περιεχομένου ή της εκπαιδευτικής διαδικασίας

6. Χρήση των σύγχρονων και ασύγχρονων μεθόδων επικοινωνίας με τους εκπαιδευτές και τους εκπαιδευόμενους.

Απειλές ασφάλειας για τον εκπαιδευόμενο

Οι δραστηριότητες ενός εκπαιδευτή μέσα σε ένα περιβάλλον ηλεκτρονικής μάθησης μπορούν να εκθέσουν το σύστημα σε κινδύνους ασφάλειας καθώς μια κακόβουλη πρόθεση μπορεί να οδηγήσει στην αλλοίωση δεδομένων και κρίσιμων πληροφοριών των εκπαιδευτών. Πιο συγκεκριμένα:

- Πρόσβαση και τροποποίηση των προσωπικών πληροφοριών του εκπαιδευόμενου από μη εξουσιοδοτημένο χρήστη.
- Πρόσβαση σε εκπαιδευτικό περιεχόμενο από μη εξουσιοδοτημένο άτομο.
- Αλλοίωση ηλεκτρονικών εξετάσεων : Χρήση προσωπικών στοιχείων ταυτοποίησης και αυθεντικοποίησης για να συμμετέχει εκ μέρους του εκπαιδευόμενου ένα μη εξουσιοδοτημένο άτομο σε ηλεκτρονικές εξετάσεις.
- Πρόσβαση σε εργασίες του εκπαιδευόμενου με στόχο την τροποποίηση, διαγραφή και υποκλοπή τους.
- Πρόσβαση σε βαθμολογίες του εκπαιδευόμενου με στόχο την τροποποίηση κα διαγραφή τους.

Διαχειριστής Συστήματος

Οι διαχειριστές σε όλα τα πληροφοριακά συστήματα έχουν ως κύρια αρμοδιότητα την αδιάλειπτη, ομαλή και ασφαλή λειτουργία του συστήματος. Συγκεκριμένα, ένας διαχειριστής συστήματος ηλεκτρονικής μάθησης έχει τις παρακάτω δυνατότητες:

- Διαχείριση προφίλ όλων των χρηστών του συστήματος
- Δημιουργία και ρύθμιση ρόλων και εκχώρηση αντίστοιχων δικαιωμάτων στους εκπαιδευτές και εκπαιδευόμενους
- Ανάθεση μαθήματος σε εκπαιδευτές και εκχώρηση αυξημένων δικαιωμάτων στα αντίστοιχα μαθήματα
- Συντήρηση συστήματος (π.χ. δημιουργία αντιγράφων ασφάλειας, αντιμετώπιση λειτουργικών προβλημάτων, ενημέρωση λογισμικού κα.)

Απειλές ασφάλειας για τους διαχειριστές

Για να μπορέσει ένας διαχειριστής να ελέγχει και να παρακολουθεί αποτελεσματικά την απόδοση ενός πληροφοριακού συστήματος, έχει καθολικά δικαιώματα σε όλα τα υποσυστήματα που το απαρτίζουν. Αυτό σημαίνει ότι οι κίνδυνοι ασφάλειας πληροφοριών που μπορεί να αντιμετωπίσει ένας διαχειριστής είναι κρίσιμης σημασίας καθώς είναι ικανοί

να προκαλέσουν αλυσιδωτά προβλήματα στην ομαλή λειτουργία του συστήματος. Ένα κακόβουλο μη εξουσιοδοτημένο άτομο έχει τις παρακάτω δυνατότητες:

- Πρόσβαση, τροποποίηση, διαγραφή προσωπικών στοιχείων όλων των εγγεγραμμένων χρηστών από μη εξουσιοδοτημένο άτομο.
- Τροποποίηση ρόλων και δικαιωμάτων των εγγεγραμμένων χρηστών του συστήματος.
- Αλλοίωση όλων των διαδικασιών που απαρτίζουν την εκπαιδευτική διαδικασία ενός ηλεκτρονικού μαθήματος (εκπαιδευτικό υλικό, ανάθεση εργασιών αξιολόγησης, διεξαγωγή ηλεκτρονικών εξετάσεων, κλίμακα βαθμολόγησης , μηχανισμοί σύγχρονης και ασύγχρονης επικοινωνίας)
- Αλλοίωση και τερματισμό των διαδικασιών συντήρησης και εποπτείας του συστήματος (π.χ. δημιουργία αντιγράφων ασφάλειας, παρακολούθηση δραστηριότητας χρηστών, ενημερώσεις λογισμικού)

3.2 Απαιτήσεις και Αντίμετρα Ασφάλειας Πληροφοριών στο Moodle

Στην ενότητα αυτή θα γίνει έρευνα σχετικά με την υλοποίηση της ασφάλειας πληροφοριών στην πλατφόρμα του Moodle βάσει των έξι απαιτήσεων ασφάλειας: Ταυτοποίηση και Αυθεντικοποίηση, Εξουσιοδότηση, Εμπιστευτικότητα, Ακεραιότητα, Μη Άρνηση της Ευθύνης, Διαθεσιμότητα [24]. Πιο συγκεκριμένα, θα περιγραφούν οι υλοποιημένοι μηχανισμοί-αντίμετρα ασφάλειας [33] που ικανοποιούν τις παραπάνω απαιτήσεις και θα αντιπαρατεθούν με προτεινόμενα αντίμετρα σύμφωνα με τη βιβλιογραφία.

3.2.1 Ταυτοποίηση και Αυθεντικοποίηση

Στόχος της απαίτησης αυτής είναι να επιτρέπει την πρόσβαση μόνο σε εγκεκριμένους χρήστες όπως επίσης και να αποτρέπει την παράνομη είσοδο χρηστών μέσα στο περιβάλλον του συστήματος ηλεκτρονικής μάθησης.

Το Moodle επιτρέπει την πρόσβαση σε ανώνυμους χρήστες, επισκέπτες και εγγεγραμμένους χρήστες.

Ανώνυμοι Χρήστες: η χρήση του Moodle επιτρέπεται χωρίς καμία πληροφορία ταυτοποίησης. Οι ανώνυμοι χρήστες έχουν περιορισμένα δικαιώματα.

Επισκέπτες: Χρήστες με ορισμένα δικαιώματα πρόσβασης στο διαθέσιμο υλικό του Moodle για τους οποίους δεν απαιτείται πρότερη εγγραφή στο σύστημα.

Εγγεγραμμένοι Χρήστες: Χρήστες που έχουν εγγραφεί στη βάση δεδομένων του Moodle και οι οποίοι έχουν μοναδική ταυτότητα και κωδικό πρόσβασης.

Το Moodle χρησιμοποιεί μηχανισμό βασισμένο σε κωδικό πρόσβασης χρησιμοποιώντας τρεις τρόπους για να διαχειρίζεται τη διαδικασία αυθεντικοποίησης

- **Αυτοεγγραφή με λογαριασμό ηλεκτρονικού ταχυδρομείου**: Οι χρήστες επιλέγουν όνομα χρήστη και κωδικό πρόσβασης και στη συνέχεια αποστέλλεται email επιβεβαίωσης στο λογαριασμό του χρήστη. Με αυτό τον τρόπο η εγγραφή του χρήστη

είναι ελεγχόμενη. Μόλις ο χρήστης εισέρχεται στο σύστημα, συγκρίνονται τα διαπιστευτήρια που εισάγει ο χρήστης με τις τιμές που είναι αποθηκευμένες στη βάση δεδομένων του Moodle.

- **Μη αυτόματη εγγραφή**: Οι λογαριασμοί χρηστών του Moodle δημιουργούνται από το διαχειριστή του συστήματος.
- **Απαγόρευση εισόδου**: Χρησιμοποιείται από το διαχειριστή για την απαγόρευση εισόδου σε συγκεκριμένους λογαριασμούς χρηστών.

Το Moodle χρησιμοποιεί δύο τρόπους αυθεντικοποίησης: μέσω εξωτερικής βάσης δεδομένων (MySQL ή PostgreSQL) ή μέσω εξωτερικού εξυπηρετητή (LDAP, IMAP, Moodle Network, NNTP, POP3, Shibboleth, RADIUS, CAS, Web Services).

Για την ενίσχυση της ταυτοποίησης χρησιμοποιούνται επιπλέον χαρακτηριστικά ασφάλειας:

- Ισχυρός κωδικός πρόσβασης χρησιμοποιώντας δύσκολους συνδυασμούς χαρακτήρων και ψηφίων
- Υποχρεωτική υποβολή ονόματος χρήστη και κωδικού πρόσβασης μετά το πέρας συγκεκριμένου χρονικού διαστήματος αδράνειας.

3.2.2 Εξουσιοδότηση

Η απαίτηση ασφάλειας της εξουσιοδότησης διασφαλίζει την ελεγχόμενη πρόσβαση χρηστών στο περιεχόμενο του Moodle που επιτρέπεται να έχει πρόσβαση.

Το Moodle υποστηρίζει μηχανισμούς ελέγχου πρόσβασης βασισμένη σε ρόλους (Role Based Access Control - RBAC) σύμφωνα με τον οποίους ρόλοι δραστηριοτήτων εκχωρούνται στους χρήστες**.** Με αυτό τον τρόπο κάθε χρήστης έχει διάφορους ρόλους συσχετισμένους με το λογαριασμό του οι οποίοι δίνουν τα απαραίτητα δικαιώματα ανάλογα με την κατηγορία χρηστών που ανήκουν.

3.2.3 Εμπιστευτικότητα

Η απαίτηση ασφάλειας της εμπιστευτικότητας εγγυάται την προβολή του περιεχομένου του Moodle μόνο από εξουσιοδοτημένους χρήστες. Πιο συγκεκριμένα, το Moodle για την υλοποίηση της απαίτησης χρησιμοποιεί τους παρακάτω μηχανισμούς:

- Δημιουργία ενός μοναδικού κλειδιού εγγραφής το οποίο εκχωρείται σε κάθε πόρο που πρέπει να ελέγχεται η πρόσβαση. Για την πρόσβαση στον πόρο, ο χρήστης είναι υποχρεωμένος να γνωρίζει το κλειδί.
- Χρήση πρωτοκόλλου ασφάλειας SSL[13] για την κρυπτογράφηση του καναλιού επικοινωνίας πελάτη εξυπηρετητή κατά την υποβολή των διαπιστευτηρίων του χρήστη (όνομα χρήστη και κωδικό πρόσβασης).

[13] Secure Socket Layer

3.2.4 Ακεραιότητα

Η απαίτηση ασφάλειας της ακεραιότητας εγγυάται την τροποποίηση του περιεχομένου μόνο από εξουσιοδοτημένους χρήστες προστατεύοντας τα δεδομένα από υποκλοπή, διαγραφή και αλλοίωση. Βάσει της γραπτής τεκμηρίωσης του Moodle δεν υπάρχει κάποιος συγκεκριμένος μηχανισμός που να διασφαλίζει την ακεραιότητα παρά μόνο οι μηχανισμοί ταυτοποίησης και εμπιστευτικότητας που ικανοποιούν έμμεσα την απαίτηση.

3.2.5 Μη Άρνηση της ευθύνης

Η απαίτηση ασφάλειας της μη άρνησης της ευθύνης διασφαλίζει την προσωποποίηση των ενεργειών των χρηστών με στόχο τον αποκλεισμό της πιθανότητας κάποιος χρήστης να αρνηθεί την προέλευση της ενέργειας.

Το Moodle έχει ενσωματωμένο μηχανισμό καταγραφής δραστηριότητας χρηστών ο οποίος χρησιμοποιείται τόσο για την ενημέρωση των εκπαιδευτών όσο και για την επίβλεψη του συστήματος από τους διαχειριστές, καταγράφοντας το ιστορικό χρήσης του κάθε χρήστη.

3.2.6 Διαθεσιμότητα

Η απαίτηση ασφάλειας της διαθεσιμότητας εγγυάται την αδιάλειπτη παροχή υπηρεσιών η-μάθησης προς τους χρήστες του Moodle.

Πιο συγκεκριμένα, το Moodle έχει δυνατότητα αυτοματοποιημένης διαδικασίας δημιουργίας αντιγράφων ασφάλειας τόσο για το κάθε μάθημα όσο και για το σύστημα διατηρώντας με αυτό τον τρόπο ακέραια όλα τα δεδομένα της βάσης δεδομένων και του καταλόγου αρχείων.

Συμπέρασμα

Όπως γίνεται αντιληπτό από τα παραπάνω σενάρια χρήσης ενός συστήματος ηλεκτρονικής μάθησης (εκπαιδευτής, εκπαιδευόμενος, διαχειριστής) αλλά και τα αντίμετρα ασφάλειας που υλοποιεί ένα πραγματικό ΣΔΗΜ όπως το Moodle , οι απειλές ασφάλειας σε ένα τέτοιου είδους πληροφοριακού συστήματος είναι ικανοί να παραβιάσουν τις βασικές απαιτήσεις ασφάλειας πληροφοριών (αυθεντικοποίηση, εξουσιόδοτηση, εμπιστευτικότητα, ακεραιότητα, μη άρνηση της ευθύνης, διαθεσιμότητα). Επομένως, για τη βιωσιμότητα ενός τέτοιου συστήματος θα πρέπει να οριστεί ένα ολοκληρωμένο πλαίσιο ασφάλειας πληροφοριών προσανατολισμένο σε περιβάλλοντα ηλεκτρονικής μάθησης να υλοποιηθούν αντίμετρα ασφάλειας τα οποία έχουν ως στόχο την εξάλειψη του κινδύνου ασφάλειας.

Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών σε Περιβάλλοντα η-Μάθησης

Λαμβάνοντας υπόψη τόσο τη δραστηριότητα των χρηστών όσο και την σημαντικότητα των πληροφοριών που εκείνοι διαχειρίζονται, μπορούμε να αντιληφθούμε ότι τα ΣΔΗΜ αντιμετωπίζουν μεγάλες αδυναμίες (vulnerabilities) ασφάλειας για τις οποίες θα πρέπει να εφαρμοστούν μέτρα ικανά να αντιμετωπίσουν κάθε πιθανή απειλή. Πολλά από αυτά τα συστήματα παρέχουν βασικούς μηχανισμούς ασφάλειας όπως αυθεντικοποίηση με κωδικό για την προστασία των πληροφοριακών αποθετηρίων, κρυπτογραφημένη επικοινωνία για ορισμένα τμήματα του συστήματος, όμως για να μπορέσει ένα τέτοιου είδους σύστημα να μετατραπεί σε ασφαλές θα πρέπει να πληροί ορισμένες προδιαγραφές και πιο συγκεκριμένα, να εμπίπτει σε ένα πλαίσιο ασφάλειας το οποίο θα ορίζει τους κανόνες αλλά και τις διαδικασίες που απαιτούνται έτσι ώστε το περιβάλλον η-μάθησης να ικανοποιεί τις έξι βασικές απαιτήσεις ασφάλειας:

- Αυθεντικοποίηση (Authentication and Identification)
- Εξουσιοδότηση (Authorization)
- Εμπιστευτικότητα και Ιδιωτικότητα (Confidentiality and Privacy)
- Ακεραιότητα πληροφοριών (Information Integrity)
- Μη άρνηση της ευθύνης (Non-denial)
- Διαθεσιμότητα (Availability)

Στόχος του κεφαλαίου αυτού είναι να προταθεί και να οριστεί ένα Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών προσανατολισμένο και προσαρμοσμένο στις ανάγκες των ΣΔΗΜ, και γενικότερα σε περιβάλλοντα η-μάθησης, βασισμένο στο πρότυπο 27002[14] του Διεθνούς Οργανισμού Προτυποποίησης[15] (International Organization for Standardization - ISO).

4.1 ISO 27001 και ISO 27002

Τα πρότυπα 27001 και 27002 ανήκουν στην σειρά προτύπων ISO/IEC 27000 η οποία περιλαμβάνει διεθνή πρότυπα ασφάλειας πληροφοριών δημοσιευμένα από το Διεθνή Οργανισμό Προτυποποίησης (ISO) και τη Διεθνή Ηλεκτροτεχνική Επιτροπή (IEC). Πιο συγκεκριμένα, το 27001 ορίζει τις προδιαγραφές ενός συστήματος διαχείρισης ασφάλειας πληροφοριών ενώ το πρότυπο 27002 παρέχει προτάσεις καλών πρακτικών για τη διαχείριση ασφάλειας πληροφοριών.

Όπως αναφέρθηκε, στη συνέχεια θα οριστεί ένα Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών βασισμένο στις καλές πρακτικές που αναφέρονται στο πρότυπο 27002, προσανατολισμένο στα περιβάλλοντα η-μάθησης.

[14] ISO 27002 - Το πρότυπο ISO 27002 είναι μια ευρέως αποδεκτή πρακτική για τη Διαχείριση Ασφάλειας Πληροφοριών.

[15] ISO – International Organization for Standardization

4.2 Ασφάλεια Πληροφοριών

Η πληροφορία αποτελεί έναν σημαντικό πόρο ο οποίος θα πρέπει να προστατεύεται κατάλληλα για την ομαλή και ασφαλή λειτουργία ενός οργανισμού. Η ανάγκη αυτή αυξάνεται και κρίνεται απαραίτητη όταν ο οργανισμός αυτός ανήκει σε ένα διασυνδεδεμένο επιχειρησιακό περιβάλλον όπου η πληροφορία εκτίθεται σε ένα συνεχώς αυξανόμενο σύνολο απειλών με διαφορετικά χαρακτηριστικά.

«Ασφάλεια πληροφοριών *είναι η διαδικασία προστασίας της πληροφορίας όπως επίσης και των συστημάτων που τη διαχειρίζονται από ένα μεγάλο εύρος απειλών με σκοπό τη διασφάλιση της επιχειρησιακής συνέχειας, την ελαχιστοποίηση του επιχειρησιακού κινδύνου αλλά και τη μεγιστοποίηση της εμπιστοσύνης προς τον οργανισμό.»* [23]

«Ασφάλεια πληροφοριών *είναι η προστασία των πληροφοριών και των πληροφοριακών συστημάτων από το μη εξουσιοδοτημένη πρόσβαση, χρήση, δημοσιοποίηση, διακοπή, αλλαγή, επιθεώρηση, καταστροφή με στόχο τη διασφάλιση των βασικών απαιτήσεων ασφάλειας.»* (United States Code)

Εγκαθιστώντας ένα λογισμικό προστασίας από ιούς ή ρυθμίζοντας ένα ισχυρό τείχος προστασίας είναι μερικά παραδείγματα αντιμέτρων ασφάλειας που θα μπορούσαν να χρησιμοποιηθούν για να προστατεύσουν προσωπικές πληροφορίες και δεδομένα. Τα περισσότερα ΣΔΗΜ υλοποιούν βασικούς μηχανισμούς ασφάλειας για την προστασία του δικτύου ή της βάσης δεδομένων, όμως με αυτό τον τρόπο δεν εξασφαλίζεται η βιωσιμότητα της ασφαλούς λειτουργίας τους. Η επίτευξη της ασφάλειας σε ένα τέτοιο σύστημα αποτελεί μια πολυδιάστατη θεμελίωση η οποία απαιτεί την υλοποίηση ενός **κατάλληλου** συνόλου αντιμέτρων που περιλαμβάνει πολιτικές ασφάλειας, διαδικασίες, τρόπους ενέργειας, οδηγούς και πρακτικές αντιμετώπισης κινδύνων, οργανωτικές δομές όπως επίσης και τη συμβολή του λογισμικού και του υλικού. Τα αντίμετρα αυτά μπορούν να είναι διαχειριστικής, διοικητικής, νομικής και τεχνικής φύσης πράγμα το οποίο καθιστά εύκολο να αντιληφθούμε ότι κατά την επίτευξη της ασφάλειας σε ένα πληροφοριακό σύστημα, όπως ένα ΣΔΗΜ, θα πρέπει να λάβουμε υπόψη όλες τις συνιστώσες ασφάλειας και όχι μόνο την τεχνική. [49]

Οι συνιστώσες ασφάλειας που θα πρέπει να υλοποιηθούν σε ένα ΣΔΗΜ και οι οποίες βασίζονται στο πρότυπο ISO 27002 είναι οι ακόλουθες [23] [49]:

- Διοίκηση Ασφάλειας Πληροφοριών
- Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών
- Ευαισθητοποίηση/Ενημέρωση Χρηστών
- Διαχείριση και Αντιμετώπισης Περιστατικών Ασφάλειας
- Σύστημα Μέτρησης Ασφάλειας ΠΣ
- Υιοθέτηση και Υλοποίηση Αντιμέτρων Ασφάλειας (τεχνική συνιστώσα)

Οι παραπάνω συνιστώσες ασφάλειας αποτελούν σύμφωνα με το ISO 27002 τους κρίσιμους παράγοντες επίτευξης ενός ασφαλούς πληροφοριακού συστήματος και ταυτόχρονα ορίζουν ένα Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών το οποίο μπορεί να εφαρμοστεί σε οργανισμούς που χρησιμοποιούν Συστήματα Διαχείρισης η-Μάθησης.

4.2.1 Διοίκηση Ασφάλειας Πληροφοριών

Πρόκειται για ένα από τα κρίσιμα στοιχεία για την επιτυχή υλοποίηση και διατήρηση της ασφάλειας πληροφοριών σε ένα πληροφοριακό σύστημα και αποτελεί τον τρόπο και οδηγό διαχείρισης της ασφάλειας μέσα στον οργανισμό. [23] [24]

Η Διοίκηση Ασφάλειας Πληροφοριών περιλαμβάνει ένα

- Πλαίσιο διοίκησης ασφάλειας το οποίο απαιτείται για την εκκίνηση και έλεγχο της υλοποίησης ασφάλειας μέσα στον οργανισμό.

  Η διοίκηση θα πρέπει να

  - εγκρίνει τις πολιτικές και διαδικασίες ασφάλειας.
  - δεσμευτεί για την τήρηση των πολιτικών αυτών.
  - αναθέσει ρόλους και αρμοδιότητες ασφάλειας σε κατάλληλα εκπαιδευμένους ανθρώπους του οργανισμού.
  - να συντονίζει και να επιθεωρεί την υλοποίηση της ασφάλειας σε όλο τον οργανισμό με σκοπό τη διασφάλιση της αποτελεσματικότητας των αντιμέτρων ασφάλειας.
  - συνάψει συμφωνίες εμπιστευτικότητας οι οποίες θα ορίζουν
    - την ανάγκη για προστασία κρίσιμων πληροφοριών του οργανισμού.
    - τις κρίσιμες πληροφορίες.
    - και το νομικό πλαίσιο.
- Πρόγραμμα σεμιναρίων ενημέρωσης των χρηστών του πληροφοριακού συστήματος για τις πολιτικές ασφάλειας πληροφοριών με στόχο τη διασφάλιση της συμμόρφωσης των χρηστών με τους κανόνες ασφάλειας αλλά και την ευαισθητοποίηση τους απέναντι σε θέματα ασφάλειας .
- Αποτελεσματική εποπτεία ασφάλειας του πληροφοριακού συστήματος με στόχο την μέτρηση απόδοσης των πολιτικών ασφάλειας που έχουν υιοθετηθεί αλλά και την αποτελεσματικότητα των αντιμέτρων ασφάλειας που έχουν υλοποιηθεί.
- Σύστημα διαχείρισης και αντιμετώπισης περιστατικών ασφάλειας.

4.2.2 Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών

Σκοπός της συνιστώσας αυτής είναι να παρέχει μια κατεύθυνση και υποστήριξη της διοίκησης προς την ασφάλεια πληροφοριών οι οποίες να είναι σύμφωνες με τις απαιτήσεις του οργανισμού αλλά και με τους νόμους και τις διατάξεις που τον διέπουν [23] [27] [49].

Η διοίκηση θα πρέπει να αποσαφηνίσει και να χαράξει μια καθαρή πολιτική σύμφωνη με τους επιχειρησιακούς σκοπούς αλλά και να δεσμευτεί για τη διατήρηση μια ενιαίας πολιτικής ασφάλειας πληροφοριών η οποία θα διέπει όλο τον οργανισμό.

Κατά την υλοποίηση της πολιτικών και διαδικασιών ασφάλειας σε ένα ΣΔΗΜ δημιουργείται ένα Έγγραφο Πολιτικής Ασφάλειας Πληροφοριών το οποίο αποτελεί έναν οδηγό διοίκησης και διαχείρισης της ασφάλειας στο σύστημα από όλα τα εμπλεκόμενα μέρη. Σε αυτόν τον οδηγό θα πρέπει να αναφέρονται ρητά οι διοικητικές δεσμεύσεις και η

προσέγγιση του οργανισμού στη διαχείριση της ασφάλειας πληροφοριών. Τα περιεχόμενα του εγγράφου παρουσιάζονται συνοπτικά παρακάτω

- Ορισμός της ασφάλειας πληροφοριών, των γενικών σκοπών της και της σημασίας της στην μεταφορά πληροφοριών.
- Αναφορά στους σκοπούς της διοίκησης έτσι όπως διαμορφώνονται από την υιοθέτηση μηχανισμών ασφάλειας πληροφοριών σύμφωνους με την επιχειρησιακή στρατηγική.
- Συνοπτική περιγραφή και επεξήγηση των πολιτικών, αρχών, προτύπων και διαδικασιών ασφάλειας στην οποία περιλαμβάνονται:
  - Συμμόρφωση με τις νομοθετικές και ρυθμιστικές απαιτήσεις του οργανισμού.
  - Απαιτήσεις για εκπαίδευση, εξάσκηση και ενημέρωση σε θέματα ασφαλείας.
  - Συνέπειες παραβίασης πολιτικής ασφάλειας πληροφοριών.
- Αναφορά των ευθυνών στη διαχείριση ασφάλειας πληροφοριών.
- Παραπομπές στην γραπτή τεκμηρίωση της πολιτικής ασφάλειας έτσι ώστε να ενημερωθούν από μια λεπτομερή περιγραφή των πολιτικών και των διαδικασιών ασφάλειας.

Όπως προκύπτει, από τα περιεχόμενα του παραπάνω εγγράφου, οι πολιτικές ασφάλειας συνοδεύονται από την γραπτή τεκμηρίωση τους όπου υπάρχει λεπτομερής περιγραφή των πολιτικών και των διαδικασιών ασφάλειας.

Παράδειγμα Πολιτικής Κωδικού Πρόσβασης

Το Σύστημα Διαχείρισης η-Μάθησης χρησιμοποιεί μηχανισμό κωδικού πρόσβασης για την αυθεντικοποίηση ενός χρήστη. Ακολουθούν οι πολιτικές που θα πρέπει να εφαρμοστούν για να διασφαλιστεί η αποτελεσματικότητα του μηχανισμού.

<u>Κανόνες Χρηστών</u>

- Τα στοιχεία ταυτοποίησης (όνομα χρήστη και κωδικός πρόσβασης) είναι προσωπικά και δεν πρέπει να χρησιμοποιούνται από άλλο χρήστη, όπως επίσης και να καταγράφονται σε εμφανή σημεία για λόγους απομνημόνευσης.
- Ο κωδικός πρόσβασης θα πρέπει να αποτελείται από τουλάχιστον 6 χαρακτήρες.
- Ο κωδικός πρόσβασης θα πρέπει να αλλάζει κάθε 30 ημέρες.
- Για την αποφυγή υποκλοπής του κωδικού πρόσβασης, μην χρησιμοποιείτε εύκολα προβλέψιμους κωδικούς.
- Ο κωδικός πρόσβασης θα πρέπει να αποτελείται από ειδικούς χαρακτήρες, γράμματα(κεφαλαία και πεζά) και αριθμούς. Στόχος της πολιτικής αυτής είναι να μειωθεί η πιθανότητα πρόβλεψης του κωδικού αυξάνοντας την «δύναμη» του.
-

<u>Κανόνες Κωδικού Πρόσβασης στο ΣΔΗΜ</u>

- Κάθε χρήστης του συστήματος έχει μοναδική ταυτότητα. Με αυτόν τον τρόπο αποφεύγεται η ύπαρξη ομαδικής ταυτότητας.

- Το σύστημα θα πρέπει να παρέχει προειδοποίηση αλλαγής του κωδικού πρόσβασης όπως επίσης και ημερομηνία λήξης κωδικού η οποία θα επιβάλει την αλλαγή του.
- Τα σύστημα θα πρέπει να απαγορεύει τη χρησιμοποίηση εύκολων κωδικών μέσω ενός μηχανισμού ελέγχου και θα πρέπει να επιβάλει το συνδυασμό χαρακτήρων, αριθμών και ειδικών χαρακτήρων.
- Απαγόρευση εισόδου ύστερα από συγκεκριμένο αριθμό αποτυχημένων προσπαθειών.
- Σε περίπτωση που το σύστημα παραμείνει ανενεργό για συγκεκριμένο χρονικό διάστημα, θα κλειδώνει αυτόματα και θα επιβάλει την εισαγωγή του κωδικού πρόσβασης εκ νέου.
- Το σύστημα θα πρέπει να διατηρεί την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών αυθεντικοποίησης κατά τη διάρκεια μεταφοράς και αποθήκευσης δεδομένων μέσω μηχανισμών κρυπτογραφίας κατά τη διακίνηση και αποθήκευση των δεδομένων.
- Το σύστημα θα πρέπει να δίνει τη δυνατότητα αλλαγής του κωδικού πρόσβασης από το χρήστη για τις περιπτώσεις που ο χρήστης θεωρεί ότι είναι απαραίτητο.
- Υλοποίηση αυτοματοποιημένης φραγής εισόδου χρήστη ύστερα από συνεχόμενες αποτυχημένες προσπάθειες εισόδου στο σύστημα. Η διάρκεια της φραγής εισόδου σχετίζεται άμεσα με την κρισιμότητα των πληροφοριών του υποσυστήματος στο οποίο προσπαθούμε να εισέλθουμε.
- Ένα ΣΔΗΜ θα πρέπει να καταγράφει τις δραστηριότητες του χρήστη (χρησιμοποιώντας τις πληροφορίες αυθεντικοποίησης) όσο η σύνδεση του είναι ενεργή έτσι ώστε να διασφαλίσει τη απαίτηση ασφάλειας της μη άρνησης της ευθύνης.

4.2.3 Ευαισθητοποίηση/Ενημέρωση Χρηστών

Σύμφωνα με το ISO 27002, θεωρείται απαραίτητη η εκπαίδευση των χρηστών ενός πληροφοριακού συστήματος σχετικά με τις πολιτικές και διαδικασίες ασφάλειας. 'Ενα ολοκληρωμένο πακέτο τακτικής εκπαίδευσης και ενημέρωσης των χρηστών ενός πληροφοριακού συστήματος προάγει την ευαισθητοποίηση σε θέματα ασφάλειας και αποσαφηνίζει τις αρμοδιότητες ασφάλειας όλων των ρόλων των τελικών χρηστών. Στόχος αυτού του προγράμματος εκπαίδευσης είναι να δημιουργήσει τις αναγκαίες συνθήκες για τη θεμελίωση της ασφάλειας σε ένα πληροφοριακό σύστημα καθώς οι τελικοί χρήστες αναλαμβάνουν τις ευθύνες των ρόλων τους και συμμορφώνονται με τα μέτρα ασφάλειας [23], [49].

4.2.4 Διαχείριση και Αντιμετώπιση Περιστατικών Ασφάλειας

Για την υλοποίηση ενός ασφαλούς πληροφοριακού συστήματος, οι διαδικασίες αντιμετώπισης περιστατικών ασφάλειας αποτελούν μια αναγκαία συνθήκη για την επιτυχή

διαχείριση κρίσης. Τα βασικά στοιχεία των διαδικασιών αυτών περιγράφονται παρακάτω [15] [23]:

- Συγκρότηση ομάδας αντιμετώπισης περιστατικών ασφάλειας η οποία θα έχει ως αρμοδιότητες:
  - Συλλογή αναφορών περιστατικών ασφάλειας
  - Καταγραφή και καταχώρηση των πληροφοριών που περιέχει η αναφορά. (Εμπλουτισμός βάσης καταγραφής περιστατικών)
  - Συλλογή περισσότερων πληροφοριών σχετικών με το περιστατικό
  - Έλεγχος αν το περιστατικό εμπίπτει σε κάποιο ήδη καταχωρημένο περιστατικό
  - Ανάλυση των δεδομένων/πληροφοριών είτε το περιστατικό έχει ήδη καταγραφεί είτε πρόκειται για καινούρια απειλή
  - Αντιμετώπιση περιστατικού βασισμένη σε προτεινόμενες δράσεις που προέκυψαν από την ανάλυση
  - Καταγραφή του περιστατικού και των δράσεων αντιμετώπισης σε περίπτωση που περιστατικό είναι καινούριο. (Εμπλουτισμός βάσης καταγραφής περιστατικών)
- Προτυποποιημένη αναφορά περιστατικών και αδυναμιών ασφάλειας μέσω ενός ασφαλούς καναλιού επικοινωνίας
  - Φόρμες συμπλήρωσης για την αναφορά περιστατικών ασφάλειας. Οι αναφορές αυτές θα παρέχουν προτυποποιημένη πληροφόρηση σχετικά με το περιστατικό και θα έχουν ως στόχο την αποτελεσματική διαχείριση της σχετικής πληροφορίας. Χρήση XML εγγράφων με προκαθορισμένη δομή.
  - Κατάλληλες διαδικασίες ανατροφοδότησης έτσι ώστε να διασφαλιστεί η πλήρης αντιμετώπιση του περιστατικού.
- Ενημέρωση και εκπαίδευση του αρμόδιου προσωπικού σχετικά με την αντιμετώπιση περιστατικών ασφάλειας.
- Αναφορά αδυναμιών ασφάλειας ενός πληροφοριακού συστήματος με προτυποποιημένη διαδικασία στην οποία θα υπάρχει εύκολη πρόσβαση για να μπορούν όλα τα εμπλεκόμενα μέρη να ενημερώνουν άμεσα την αρμόδια ομάδα αντιμετώπισης. Βασικός κανόνας σε περίπτωση εντοπισμού αδυναμίας ασφάλειας είναι να μην δοκιμάζεται στο σύστημα για να μην προκληθεί ζημιά.

4.2.5 Σύστημα Αξιολόγησης Ασφάλειας Πληροφοριακού Συστήματος

Σύμφωνα με το ISO 27002, η αξιολόγηση των επιδόσεων της ασφάλειας πληροφοριών αποτελεί έναν από τους κρίσιμους παράγοντες επίτευξης ενός ασφαλούς πληροφοριακού συστήματος [23]. Η αξιολόγηση επιτυγχάνεται με την υλοποίηση ενός μηχανισμού ο οποίος ελέγχει κατά πόσο

- οι επιμέρους μηχανισμοί ασφάλειας (υλοποιημένα αντίμετρα ασφάλειας) που έχουν υιοθετηθεί, μειώνουν τους κινδύνους ασφάλειας

- το πληροφοριακό σύστημα (e-LMS) είναι συμμορφωμένο με τις πολιτικές και διαδικασίες ασφάλειας.

4.2.6 Υιοθέτηση και Υλοποίηση Αντιμέτρων Ασφάλειας (Τεχνική Συνιστώσα Ασφάλειας Πληροφοριών)

Πρόκειται για τις τεχνικές προδιαγραφές ασφάλειας ενός πληροφοριακού συστήματος οι οποίες έχουν ως κύριο στόχο τη διασφάλιση των έξι βασικών απαιτήσεων ασφάλειας πληροφοριών: Ταυτοποίηση και Αυθεντικοποίηση, Εξουσιοδότηση, Εμπιστευτικότητα, Ακεραιότητα, μη Άρνηση της Ευθύνης και Διαθεσιμότητα και είναι απαραίτητες για ένα ασφαλές περιβάλλον η-μάθησης [39].

Σύμφωνα με το πρότυπο ISO 27002 κάποια από τα προτεινόμενα αντίμετρα ασφάλειας είναι τα παρακάτω [23]:

1. Εφαρμογή μοναδικού κωδικού ασφάλειας για κάθε χρήστη όπως επίσης και χρήση κατάλληλου μηχανισμού και τεχνικής αυθεντικοποίησης με στόχο την ασφαλή επιβεβαίωση ότι ο χρήστης είναι αυτός που ισχυρίζεται πως είναι. (Ταυτοποίηση και Αυθεντικοποίηση)
2. Εφαρμογή κατάλληλου συστήματος διαχείρισης πρόσβασης χρηστών για τη συστηματική παρακολούθηση και διασφάλιση της εξουσιοδότησης και εμπιστευτικότητας.
3. Εφαρμογή μηχανισμών κρυπτογραφίας για την προστασία των απαιτήσεων της εμπιστευτικότητας και ακεραιότητας των δεδομένων
4. Εφαρμογή αποτελεσματικού συστήματος δημιουργίας αντιγράφων ασφάλειας όπως επίσης και σχεδίου – διαδικασίας επιχειρησιακής συνέχειας και ανάκαμψης. (Ακεραιότητα και Διαθεσιμότητα πληροφοριακού συστήματος)
5. Εφαρμογή ψηφιακών υπογραφών κατά τη επικοινωνία των εμπλεκόμενων μερών όπως επίσης και κατά τη διακίνηση η-εγγράφων με στόχο την υλοποίηση της απαίτησης ασφάλειας της μη Άρνησης της ευθύνης.

Στη συνέχεια ακολουθεί λεπτομερής αναφορά στα πιθανά αντίμετρα ασφάλειας που μπορούν να υλοποιηθούν σε ένα ΣΔΗΜ έτσι ώστε να πληρούνται οι βασικές απαιτήσεις ασφάλειας.

Ταυτοποίηση και Αυθεντικοποίηση

Ο βασικοί στόχοι της απαίτησης αυτής είναι να επιτρέπει την πρόσβαση μόνο σε εγκεκριμένους χρήστες όπως επίσης και να αποτρέπει την παράνομη είσοδο χρηστών μέσα στο περιβάλλον του συστήματος η-μάθησης. Για την επίτευξη των παραπάνω στόχων ακολουθείται μια διαδικασία δύο βημάτων η οποία έχει ως εξής:

1) Γίνεται ταυτοποίηση του χρήστη ως ένας εγγεγραμμένος χρήστης του συστήματος
2) Επιβεβαιώνεται ότι ο χρήστης είναι αυτός που ισχυρίζεται πως είναι (αυθεντικοποίηση)

Ένα απλό παράδειγμα της παραπάνω διαδικασίας είναι το εξής: Αν ένας χρήστης θέλει να εισαχθεί στο σύστημα, θα πρέπει να χρησιμοποιήσει ένα όνομα για τις ανάγκες ταυτοποίησης. Το συγκεκριμένο όνομα ταυτοποιεί ότι υπάρχει εγγεγραμμένος χρήστης με αυτό το όνομα αλλά δεν αυθεντικοποιεί τον χρήστη αφού κάποιος άλλος χρήστης έχει τη δυνατότητα να χρησιμοποιεί το ίδιο όνομα. Ο κωδικός πρόσβασης είναι αυτός που αποδεικνύει την ταυτότητα του χρήστη και τον αυθεντικοποιεί.

Από το παραπάνω παράδειγμα αναδεικνύεται ένας μεγάλος προβληματισμός σχετικά με την απαίτηση ταυτοποίησης/αυθεντικοποίησης. Η συγκεκριμένη απαίτηση στις περισσότερες περιπτώσεις προϋποθέτει σχετική κατάρτιση από την πλευρά του χρήστη. Έχοντας ως γνώμονα αυτή την προσέγγιση, τα περισσότερα ΣΔΗΜ καταφεύγουν σε απλές λύσεις αυθεντικοποιήσης χωρίς να παρέχουν την επιθυμητή ασφάλεια. Ο λόγος για τον οποίο γίνεται αυτό είναι γιατί οι πιο ασφαλείς μέθοδοι αυθεντικοποίησης δεν είναι φιλικοί προς το χρήστη και κατ'επέκταση απορρίπτονται καθώς επιλέγεται ως κριτήριο η φιλικότητα προς το χρήστη και όχι η προηγμένη ασφάλεια. Θα πρέπει όμως να ληφθεί υπόψη ότι ακόμη και οι πιο ασφαλείς μέθοδοι ταυτοποίησης/αυθεντικοποίησης μπορούν να παρακαμφθούν αν ο χρήστης δε θέλει να ακολουθήσει τους κανόνες που ορίζει η πολιτική ασφάλειας κωδικού πρόσβασης.

Για την επίτευξη μιας ισχυρής και ασφαλούς ταυτοποίησης και αυθεντικοποίησης χρήστη σε ένα οποιοδήποτε ΣΔΗΜ υπάρχει η δυνατότητα χρήσης ενός συνδυασμού των παρακάτω αντιμέτρων ασφάλειας [3].

Μηχανισμοί Κωδικού Πρόσβασης (Password-Based Mechanisms) [39]***:***

Στα συστήματα που υλοποιούν μηχανισμό κωδικού πρόσβασης, οι χρήστες είναι υποχρεωμένοι να επιλέγουν μοναδικό όνομα χρήστη και κωδικό πρόσβασης κατά την εγγραφή τους στο συστημα. Ο συνδυασμός των δύο στοιχείων αποθηκεύεται στη βάση δεδομένων του ΣΔΗΜ και αποτελεί την ταυτότητα του κάθε χρήστη.

Είναι απαραίτητο να ληφθούν υπόψη τα παρακάτω [3]:

- Το πληροφοριακό σύστημα θα πρέπει να υποχρεώνει το χρήστη να έχει μοναδική ταυτότητα χρήστη. Συνεπώς απαγορεύεται η δημιουργία ομαδικής ταυτότητας εισόδου στο σύστημα.
- Ένα σύστημα η-μάθησης θα πρέπει να καταγράφει τις πληροφορίες αυθεντικοποίησης με στόχο να παρακολουθεί τη δραστηριότητα των χρηστών και κατ'επέκταση να επιβάλλει την απαίτηση ασφάλειας της μη άρνησης της ευθύνης.
- Το σύστημα θα πρέπει να αποφεύγει κάθε τρύπα ασφάλειας για κάποιον που προσπαθεί να παρακάμψει τις φάσεις της διαδικασίας ταυτοποίησης/αυθεντικοποίησης. Αυτό σημαίνει ότι το σύστημα θα πρέπει να του επιβάλλει την εισαγωγή κατάλληλων δεδομένων προκειμένου να εισαχθεί στο σύστημα.
- Ασφαλής επικοινωνία και αποθήκευση των πληροφοριών αυθεντικοποίησης για λόγους εμπιστευτικότητας και ακεραιότητας των δεδομένων.

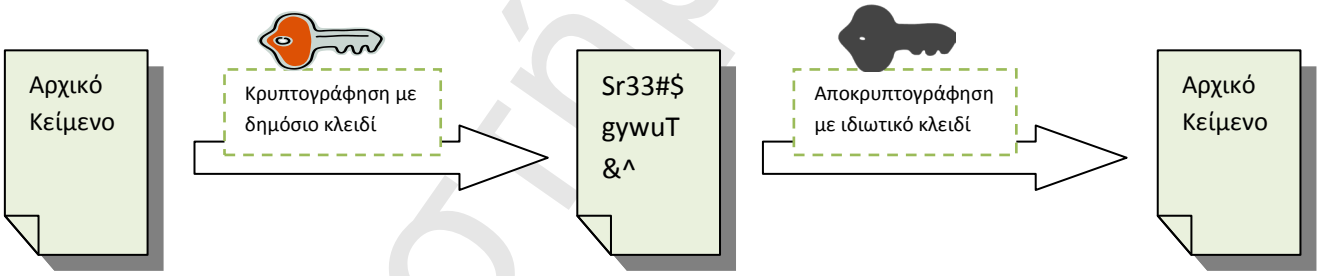
Οι μηχανισμοί κωδικών πρόσβασης αποτελούν μια εύκολη και ανέξοδη λύση η οποία είναι ταυτόχρονα και η πιο διαδεδομένη επιλογή για τα ΣΔΗΜ [6]. Όμως δεν παρέχει επαρκή ασφάλεια για τα πιο ευαίσθητα υποσυστήματα ενός ΠΣ. Ένα χαρακτηριστικό σενάριο που αποδεικνύει την ανεπάρκεια αυτή είναι η περίπτωση διεξαγωγής εξετάσεων από απόσταση στην οποία δεν μπορεί να αποδειχθεί αν ο εξεταζόμενος είναι ίδιος με τον πραγματικό μαθητή καθώς ένας μη εξουσιοδοτημένος χρήστης μπορεί να χρησιμοποιήσει τον κωδικό ενός εξουσιοδοτημένου χρήστη του συστήματος.

Από τα παραπάνω συμπεραίνουμε ότι ο μηχανισμός κωδικού πρόσβασης αποτελεί ένα απαραίτητο αλλά όχι μοναδικό αντίμετρο ασφάλειας το οποίο θα πρέπει να είναι υλοποιημένο σε ένα ΣΔΗΜ. Θα πρέπει να ακολουθεί την σχετική πολιτική ασφάλειας κωδικού πρόσβασης και οι χρήστες του ΠΣ να είναι κατάλληλα ενημερωμένοι. Προτείνεται η χρήση του μηχανισμού κωδικού πρόσβασης να συνδυάζεται με ένα από τα επόμενα αντίμετρα ασφάλειας.

Υποδομή Δημόσιου Κλειδιού [39] [18]

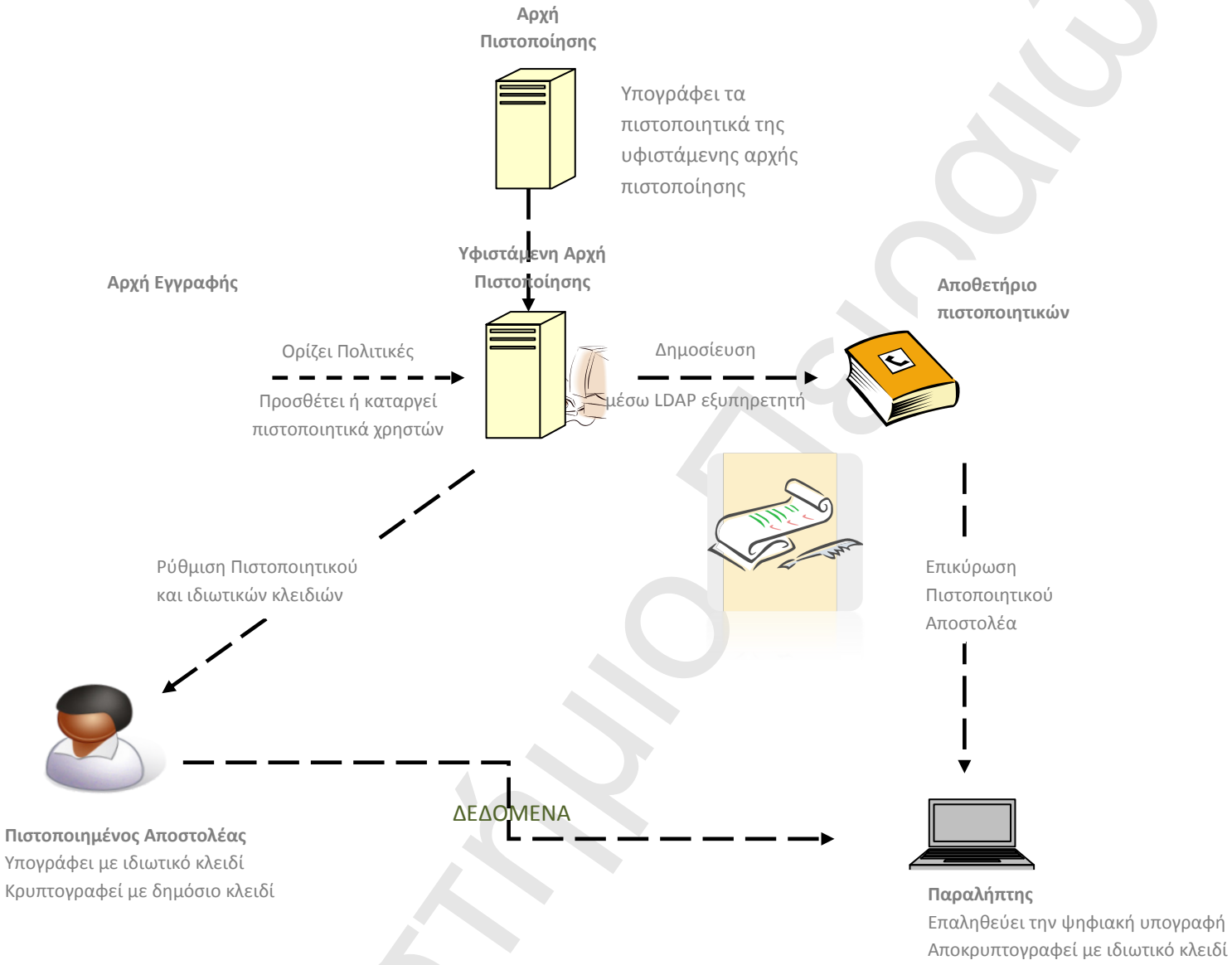
Μία Υποδομή Δημόσιου Κλειδιού είναι δυνατό να καλύψει τις τέσσερις βασικές απαιτήσεις ασφάλειας πληροφοριών: αυθεντικοποίηση, ακεραιότητα, εμπιστευτικότητα, και μη-άρνηση ευθύνης. Συνεπώς μπορεί να αποτελέσει ολιστική προσέγγιση στην υλοποίηση ενός ασφαλούς ΣΔΗΜ.

Η λειτουργία μιας ΥΔΚ είναι βασισμένη στην ασύμμετρη κρυπτογράφηση. Ένα πληροφοριακό σύστημα που ανήκει σε ένα περιβάλλον ΥΔΚ έχει χρήστες οι οποίοι κατέχουν ένα κρυπτογραφικό ζευγάρι.



Σχήμα 1. Κρυπτογραφία Δημόσιου Κλειδιού

Κάθε βασικό ζευγάρι περιέχει ένα ιδιωτικό και ένα δημόσιο κρυπτογραφικό κλειδί με μια μοναδική ιδιότητα: όταν το ένα χρησιμοποιείται με έναν αλγόριθμο κωδικοποίησης για να κρυπτογραφήσει τα δεδομένα, το άλλο μπορεί να χρησιμοποιηθεί με τον ίδιο αλγόριθμο για να αποκρυπτογραφήσει τα δεδομένα. Το κλειδί κωδικοποίησης δεν μπορεί να χρησιμοποιηθεί για την αποκωδικοποίηση. Τα δημόσια κλειδιά πιστοποιούνται από ένα αρμόδιο συμβαλλόμενο μέρος, μια Έμπιστη Τρίτη Οντότητα (ΕΤΟ). Ως Έμπιστη Τρίτη Οντότητα (ΕΤΟ) ορίζεται «μια αρχή ασφαλείας ή ο αντιπρόσωπος της η οποία θεωρείται έμπιστη από τους χρήστες με σκοπό τη παροχή δράσεων σχετικών με ασφάλεια, όπως π.χ. την υποστήριξη της χρήσης ψηφιακών υπογραφών και την εμπιστευτικότητα των υπηρεσιών». Το δημόσιο κλειδί διανέμεται ευρέως, συχνά μέσο ενός καταλόγου ή μιας βάσης δεδομένων που μπορεί να αναζητηθεί από το κοινό. Παρακάτω περιγράφεται σχηματικά μια απλή υποδομή δημόσιου κλειδιού.



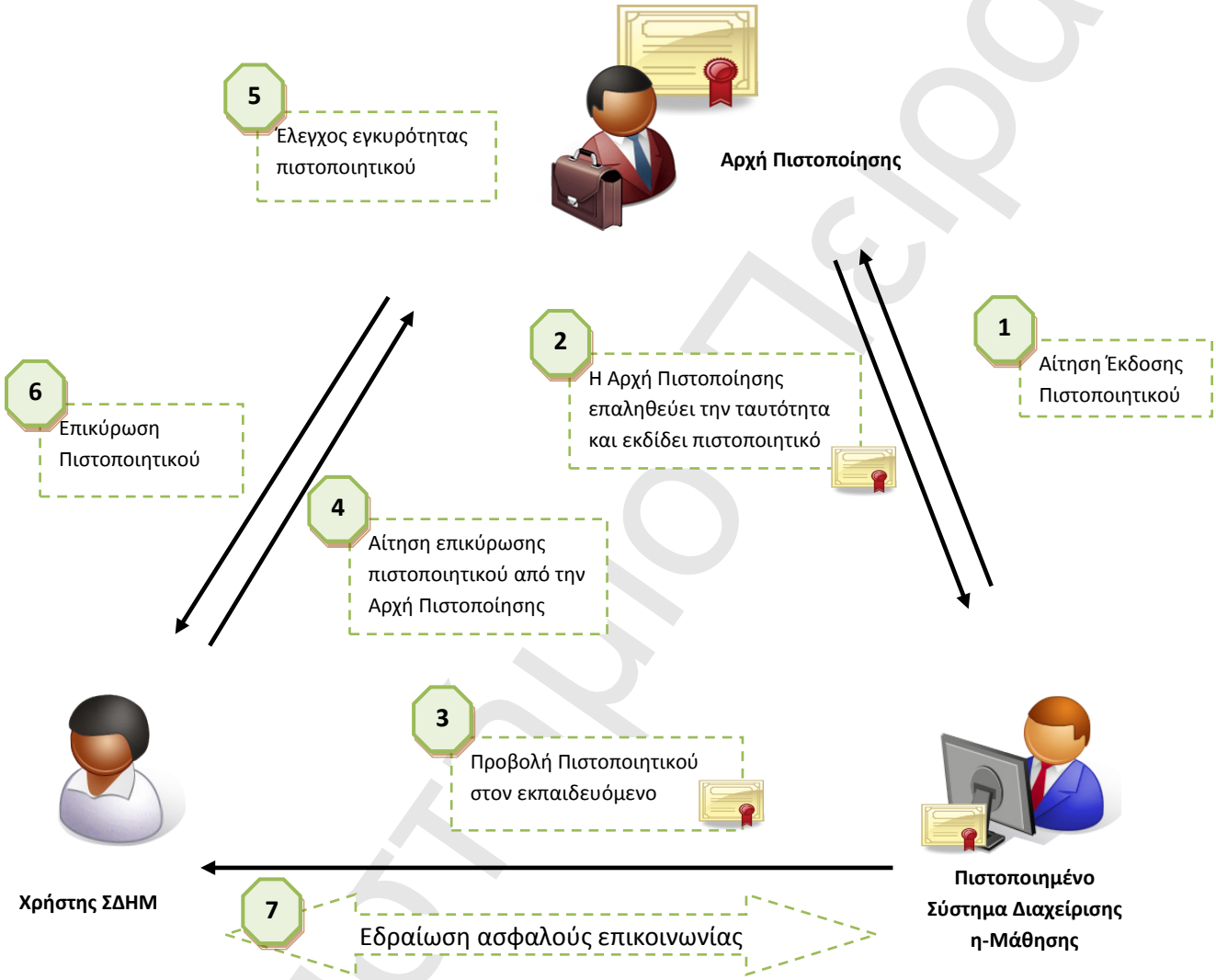
Σχήμα 2. Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)

Υπηρεσία ΥΔΚ	Συμπεριφορικά Χαρακτηριστικά
Εγγραφή	Η υπηρεσία της εγγραφής έχει ως κύριους στόχους: • Εγγραφή καινούριων χρηστών στην Υποδομή Δημόσιου Κλειδιού και προώθηση αιτήματος έκδοσης ψηφιακού πιστοποιητικού στην αρμόδια αρχή πιστοποίησης. • Ορισμό πολιτικών σχετικά με τους κανόνες έκδοσης, χρήσης και ανάκλησης των ψηφιακών πιστοποιητικών. • Αδιάλειπτη πληροφόρηση προς την αρχή πιστοποίησης σχετικά με τα προς ανάκληση ψηφιακά πιστοποιητικά σύμφωνα με τις καθορισμένες πολιτικές • Αναγνώριση και αυθεντικοποίηση του χρήστη, έτσι ώστε να

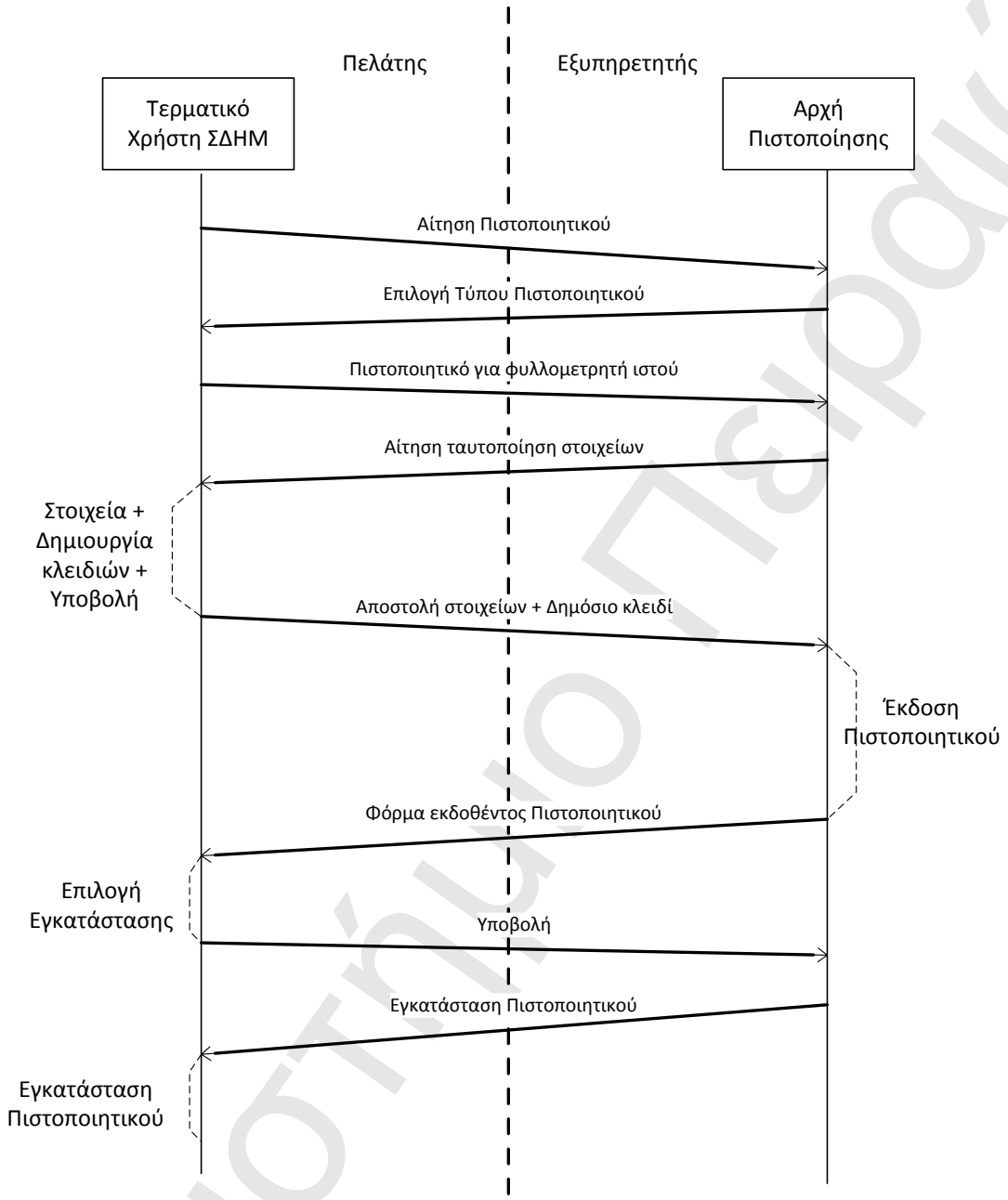
	πραγματοποιηθεί η αξιόπιστη σύνδεση του με το δημόσιο κλειδί του . Η Αρχή Εγγραφής (Registration Athority) είναι υπεύθυνη για την υπηρεσία εγγραφής σε ένα περιβάλλον ΥΔΚ.
Πιστοποίηση	Η πιστοποίηση έχει ως στόχο τη σύνδεση μιας οντότητας με το δημόσιο κλειδί της και το πιστοποιητικό αποτελεί το ηλεκτρονικό μέσο της σύνδεσης αυτής. Κατά την επικοινωνία χρηστών σε ένα περιβάλλον ΥΔΚ, τα ψηφιακά πιστοποιητικά είναι το βασικό στοιχείο εγκυρότητας κατά την αυθεντικοποίηση ή κατά την επιβεβαίωση ψηφιακών υπογραφών κτλ. Η Αρχή Πιστοποίησης (Certification Authority) είναι υπεύθυνη για τη συγκεκριμένη υπηρεσία και αποτελεί το βασικό σημείο εμπιστοσύνης της όλης υποδομής. Η πιστοποίηση περιλαμβάνει τις παρακάτω λειτουργίες: • Έκδοση/ανανέωση πιστοποιητικών βάσει συγκεκριμένων προτύπων. • Διανομή πιστοποιητικών στους χρήστες. • Αποθήκευση πιστοποιητικών στο Κατάλογο για κοινή χρήση. • Ανάκληση πιστοποιητικών με έκδοση Λίστας ανάκλησης πιστοποιητικών (ΛΑΠ), η οποία περιέχει όλα τα πιστοποιητικά που δεν ισχύουν ή που έχουν λήξει . Οι ΥΔΚ βασίζονται στο πρότυπο X.509 v.3 [X509] του ITU-T για την έκδοση και διαμόρφωση των ψηφιακών πιστοποιητικών που εκδίδουν.
Κατάλογος	Η υπηρεσία Καταλόγου αυτή μέσω κατάλληλου Εξυπηρετητή Καταλόγου (Directory Server) έχει ως στόχο • την αποθήκευση και διάθεση των εκδοθέντων από την ΕΤΟ πιστοποιητικών και δημόσιων κλειδιών. • την αποθήκευση των Λιστών Ανάκλησης Πιστοποιητικών για έλεγχο της εγκυρότητας και ισχύος πιστοποιητικών. Η οργάνωση του Καταλόγου γίνεται βάσει κατάλληλων προτύπων και πρωτοκόλλων .
Χρονοσφράγιση	Η υπηρεσία χρονοσφράγισης έχει ως βασική λειτουργία την επικόλληση ημερομηνίας και ώρας σε δεδομένα, με σκοπό την απόδειξη ότι τα τελευταία δημιουργήθηκαν ή απεστάλησαν σε μία συγκεκριμένη χρονική στιγμή. Με το τρόπο αυτό ουσιαστικά αποδεικνύεται και η μοναδικότητα των ίδιων των δεδομένων. Η υπηρεσία εκτελείται από ειδική *Αρχή Χρονικής Σφραγίδας* της ΥΔΚ, βάσει κατάλληλων μεθόδων και προτύπων .
Διαπιστοποίηση	Η υπηρεσία διαπιστοποίησης έχει ως βασική λειτουργία τη διασφάλιση των συναλλαγών μεταξύ χρηστών εγγεγραμμένων σε διαφορετικές ΥΔΚ. Ως «δια-πιστοποιητικό» εννοείται το πιστοποιητικό που εκδίδεται από μία Αρχή Πιστοποίησης Α σε μία άλλη Αρχή Πιστοποίησης Β και εκφράζει την εμπιστοσύνη της Α ως προς τη Β. Έτσι, βάσει του «δια-πιστοποιητικού», ένας χρήστης Χ που εμπιστεύεται την ΑΠ Α, μπορεί να εμπιστευτεί κάθε χρήστη Υ

	που πιστοποιείται από την ΑΠ Β. Τα δια-πιστοποιητικά μπορεί να είναι μονόδρομα ή αμφίδρομα. Κατά τη δεύτερη περίπτωση η εμπιστοσύνη μεταξύ δύο χρηστών των ΑΠ Α και ΑΠ Β είναι αμοιβαία.

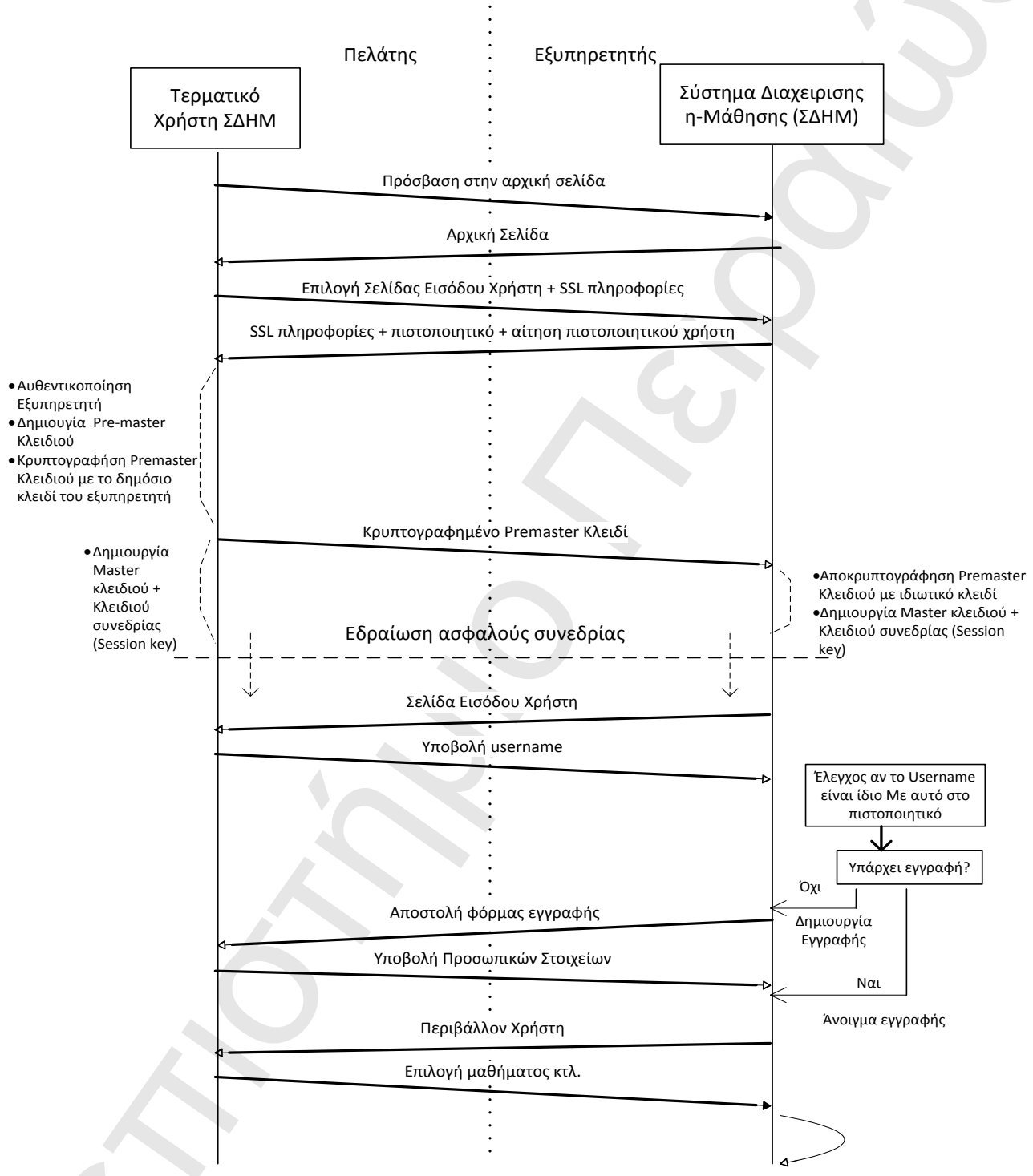
Πίνακας 3. Υπηρεσίες Υποδομής Δημόσιου Κλειδιού



Σχήμα 3. Εδραίωση Επικοινωνίας σε ΥΔΚ



Σχήμα 4. Αίτηση Πιστοποιητικού σε ΥΔΚ



Σχήμα 5. Αυθεντικοποίηση Εκπαιδευόμενου

Το ιδιωτικό κλειδί παραμένει ένα στενά φυλαγμένο μυστικό από τον ιδιοκτήτη. Υπάρχουν μερικές δυνατότητες για την ιδιωτική βασική αποθήκευση (τα κλειδιά είναι μακριές σειρές κομματιών και η απομνημόνευση τους είναι αδύνατη). Υπάρχουν τρεις δυνατότητες αποθήκευσης: σκληρός δίσκος, δισκέτα και έξυπνη κάρτα.

Τέλος, η επικοινωνία των χρηστών μιας ΥΔΚ βασίζεται στην επικοινωνία μέσω ασφαλών καναλιών κρυπτογραφημένης επικοινωνίας.

Token-based μηχανισμοί [39]

Η υλοποίηση των μηχανισμών αυτών είναι οι έξυπνες κάρτες στις οποίες αποθηκεύονται ιδιωτικές και κρίσιμες πληροφορίες οι οποίες είναι ικανές να αναγνωρίσουν μοναδικά τον κάτοχο. Αποτελούν την ψηφιακή ταυτότητα του κατόχου και ενισχύουν σημαντικά τη διαδικασία ταυτοποίησης/αυθεντικοποίησης σε ένα πληροφοριακό σύστημα.

Οι έξυπνες κάρτες, αντίθετα από τις μαγνητικές κάρτες, μπορούν να έχουν όλες τις απαραίτητες λειτουργίες και τις πληροφορίες για την κάρτα. Επομένως, δεν απαιτούν πρόσβαση σε μακρινές βάσεις δεδομένων κατά την διάρκεια της συναλλαγής. Αυτό έχει σαν αποτέλεσμα να μειώνονται οι πιθανότητες επίθεσης αφού δε χρησιμοποιείται κάποιο κανάλι επικοινωνίας με κάποια απομακρυσμένη τοποθεσία για τη μεταφορά δεδομένων. Οι έξυπνες κάρτες χρησιμοποιούνται ευρέως στις τηλεπικοινωνίες, το ηλεκτρονικό εμπόριο, το τραπεζικό σύστημα, το σύστημα υγείας κ.α. με στόχο την αυθεντικοποίηση, τη συναλλαγή και την αποθήκευση των δεδομένων συναλλαγής. Αυτές οι λειτουργίες μπορούν να χρησιμοποιηθούν και σε ένα σύστημα η-μάθησης, ειδικά στις υπηρεσίες που χρησιμοποιούν κρίσιμα υποσυστήματα της πλατφόρμας η-μάθησης (π.χ. θέματα εξετάσεων, στοιχεία πιστωτικής κάρτας για πληρωμή διδάκτρων, διαδικασία εξέτασης, καταγραφή βασικών και απαραίτητων δεδομένων παρακολούθησης μαθημάτων κτλ.)

Βιομετρική [39]

Οι μηχανισμοί που βασίζονται στη Βιομετρική αποθηκεύουν μοναδικά γνωρίσματα ενός ανθρώπου με στόχο την υλοποίηση ισχυρής αυθεντικοποίησης σε ένα Πληροφοριακό Σύστημα. Πρόκειται για μοναδικά, μετρήσιμα φυσικά ή/και συμπεριφορικά χαρακτηριστικά ενός ανθρώπου τα οποία ψηφιοποιούνται, αποθηκεύονται και συνδέονται με την ταυτότητα του χρήστη μέσα στη βάση δεδομένων του συστήματος. Μερικές από της βιομετρικές μεθόδους που μπορούν να χρησιμοποιηθούν για την ταυτοποίηση/αυθεντικοποίηση ενός ατόμου είναι οι παρακάτω:

Φυσικά Χαρακτηριστικά	Συμπεριφορικά Χαρακτηριστικά
• Δακτυλικό Αποτύπωμα • Γεωμετρία Χεριού • Σάρωση Ίριδας Οφθαλμού • Σάρωση αμφιβληστροειδούς • Αναγνώριση Προσώπου	• Αναγνώριση Φωνής • Αναγνώριση γραφικού χαρακτήρα

Όπως βλέπουμε οι μηχανισμοί Βιομετρικής βασίζονται στα χαρακτηριστικά/γνωρίσματα του ανθρώπου με αποτέλεσμα να προσφέρουν έναν ασφαλή και ισχυρό τρόπο αυθεντικοποίησης. Οι μηχανισμοί αυτοί θα μπορούσαν να ενσωματωθούν σε ένα ΣΔΗΜ και να χρησιμοποιηθούν σε κάποιες από τις υπηρεσίες του όπως για παράδειγμα,

- κατά τη διάρκεια των εξετάσεων θα μπορούσαν οι εξεταζόμενοι να αναγνωρίζονται μοναδικά μέσω ενός τέτοιου μηχανισμού αποφεύγοντας έτσι το πρόβλημα της διπλοπροσωπίας. Οι μηχανισμοί αυτοί θα μπορούσαν να χρησιμοποιηθούν είτε αν οι εξετάσεις γίνονταν σε ειδικά διαμορφωμένους χώρους είτε εξ'αποστάσεως από κάποιον ιδιωτικό χώρο.
- Για την είσοδο των εκπαιδευτών στο υποσύστημα συγγραφής και αποθήκευσης θεμάτων εξέτασης θα μπορούσαν να χρησιμοποιηθούν μηχανισμοί Βιομετρικής με στόχο την αποφυγή εισόδου ενός μη εξουσιοδοτημένου χρήστη στα θέματα εξετάσεων.

Για να μπορέσει ένας μηχανισμός βιομετρικής να είναι αποτελεσματικός, θα πρέπει υλοποιηθεί βασισμένος σε μια ορθή προσέγγιση. Άρα θα πρέπει να οριστεί αν θα χρησιμοποιηθεί κεντρική ή διενεμημένη αποθήκευση των βιομετρικών υπογραφών, στο αν ο αλγόριθμος σύγκρισης είναι ενσωματωμένος ή όχι στο υπόλοιπο σύστημα, στον τρόπο επικοινωνίας των διαφόρων συστατικών του βιομετρικού μηχανισμού και στο πως είναι υλοποιημένη η διαδικαστική ασφάλεια για τη χρήση του συστήματος.

Μερικοί κίνδυνοι ασφάλειας που μπορούν να παρουσιαστούν σε ένα τέτοιο σύστημα ασφάλειας

- Επιθέσεις υποκλοπής και επανεκπομπής
- Επιθέσεις αντικατάστασης βιομετρικού δείγματος στη βάση δεδομένων μιας κεντρικοποιημένη αρχιτεκτονικής πληροφοριακού συστήματος
- Επιθέσεις κατά τη στιγμή της εγγραφής
- Επιθέσεις στα επιμέρους συστήματα του βιομετρικού μηχανισμού
- Επιθέσεις από το προσωπικό διαχείρισης του συστήματος

Από τα παραπάνω παραδείγματα, είναι σαφές ότι η συνολική σχεδίαση του συστήματος πιστοποίησης ταυτότητας του χρήστη πρέπει να γίνεται πολύ προσεκτικά, ώστε να προστατεύονται στο μέγιστο τέτοια ευαίσθητα δεδομένα τηρώντας τις απαιτήσεις της εμπιστευτικότητας και της ακεραιότητας τους.

Όπως αναφέρθηκε και παραπάνω, για να υλοποιηθεί ένας ισχυρότερος και αποτελεσματικότερος μηχανισμός ταυτοποίησης και αυθεντικοποίησης θα πρέπει να επιλεγεί ένας συνδυασμός των παραπάνω 4 μηχανισμών/αντιμέτρων ασφάλειας. Ακολουθούν μερικά παραδείγματα τέτοιων συνδυασμών:

Βιομετρικές Έξυπνες Κάρτες [39]

Η βιομετρική ασφάλεια είναι πιο δυνατή από τις μεθόδους όπως οι ισχυροί κωδικοί πρόσβασης, οι αριθμοί PIN, οι έξυπνες κάρτες ή η Υποδομή Δημόσιου Κλειδιού (ΥΔΚ) επειδή η βιομετρική προσδιορίζει τα άτομα παρά τις συσκευές.. Ένας βιομετρικός έλεγχος, όπως ένα δακτυλικό αποτύπωμα, είναι ένα κλειδί που δεν μπορεί ποτέ να χαθεί και χαρακτηρίζει μοναδικά τον κάτοχο του. Η βιομετρική τεχνολογία έχει συνδυαστεί με τη τεχνολογία των έξυπνων καρτών για να προωθήσει τις βιομετρικές έξυπνες κάρτες. Δηλαδή, η βιομετρική χρησιμοποιείται για την επικύρωση στα πρότυπα ασφάλειας έξυπνων καρτών. Με την

προσθήκη της βιομετρικής τεχνολογίας σε μια λύση έξυπνων καρτών, βελτιώνουν την ασφάλεια των καρτών και προστατεύουν την ιδιοκτησία του κατόχου κάρτας. Η προσθήκη της βιομετρικής τεχνολογίας σε μια έξυπνη κάρτα βελτιώνει πολύ την ασφάλεια της κάρτας. Η βιομετρική τεχνολογία επιτρέπει στις εταιρίες που εκδίδουν την κάρτα να είναι βέβαιες ότι το άτομο που επιτρέπουν να έχουν πρόσβαση στις πληροφορίες ή μια θέση, είναι το ίδιο άτομο. Τα βιομετρικά χαρακτηριστικά γνωρίσματα είναι μοναδικά σε ένα πρόσωπο και δεν μπορούν να αναπαραχθούν από έναν κακόβουλο χρήστη, όπως μπορούν τα PINs και οι κωδικοί πρόσβασης. Χρησιμοποιώντας περισσότερα από ένα βιομετρικά προσδιοριστικά, τα ψεύτικα ποσοστά αποδοχής, καθώς επίσης και τα ψεύτικα ποσοστά απόρριψης, παρουσιάζουν εντυπωσιακή πτώση. Η βιομετρική έξυπνη κάρτα συνδυάζει τη δύναμη της μοναδικότητας των ανθρώπινων χαρακτηριστικών με τη δυνατότητα των έξυπνων καρτών να εκτελούν όλες τις απαραίτητες λειτουργίες χωρίς την απομακρυσμένη πρόσβαση σε κάποια βάση δεδομένων.

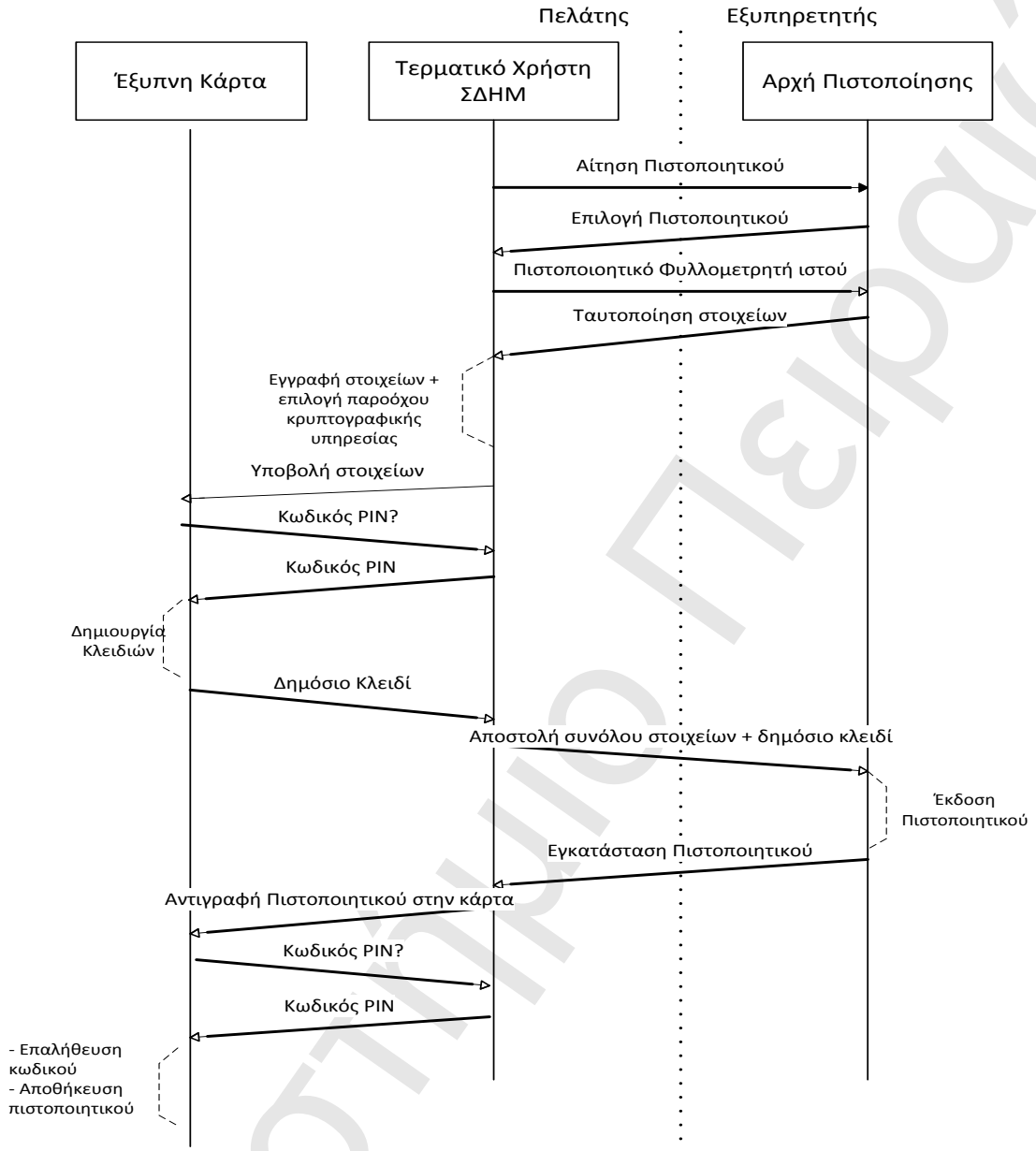
Οι βιομετρικές πληροφορίες που αποθηκεύονται στην έξυπνη κάρτα επιτρέπουν στον τελικό χρήστη να μεταφέρει τα δικά του βιο-δεδομένα. Ο κάτοχος κάρτας γράφει τα βιο-στοιχεία του (δακτυλικό αποτύπωμα, φωνή ή/και πρόσωπο) και αυτές οι πληροφορίες οργανώνονται μέσω ενός αλγορίθμου, ο οποίος δημιουργεί έναν αριθμό που κρυπτογραφείται και αποθηκεύεται στην κάρτα. Η πιστοποίηση ταυτότητας εκτελείται με τη σύγκριση τσιπ των βιομετρικών προτύπων που αποθηκεύονται στην έξυπνη κάρτα με τα βιομετρικά δεδομένα που συγκεντρώνονται σε κάθε συναλλαγή. Ο χρήστης κρατά την κάρτα με αυτά, χρησιμοποιώντας την σε περίπτωση ανάγκης. Ο χρήστης διατηρεί τον πλήρη έλεγχο των προσωπικών βιομετρικών δεδομένων τους. Εάν η κάρτα χαθεί ή κλαπεί, δεν μπορεί να χρησιμοποιηθεί από οποιονδήποτε άλλον.

Έξυπνες Κάρτες ΥΔΚ [39]

Σε ένα περιβάλλον ΥΔΚ, όπως περιγράφηκε παραπάνω, τα δημόσια κλειδιά πιστοποιούνται από μια Έμπιστη Τρίτη Οντότητα (ΕΤΟ). Το δημόσιο κλειδί διανέμεται ευρέως ενώ το ιδιωτικό κλειδί αποθηκεύεται από τον ιδιοκτήτη. Ο καλύτερος τρόπος αποθήκευσης είναι η έξυπνη κάρτα.

Μερικοί σύγχρονοι επεξεργαστές έξυπνων καρτών έχουν ακόμη και τους ενσωματωμένους κρυπτογραφικούς επεξεργαστές που επιτρέπουν την υπογραφή και τη βασική παραγωγή να γίνουν εξ ολοκλήρου στην κάρτα, έτσι ώστε το ιδιωτικό κλειδί να μην αποκαλυφθεί ή να ακυρωθεί ποτέ. Ο μικροεπεξεργαστής δίνει στην έξυπνη κάρτα ένα μεγάλο πλεονέκτημα πέρα από τα μαγνητικά ή οπτικά μέσα αποθήκευσης. Μια έξυπνη κάρτα ΥΔΚ μπορεί να είναι πολύ ασφαλής, εξαλείφοντας οποιασδήποτε δυνατότητα του βασικού ζευγαριού που είναι έξω κατά τη διάρκεια της δημιουργίας και της μεταφοράς. Μια έξυπνη κάρτα μπορεί να περιέχει το ιδιωτικό κλειδί του χρήστη, που μπορεί να χρησιμοποιηθεί μόνο από κάποιο με τη φυσική κατοχή του σημείου, και τη γνώση μιας μυστικής μεταβίβασης φράσης και ίσως ένα βιομετρικό προσδιοριστικό.

Στο παρακάτω διάγραμμα ακολουθίας περιγράφεται η διαδικασία αίτησης πιστοποιητικού ενός εκπαιδευόμενου χρησιμοποιώντας μια έξυπνη κάρτα PKI.



Σχήμα 6. Αίτηση Πιστοποιητικού για Έξυπνη Κάρτα ΥΔΚ

Σε όλους τους μηχανισμούς/μοντέλα αυθεντικοποίησης που απαιτείται απομακρυσμένη επικοινωνία είναι ευνόητο ότι το κανάλι επικοινωνίας θα πρέπει να είναι ασφαλές και αυτό επιτυγχάνεται με κάποια υλοποίηση του πρωτοκόλλου SSL (Secure Socket Layer). Το SSL θα περιγραφεί αναλυτικά στην απαίτηση ασφάλειας της εμπιστευτικότητας. Πρόκειται για ένα πρωτόκολλο που παρέχει ένα ιδιωτικό κανάλι μεταξύ των εφαρμογών επικοινωνίας, το οποίο εξασφαλίζει τη μυστικότητα των δεδομένων, την αυθεντικοποίηση των εμπλεκόμενων μερών και την ακεραιότητα.

Εξουσιοδότηση

Η απαίτηση ασφάλειας της εξουσιοδότησης είναι γνωστή και ως Λογικός Έλεγχος Προσπέλασης (Logical Access Control - LAC). Η εξουσιοδότηση είναι η διαδικασία η οποία καθορίζει για ένα ταυτοποιημένο χρήστη αν θα αποκτήσει δικαιώματα πρόσβασης σε πληροφοριακούς πόρους του συστήματος όπως επίσης και τι είδους δικαιώματα θα αποκτήσει. Στόχος της εξουσιοδότησης είναι η διασφάλιση ότι κάθε χρήστης ενός ΣΔΗΜ θα έχει πρόσβαση και λειτουργικότητες μόνο για τους πόρους που ορίζει ο ρόλος που του έχει ανατεθεί.

Ακολουθεί περιγραφή μηχανισμών ελέγχου πρόσβασης οι οποίοι υιοθετούν διαφορετική φιλοσοφία υλοποίησης της εξουσιοδότησης σε ένα πληροφοριακό σύστημα.

Διακριτικός Έλεγχος Πρόσβασης (Discretionary Access Control (DAC)) [39] [51]

Η βασική ιδέα του μηχανισμού είναι ότι όλοι οι χρήστες αποφασίζουν ποιος (άλλος χρήστης) θα μπορεί να έχει πρόσβαση στα αντικείμενα τα οποία δημιουργούν. Η φιλοσοφία του μηχανισμού αυτού μπορεί να γίνει εύκολα αντιληπτή καθώς καθημερινά έρχονται σε επαφή με ηλεκτρονικά αρχεία για τα οποία έχουν τη δυνατότητα να ορίζουν δικαιώματα ανάγνωσης και εγγραφής.

Πρόκειται για έναν αρκετά ευέλικτο μηχανισμό με το μειονέκτημα ότι γίνεται αρκετά πολύπλοκος για μεγάλες ομάδες χρηστών. Επιπλέον το σύστημα είναι ασφαλές μόνο αν κάθε χρήστης τηρεί τις πολιτικές ασφάλειας απόδοσης δικαιωμάτων σε άλλους χρήστες. Χαρακτηριστικό παράδειγμα αποτελεί η περίπτωση κατά την οποία ένας χρήστης δημιουργεί εμπιστευτικό υλικό και θέλει να γίνει έλεγχος από κάποιος συνεργάτη του. Ο χρήστης δίνει δικαίωματα ανάγνωσης και εγγραφής στο συνεργάτη του αλλά εκείνος αποθηκεύει το έγγραφο σε τοπικό φάκελο του υπολογιστή του αφαιρώντας το από το σύστημα. Σε αυτή την περίπτωση παραβιάζουμε την αρχή της εμπιστευτικότητας αφού ο συνεργάτης θα πρέπει να θέσει τα κατάλληλα δικαιώματα στο έγγραφο που έχει συγγραφεί από άλλο χρήστη.

Για την αντιμετώπιση τέτοιας απειλής, χρησιμοποιείται ο μηχανισμός ελέγχου πρόσβασης βασισμένος σε ρόλους, με τον παρών μηχανισμό να προσφέρεται ως προαιρετικός.

Μηχανισμός Ελέγχου Πρόσβασης βασισμένος σε ρόλους (Role-based Access Control) [39] [51]

Το συγκεκριμένο μοντέλο ελέγχου πρόσβασης χρησιμοποιείται κατά κύριο λόγο στα λειτουργικά συστήματα, τα συστήματα διαχείρισης βάσεων δεδομένων και στις υπηρεσίες Ιστού.

Πρόκειται για τη λογική επέκταση του προηγούμενου μοντέλου ελέγχου πρόσβασης. Στο παρόν μοντέλο τα δικαιώματα εκχωρούνται σε ρόλους και όχι σε χρήστες. Για παράδειγμα ο ρόλος «εγγραφή σε μάθημα (ανάγνωση)» μπορεί να δώσει **δικαιώματα ανάγνωσης** στα αντικείμενα «εκπαιδευόμενοι», «μαθήματα» και «εγγραφή σε μάθημα». Ο ρόλος «εγγραφή σε μάθημα (εγγραφή)» μπορεί να δώσει δικαιώματα ανάγνωσης στα αντικείμενα «εκπαιδευόμενοι», «μαθήματα», και δικαιώματα εγγραφής στην «εγγραφή σε μάθημα». Οι

παραπάνω ρόλοι ονομάζονται και ρόλοι εργασιών καθώς περιγράφουν συγκεκριμένες εργασίες και καθορίζουν ποια δικαιώματα απαιτούνται και για ποιες εργασίες.

Επίσης ο παρών μηχανισμός έχει τη δυνατότητα να εκχωρεί ρόλους σε άλλους ρόλους με στόχο να δημιουργηθεί ιεραρχία εξουσιοδότησης. Οι ρόλοι εργασιών συνήθως συναθροίζονται στους ρόλους ιδιότητας. Για παράδειγμα, ο ρόλος «εκπαιδευτής» περιλαμβάνει του ρόλους εργασιών «εγγραφή σε μάθημα (εγγραφή)», «εγγραφή σε μάθημα (ανάγνωση)», «αξιολόγηση μαθητών». Τέλος οι ρόλοι ιδιοτήτων εκχωρούνται στους χρήστες του συστήματος.

Αυστηρός Έλεγχος Πρόσβασης (Mandatory Control Access) [39] [51]

Ο συγκεκριμένος έλεγχος πρόσβασης δεν επιτρέπει στον χρήστη να αποφασίσει ποιος μπορεί να προσπελάσει τα δεδομένα. Η πιο κοινή μορφή ενός τέτοιου μοντέλου είναι τα πολυεπίπεδα πληροφοριακά συστήματα που χρησιμοποιούνται κυρίως στο στρατό. Όμως σε ορισμένες περιπτώσεις το παρόν μοντέλο προτείνεται και σε συστήματα η-μάθησης.

Στα πολυεπίπεδα πληροφοριακά συστήματα, τα δεδομένα κατηγοριοποιούνται ανάλογα με το επίπεδο σημαντικότητας/μυστικότητας με αποτέλεσμα οι χρήστες ταξινομούνται σε συγκεκριμένο επίπεδο έχοντας τη δυνατότητα πρόσβασης σε δεδομένα χαμηλότερου επιπέδου και ταυτόχρονα απαγόρευση σε υψηλότερου. Οι χρήστες έχουν τη δυνατότητα εγγραφής στο επίπεδο τους και στα υψηλότερα. Για παράδειγμα ένας χρήστης που είναι εξουσιοδοτημένος να προσπελαύνει απόρρητα έγγραφα έχει τη δυνατότητα να δημιουργεί έγγραφα μόνο στα επίπεδα «απόρρητο» και «άκρως απόρρητο». Με αυτό τον τρόπο αποφεύγεται η λανθασμένη τοποθέτηση του εγγράφου σε επίπεδο που μπορεί να το δει ελεύθερα κάποιος. Το συγκεκριμένο μοντέλο ασφάλειας αναπτύχθηκε από τον Bell La Padula. Στο συγκεκριμένο μοντέλο είναι πιθανό για ένα δημιουργό να ταξινομήσει μια πληροφορία σε υψηλότερο επίπεδο από αυτό που πραγματικά ανήκει. Το «λάθος» αυτό δε βάζει σε κίνδυνο τη μυστικότητα της πληροφορίας. Οι συγκεκριμένοι κανόνες είναι γνωστοί ως “no-read-up”και 'no-write-down', δηλαδή κάποιος μπορεί να δημιουργήσει έγγραφα μόνο για τα υψηλότερα επίπεδα και να διαβάσει έγγραφα μόνο για τα χαμηλότερα επίπεδα . Το συγκεκριμένο μοντέλο εγγυάται μόνο τη διατήρηση της μυστικότητα και όχι της ακεραιότητας των δεδομένων. Η ακεραιότητα των δεδομένων επιτυγχάνεται από το μοντέλο που υλοποίησε ο Biba μετατρέποντας τις ιδιότητες 'no-read-up' και 'nowrite-down' σε 'no-read-down' και 'no-write-up'.

Ο συγκεκριμένος μηχανισμός ελέγχου πρόσβασης θα μπορούσε να υλοποιηθεί ίσως για την εκπαίδευση και επιμόρφωση των εργαζομένων μέσα σε μια εταιρία με άκρως απόρρητες πληροφορίες.

<u>Εμπιστευτικότητα</u>

Ο βασικός στόχος της εμπιστευτικότητας σε ένα πληροφοριακό σύστημα είναι να προστατέψει από μη εξουσιοδοτημένους χρήστες το περιεχόμενο της πληροφορίας κατά τη διάρκεια της αποθήκευσης και της μεταφοράς. Οι μηχανισμοί που έχουν προαναφερθεί

συντελούν εμμέσως στην επίτευξη της εμπιστευτικότητας σε ένα περιβάλλον η-μάθησης καθώς έχουν ως στόχο την ασφάλεια του περιεχομένου.

Επιπλέον, η κρυπτογραφία αποτελεί βασικό στοιχείο των διαδικασιών που ακολουθούνται προκειμένου να διασφαλίσουμε ότι η προστατευόμενη πληροφορία δε θα αλλοιωθεί από κάποιον μη εξουσιοδοτημένο χρήστη. Ακολουθούν ορισμένα αντίμετρα ασφάλειας που υιοθετούνται τα οποία βασίζονται σε μηχανισμούς

Πρωτόκολλο ασφάλειας επικοινωνιών SSL (Secure Socket Layer) [39]

Το SSL είναι ένα πρωτόκολλο ασφάλειας που αναπτύχθηκε από την Netscape Communications Corporation, σε συνεργασία με την RSA Data Security, Inc. Ο πρωτεύων στόχος του πρωτοκόλλου SSL είναι η παροχή ενός ιδιωτικού καναλιού μεταξύ των εφαρμογών επικοινωνίας, το οποίο να εξασφαλίζει τη μυστικότητα/εμπιστευτικότητα των δεδομένων, την αυθεντικοποίηση των εμπλεκόμενων μερών και την ακεραιότητα των δεδομένων.

Το πρωτόκολλο SSL σχεδιάστηκε για να παρέχει μυστικότητα μεταξύ δύο εφαρμογών που επικοινωνούν (έναν πελάτη (client) και έναν εξυπηρετητή (server)). Επιπλέον, το πρωτόκολλο σχεδιάστηκε ώστε να επιτρέπει σε έναν SSL εξυπηρετητή να αυθεντικοποιεί τον εαυτό του σε έναν SSL πελάτη, να επιτρέπει στον πελάτη να αυθεντικοποιεί τον εαυτό του στον εξυπηρετητή και τέλος να επιτρέπει τη δημιουργία κρυπτογραφημένης σύνδεσης μεταξύ τους.

Μια κρυπτογραφημένη σύνδεση SSL απαιτεί όλες οι πληροφορίες που στέλνονται μεταξύ του πελάτη και του εξυπηρετητή να είναι κρυπτογραφημένες από το λογισμικό που τις αποστέλλει και να αποκρυπτογραφούνται από το λαμβάνουν λογισμικό, παρέχοντας κατά συνέπεια έναν υψηλό βαθμό εμπιστευτικότητας. Η εμπιστευτικότητα είναι σημαντική για αμφότερα τα συμβαλλόμενα μέρη σε οποιαδήποτε ‘ιδιωτική’ συναλλαγή. Επιπλέον, όλα τα στοιχεία που στέλνονται μέσω μιας κρυπτογραφημένης σύνδεσης SSL προστατεύονται με έναν μηχανισμό που ανιχνεύει τις αλλαγές που έχουν γίνει στα δεδομένα κατά τη μεταφορά τους από την πηγή στον προορισμό.

Το πρωτόκολλο SSL εμπεριέχει δύο υπό-πρωτόκολλα: Το *Πρωτόκολλο Καταγραφής SSL (SSL record protocol)* και το *Πρωτόκολλο Χειραψίας SSL (SSL Handshake protocol)*. Το πρώτο καθορίζει την μορφή με την οποία αναμεταδίδονται τα δεδομένα. Το δεύτερο χρησιμοποιεί το πρωτόκολλο καταγραφής για την ανταλλαγή μιας σειράς μηνυμάτων μεταξύ του εξυπηρετητή και του πελάτη όταν ο πρώτος δημιουργεί μια σύνδεση SSL μεταξύ τους. Αυτή η ανταλλαγή των μηνυμάτων έχει ως σκοπό να διευκολύνει τις ακόλουθες ενέργειες:

- Αυθεντικοποίηση του εξυπηρετητή στον εξυπηρετούμενο πελάτη.
- Επιτρέπει στον εξυπηρετητή και στον εξυπηρετούμενο να επιλέξουν τον κρυπτογραφικό αλγόριθμο που θα χρησιμοποιήσουν βάσει αυτών που υποστηρίζουν.
- Προαιρετικά την αυθεντικοποίηση του πελάτη στον εξυπηρετητή.
- Την χρησιμοποίηση κρυπτογράφησης δημοσίου κλειδιού για την δημιουργία κοινών μυστικών.
- Την δημιουργία μιας κρυπτογραφημένης σύνδεσης SSL.

Το πρωτόκολλο SSL παρέχει τη "ασφάλεια καναλιού" η οποία έχει τρεις βασικές ιδιότητες:

- το κανάλι είναι ιδιωτικό: η κρυπτογράφηση χρησιμοποιείται για όλα τα μηνύματα αφότου μια απλή ανταλλαγή μηνυμάτων χρησιμοποιηθεί για να καθορίσει ένα μυστικό κλειδί.
- το κανάλι επικυρώνεται: το σημείο εξυπηρέτησης της συνομιλίας επικυρώνεται πάντα, ενώ το σημείο τέλους πελατών επικυρώνεται προαιρετικά.
- το κανάλι είναι αξιόπιστο: η μεταφορά μηνυμάτων περιλαμβάνει έναν έλεγχο ακεραιότητας μηνυμάτων (που χρησιμοποιεί έναν MAC).

Αλγόριθμοι που χρησιμοποιούνται από το SSL

Το πρωτόκολλο SSL υποστηρίζει ποικιλία διαφορετικών αλγορίθμων κρυπτογράφησης για τη χρήση σε διαδικασίες όπως η αυθεντικοποίηση του εξυπηρετητή και του πελάτη, η διαβίβαση των πιστοποιητικών και η καθιέρωση των κλειδιών των συνόδων. Οι πελάτες και οι εξυπηρετητές ενδέχεται να υποστηρίζουν διαφορετικά σύνολα αλγορίθμων ανάλογα με την έκδοση της SSL που υποστηρίζουν καθώς και λόγω άλλων παραμέτρων. Μεταξύ των άλλων λειτουργιών του, το πρωτόκολλο χειραψίας του SSL καθορίζει πώς ο εξυπηρετητής και ο πελάτης διαπραγματεύονται ποιούς αλγορίθμους θα χρησιμοποιήσουν για να αυθεντικοποιήσουν ο ένας τον άλλον, για να διαβιβάσουν τα πιστοποιητικά και για να καθιερώσουν τα κλειδιά των συνδέσεων.

Οι αλγόριθμοι που χρησιμοποιούνται είναι οι εξής:

- **DES**. Data Encryption Standard, ένας αλγόριθμος κρυπτογράφησης που χρησιμοποιείται από την Αμερικανική κυβέρνηση.
- **DSA**. Digital Signature Algorithm, μέρος των ψηφιακών προτύπων επικύρωσης που χρησιμοποιούνται από την Αμερικανική κυβέρνηση.
- **KEA**. Key Exchange Algorithm, ένας αλγόριθμος που χρησιμοποιείται για την ανταλλαγή κλειδιών από την Αμερικανική κυβέρνηση.
- **MD5**. Message Digest Algorithm, αλγόριθμος που αναπτύχθηκε από τον Rivest.
- **RC2** και **RC4.** ciphers κρυπτογράφησης του Rivest που αναπτύσσονται για την RSA Data Security.
- **RSA**. Ένας αλγόριθμος δημοσίου-κλειδιού που χρησιμοποιείται για κρυπτογράφηση και για αυθεντικοποίηση. Αναπτυγμένος από τους Rivest, Shamir, και Adleman.
- **RSA Key-Exchange**. Ένας αλγόριθμος ανταλλαγής-κλειδιών για τη SSL βασισμένος στον αλγόριθμο RSA.
- **SHA-1**. Secure Hash Algorithm. Μια συνάρτηση κατακερματισμού που χρησιμοποιείται από την Αμερικανική κυβέρνηση.
- **SKIPJACK**. Ένας απόρρητος αλγόριθμος δημοσίου-κλειδιού που εφαρμόζεται στο FORTEZZA.

- **Triple DES**. DES που εφαρμόζεται τρεις φορές.

Αλγόριθμοι ανταλλαγής κλειδιών (Key Exchange) όπως είναι ο KEA και ο RSA keyexchange, καθορίζουν τον τρόπο με τον οποίο ο εξυπηρετητής και ο πελάτης καθορίζουν το συμμετρικό κλειδί που θα χρησιμοποιήσουν κατά την διάρκεια της SSL σύνδεσης. Ο συνηθέστερος SSL Cipher suite που χρησιμοποιούν είναι ο RSA key-exchange.

Οι διαχειριστές μπορούν να ενεργοποιήσουν ή απενεργοποιήσουν οποιεσδήποτε από τους υποστηριζόμενους αλγορίθμους τόσο για τους πελάτες όσο και για τους εξυπηρετητές. Όταν ένας πελάτης και ένας εξυπηρετητής ανταλλάσσουν πληροφορίες κατά τη διάρκεια του πρωτοκόλλου χειραψίας, προσδιορίζουν τους ισχυρότερους αλγορίθμους που υποστηρίζουν και οι δύο μεριές και χρησιμοποιούν εκείνους για τη μεταξύ τους επικοινωνία.

Ασφάλεια σε υπηρεσίες ιστού (WS-Security) [39]

Η υπηρεσία ιστού (web service) [3, 4, 20] είναι κάθε υπηρεσία που είναι διαθέσιμη μέσω του διαδικτύου (internet) ή ιδιωτικών εταιρικών δικτύων (intranets), χρησιμοποιεί ένα τυποποιημένο σύστημα XML επικοινωνίας και δεν είναι συνδεδεμένη με οποιοδήποτε λειτουργικό σύστημα ή γλώσσα προγραμματισμού. Οι υπηρεσίες ιστού επιτρέπουν σε εφαρμογές και σε διαδικτυακές συσκευές να επικοινωνούν μεταξύ τους και να συνδυάζουν τη λειτουργικότητά τους, για να παρέχουν υπηρεσίες μεταξύ τους.

Οι υπηρεσίες ιστού απαιτούν αρκετές συγγενικές τεχνολογίες βασισμένες στην XML για να μεταφέρουν και να μετασχηματίζουν δεδομένα μέσα και έξω από προγράμματα και βάσεις δεδομένων.

Extensible Markup Language (XML)

Η XML σχεδιάστηκε για να ξεπεράσει περιορισμούς της HyperText Markup Language (HTML) και ειδικότερα να υποστηρίξει καλύτερα τη δημιουργία και τη διαχείριση δυναμικού περιεχομένου. Επιπλέον δίνει στα έγγραφα ένα μεγαλύτερο επίπεδο προσαρμοστικότητας στη μορφή και τη δομή από αυτό που υπήρχε παλαιότερα στην HTML. Η XML προσφέρει στους σχεδιαστές της HTML τη δυνατότητα να προσθέτουν περισσότερα στοιχεία στη γλώσσα.. Στην HTML οι ετικέτες (tags) είναι προκαθορισμένες, ενώ η XML παρέχει τη δυνατότητα στους χρήστες να καθορίζουν τις ετικέτες.

Simple Object Access Protocol (SOAP)

Το SOAP [1, 6, 7, 19, 30] είναι ένα πρωτόκολλο σχεδιασμένο για την ανταλλαγή XML εγγράφων μέσω διαφορετικών πρότυπων τεχνολογιών διαδικτύου, συμπεριλαμβανομένων των HTTP, Simple Mail Transfer Protocol (SMTP) και File Transfer Protocol (FTP). Το SOAP είναι βασικά ένα μοντέλο μονόδρομης επικοινωνίας, το οποίο εγγυάται ότι ένα μήνυμα μεταφέρεται από τον αποστολέα στον παραλήπτη, ενδεχομένως περιλαμβάνοντας ενδιάμεσους σταθμούς που μπορούν να επεξεργαστούν μέρος του μηνύματος ή να το μεταβάλουν.

Web Services Description Language (WSDL) - Γλώσσα Περιγραφής Υπηρεσιών Ιστού

Για να ολοκληρωθεί η αρχιτεκτονική επικοινωνίας των υπηρεσιών ιστού είναι να καθοριστεί το πως οι χρήστες θα έχουν πρόσβαση σε μία υπηρεσία μόλις αυτή τεθεί σε εφαρμογή. Η WSDL προδιαγραφή παρέχει ένα συμβόλαιο μεταξύ του αιτούντος και του παροχέα της υπηρεσίας.

Περιγράφει ένα κοινό τρόπο στον οποίο παρουσιάζονται οι τύποι των δεδομένων που λαμβάνουν χώρα στα μηνύματα, οι λειτουργίες οι οποίες πρόκειται να εκτελεστούν στα μηνύματα και η αντιστοίχηση των μηνυμάτων πάνω σε συναλλαγές του δικτύου. Η WSDL έχει XML μορφή, η οποία περιγράφει τι κάνει μια υπηρεσία, πως υλοποιεί τις λειτουργίες της και που θα τη βρούμε.

Η WSDL διαιρείται σε τρία βασικά στοιχεία και επτά τμήματα τα όποια είναι: τα data type definitions, τα abstract operations και τα service bindings. Κάθε βασικό στοιχείο μπορεί να καθοριστεί σε ένα ξεχωριστό XML έγγραφο και να εισαχθεί σε διαφορετικούς συνδυασμούς για να δημιουργήσει μια τελική περιγραφή υπηρεσιών ιστού ή μπορεί όλα να οριστούν σε ένα μόνο έγγραφο. Τα data type definitions (Data types, Messages) προσδιορίζουν τη δομή και το περιεχόμενο των μηνυμάτων. Τα Abstract Operations (Operations, Port Types, Binding) προσδιορίζουν τις λειτουργίες που εκτελούνται στο περιεχόμενο του μηνύματος και τα Service Bindings (Port, Service) προσδιορίζουν τη μετάδοση δεδομένων, η οποία θα μεταφέρει το μήνυμα στον προορισμό του.

Universal Description, Discovery and Integration (UDDI) - Πρωτόκολλο Περιγραφής, Ανακάλυψης και Ολοκλήρωσης

Το UDDI ως τεχνική προδιαγραφή παρέχει μια μέθοδο για δημοσίευση και εύρεση των περιγραφών μιας υπηρεσίας. Είναι μια κεντρική υπηρεσία καταλόγου, όπου υπηρεσίες ιστού μπορούν να καταχωρηθούν και να προσδιοριστούν σε έναν παροχέα υπηρεσιών.

Μηχανισμοί ασφάλειας στις υπηρεσίες ιστού [39]

XML Κρυπτογράφηση

Οι βασικοί στόχοι της XML κρυπτογράφησης (XML Encryption) [43] [44] είναι:

- Υποστήριξη της κρυπτογράφησης οποιουδήποτε αυθαίρετου ψηφιακού περιεχομένου, συμπεριλαμβανομένων των XML εγγράφων.
- Εξασφάλιση ότι τα κρυπτογραφημένα δεδομένα, κατά τη μεταφορά ή την αποθήκευση, δεν μπορούν να προσπελασθούν από μη εξουσιοδοτημένα πρόσωπα.
- Διατήρηση της ασφάλειας των δεδομένων όχι μόνο όταν τα δεδομένα μεταφέρονται (πράγμα που εγγυάται το SSL), αλλά και όταν είναι σε στάση σε έναν συγκεκριμένο κόμβο.
- Παρουσίαση των κρυπτογραφημένων δεδομένων σε XML μορφή.
- Είναι δυνατό τμήματα του XML να κρυπτογραφηθούν επιλεκτικά.

Σε αντίθεση με την XML κρυπτογράφηση, χρησιμοποιώντας SSL άνω του HTTP (γνωστό ως HTTPS), ολόκληρο το μήνυμα κρυπτογραφείται. Ολόκληρο το μήνυμα αποκρυπτογραφείται έπειτα στον πρώτο προορισμό και είναι ανοικτό για επισκόπηση (snooping) προτού κρυπτογραφηθεί πάλι συνολικά για το δεύτερο άλμα. Η κρυπτογράφηση που προσφέρεται από το SSL άνω του HTTP υπάρχει μόνο για μεταφορά και δεν είναι σταθερή.

Η συγκεκριμένη προδιαγραφή καθορίζει μια διαδικασία για κρυπτογράφηση δεδομένων και παρουσίαση του αποτελέσματος σε XML. Τα δεδομένα μπορούν να είναι αυθαίρετα δεδομένα (συμπεριλαμβανομένου ενός εγγράφου XML), ένα στοιχείο XML, ή περιεχόμενα στοιχείου XML. Το αποτέλεσμα της κρυπτογράφησης δεδομένων είναι ένα στοιχείο EncryptedData, που περιέχει ή προσδιορίζει (μέσω μιας αναφοράς URI) τα cipher δεδομένα.

XML Ψηφιακές Υπογραφές

Οι XML ψηφιακές υπογραφές (XML Digital Signatures) [11] είναι ένα πρότυπο για την ασφαλή επικύρωση της προέλευσης των μηνυμάτων. Η προδιαγραφή της XML υπογραφής επιτρέπει στα έγγραφα XML να υπογραφούν με ένα τυποποιημένο τρόπο, χρησιμοποιώντας διαφορετικούς αλγόριθμους ψηφιακής υπογραφής. Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν για επικύρωση των μηνυμάτων και για μη-αποποίηση. Η αναλυτική περιγραφή των ψηφιακών υπογραφών θα γίνει στην απαίτηση ασφάλειας της μη-άρνησης της ευθύνης.

Το πρότυπο XML υπογραφής παρέχει ένα σύνολο κανόνων και μια XML σύνταξη για την κωδικοποίηση, τον υπολογισμό και την επαλήθευση των ψηφιακών υπογραφών από τα αυθαίρετα δεδομένα. Εκτός από την παροχή πιστοποίησης, ακεραιότητας δεδομένων και υποστήριξη για μη-αποποίηση των δεδομένων που υπογράφονται, η XML υπογραφή έχει σχεδιαστεί για να εκμεταλλεύεται το διαδίκτυο και την XML. Ένα θεμελιώδες χαρακτηριστικό γνώρισμα της XML υπογραφής είναι η δυνατότητα να υπογράφει συγκεκριμένα τμήματα του XML εγγράφου, αντί για το πλήρες έγγραφο. Αυτό γίνεται χρήσιμο όταν τα έγγραφα αθροίζουν πολλά κομμάτια πληροφορίας από διαφορετικές πηγές, κάθε ένα με τη δική του απόδειξη αυθεντικότητας. Η επικύρωση μιας υπογραφής απαιτεί ότι τα υπογεγραμμένα δεδομένα είναι προσιτά με κάποιο είδος αναφοράς. Αυτή η αναφορά μπορεί να είναι ένα URI, ένα μέρος του ίδιου πόρου με την υπογραφή, που ενσωματώνεται μέσα στην υπογραφή, ή ενσωματώνει την υπογραφή μέσα σε αυτό.

XML Key Management Specification (XKMS)

Μια από τις μεγαλύτερες απαιτήσεις για την ανάπτυξη όλων αυτών των νέων τεχνολογιών κρυπτογράφησης, ψηφιακών υπογραφών και πιστοποίησης, είναι να διατηρηθούν όλα τα δημόσια και ιδιωτικά κλειδιά, οι ψηφιακές υπογραφές και τα ψηφιακά πιστοποιητικά οργανωμένα και ασφαλή. Αρκετά προϊόντα υποδομής δημόσιου κλειδιού (PKI) της αγοράς σχεδιάστηκαν για να απλοποιήσουν τη διαχείριση αυτών των συστατικών ασφάλειας. Παρόλα αυτά, δεν υπάρχει ακόμα ένας πρότυπος τρόπος για την προσπέλαση τέτοιων συστημάτων σε ένα περιβάλλον υπηρεσιών ιστού βασισμένων στο πρωτόκολλο SOAP.

Η XKMS [22] δημιουργήθηκε κάτω από την επίβλεψη του W3C, με σκοπό να παρέχει ένα τυποποιημένο σύνολο XML ορισμών για τη διαχείριση των υπηρεσιών πιστοποίησης, κρυπτογράφησης και ψηφιακών υπογραφών. Αυτό επιτρέπει στους σχεδιαστές να έχουν μια έμπιστη τρίτη οντότητα που βρίσκει και παρέχει τα κατάλληλα κλειδιά και πιστοποιητικά. Αυτή η έμπιστη τρίτη οντότητα ενεργεί σαν μεσάζοντας, ο οποίος απελευθερώνει τον προγραμματιστή της υπηρεσίας ιστού από την υποχρέωση να ελέγχει τη διαθεσιμότητα των κλειδιών ή των πιστοποιητικών και να εξασφαλίζει την εγκυρότητά τους.

Security Assertion Markup Language (SAML)

Η SAML [36] [38] έχει αναπτυχθεί από την OASIS XML-Based Security Services Technical Committee (SSTC). Είναι ένα πλαίσιο βασισμένο σε XML για την ανταλλαγή ασφαλούς πληροφορίας. Αυτή η ασφαλής πληροφορία εκφράζεται στη μορφή των δηλώσεων γύρω από υποκείμενα, όπου ένα υποκείμενο είναι μια οντότητα (άνθρωπος ή υπολογιστής) η οποία έχει μια ταυτότητα σε μερικά ασφαλή πεδία. Ένα τυπικό παράδειγμα ενός υποκειμένου είναι ένα άτομο, ταυτοποιημένο από τη διεύθυνση του ηλεκτρονικού ταχυδρομείου του σε ένα ειδικό internet DNS πεδίο. Οι δηλώσεις μπορούν να μεταφέρουν πληροφορία σχετικά με ενέργειες αυθεντικοποίησης και θέματα εξουσιοδότησης σχετικά με το πότε τα υποκείμενα επιτρέπεται να έχουν πρόσβαση σε κάποιους πόρους.

Η SAML ορίζει ένα πρωτόκολλο με το οποίο οι πελάτες μπορούν να αιτηθούν δηλώσεις από τις SAML αρχές και να πάρουν μια απάντηση από αυτές. Αυτό το πρωτόκολλο αποτελείται από μορφές αίτησης και ανταπόκρισης βασισμένες σε XML, που μπορούν να οριοθετηθούν σε αρκετά διαφορετικές υποκείμενες επικοινωνίες και πρωτόκολλα μεταφοράς. Οι SAML αρχές μπορεί να χρησιμοποιούν διαφορετικές πηγές πληροφορίας, όπως εξωτερική πολιτική τροφοδοσίας, αποθήκευσης και δηλώσεων, η οποία έχει αποκτηθεί ως είσοδο στις αιτήσεις, δημιουργώντας τις απαντήσεις.

eXtensible Access Control Markup Language (XACML)

Η XACML [37] ακολουθήθηκε για να ορίσει ένα βασικό σχήμα για τη δήλωση των πολιτικών εξουσιοδότησης σε XML έναντι αντικειμένων τα οποία ταυτοποιούνται από μόνα τους σε XML.

Υπάρχουν αρκετές ιδιόκτητες ή καθορισμένες από εφαρμογή γλώσσες πολιτικής ελέγχου προσπέλασης, αλλά αυτές οι πολιτικές δεν μπορούν να μοιραστούν πέραν διαφορετικών εφαρμογών και παρέχουν ασήμαντο κίνητρο για να αναπτύξουν εργαλεία συγκρότησης πολιτικής.

Ακεραιότητα

Στόχος της απαίτησης ασφάλειας της ακεραιότητας είναι η προστασία του περιεχομένου από τη μη εξουσιοδοτημένη τροποποίησή ή διαγραφή του κατά τη μεταφορά του. Πιο συγκεκριμένα, είναι η διασφάλιση πως το περιεχόμενο των δεδομένων που αποστέλλονται είναι ακριβώς ίδια με αυτά που φτάνουν στον παραλήπτη. Προκειμένου να υλοποιήσουμε την ακεραιότητα σε ένα περιβάλλον η-μάθησης θα πρέπει να ισχύουν τα παρακάτω:

- Αποτελεσματική και ισχυρή ταυτοποίηση και αυθεντικοποίηση
- Αποτελεσματική εξουσιοδότηση χρηστών.
- Ασφαλές (εμπιστευτικό) περιβάλλον διακίνησης δεδομένων μέσω ασφαλών καναλιών επικοινωνίας
- Χρήση του Κωδικού Αυθεντικοποίησης Μηνύματος (Message Authentication Code – MAC): Είναι ένας μηχανισμός ελέγχου ακεραιότητας μηνύματος και βασίζεται σε μια συνάρτηση κατακερματισμού που δέχεται ως είσοδο ένα μυστικό κλειδί και ένα μήνυμα τυχαίου μεγέθους (πληροφορία προς αυθεντικοποίηση) και έχει ως έξοδο ένα κωδικό αυθεντικοποίησης μηνύματος-πληροφορίας.

Ο αποστολέας παράγει τον κωδικό αυθεντικοποίησης μηνύματος τον οποίο αποστέλλει μαζί με το αυθεντικό μήνυμα στον παραλήπτη

Ο παραλήπτης υπολογίζει τον κωδικό χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού (keyed-MD5) μαζί με το διαμοιραζόμενο μυστικό κλειδί και στη συνέχεια συγκρίνει τους δύο κωδικούς μεταξύ τους.

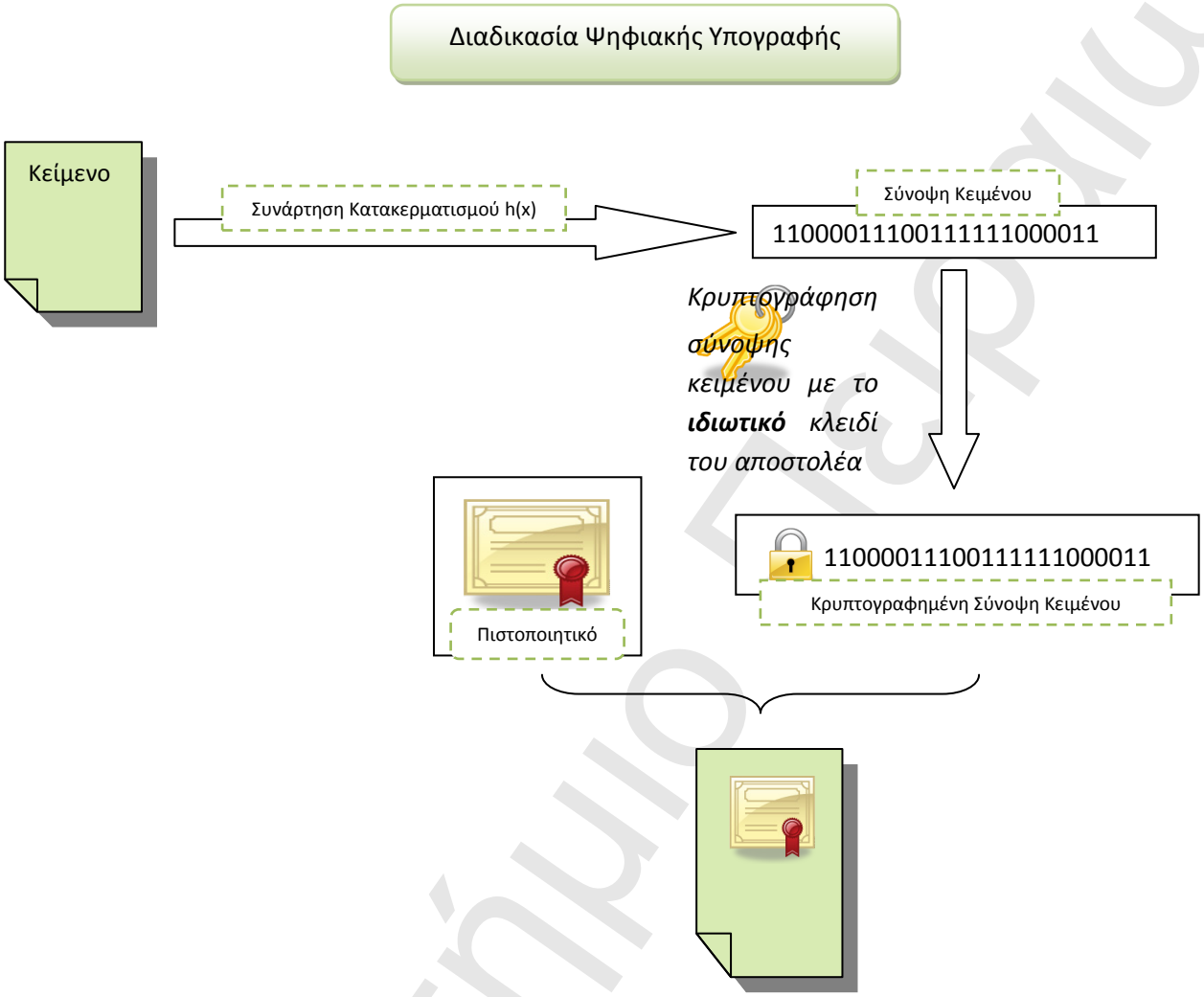
Μη Άρνηση Ευθύνης

Σε ένα ασφαλές περιβάλλον η-μάθησης κάθε δραστηριότητα χρήστη θα πρέπει να αντιστοιχίζεται και να συνδέεται άρρηκτα με κάποιο χρήστη. Στόχος είναι να αποκλειστεί η πιθανότητα κάποιος χρήστη να αμφισβητήσει την εγκυρότητα του συστήματος. Βασικός μηχανισμός που διασφαλίζει την απαίτηση αυτή είναι οι ψηφιακές υπογραφές.

Ψηφιακές Υπογραφές και Χρονοσφράγιση

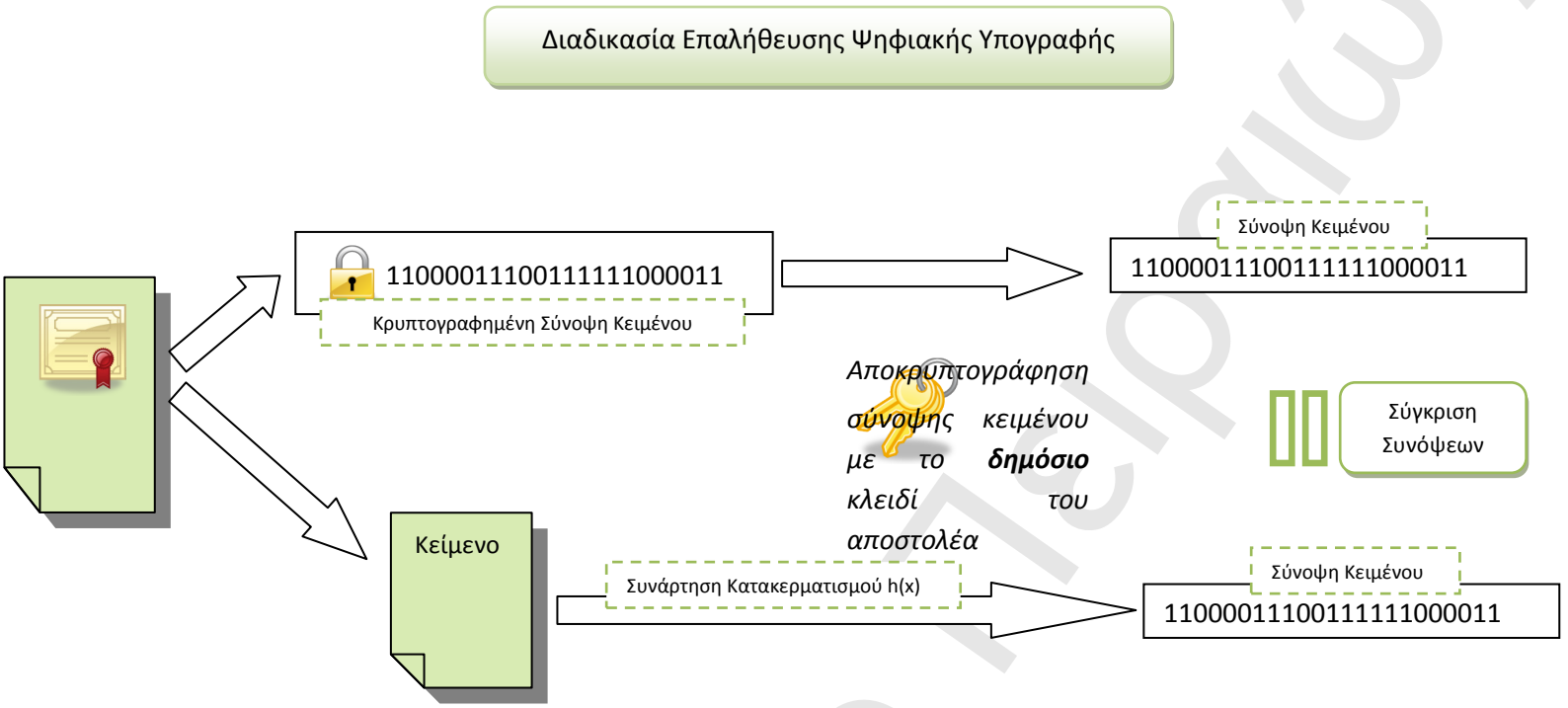
Το γεγονός ότι στην ισόμετρη κρυπτογραφία το ιδιωτικό κλειδί το έχει μόνο ο ιδιοκτήτης του, σημαίνει ότι το αποτέλεσμα οποιασδήποτε συνάρτησης χρησιμοποιεί το κλειδί αυτό, μπορεί να θεωρηθεί ότι έχει επιτελεστεί από τον συγκεκριμένο ιδιοκτήτη και κανέναν άλλο. Μια ψηφιακή υπογραφή δημιουργείται από την χρήση του ιδιωτικού κλειδιού προκειμένου να «υπογραφούν» ηλεκτρονικά δεδομένα με τέτοιο τρόπο που να μην μπορεί να πλαστογραφηθεί.

Στο ακόλουθο σχήμα παρουσιάζεται η τυπική διαδικασία δημιουργίας μιας ψηφιακής υπογραφής. Αρχικά εφαρμόζεται μια συνάρτηση κατακερματισμού h(x) στο κείμενο που θα υπογραφεί. Στη συνέχεια η σύνοψη που προκύπτει κρυπτογραφείται με το ιδιωτικό κλειδί του υπογράφοντος σύμφωνα με έναν συγκεκριμένο αλγόριθμο και έτσι προκύπτει μια κρυπτογραφημένη σύνοψη. Αυτή ακριβώς η κρυπτογραφημένη σύνοψη αποτελεί την «ψηφιακή υπογραφή» και αποστέλλεται μαζί με το κείμενο στον παραλήπτη, συνοδευμένη από το δημόσιο κλειδί του αποστολέα.



Σχήμα 7. Ψηφιακή Υπογραφή

Στο Σχήμα 7 παρουσιάζεται η τυπική διαδικασία δημιουργίας μιας ψηφιακής υπογραφής. Αρχικά εφαρμόζεται μια συνάρτηση κατακερματισμού h(x) στο κείμενο που θα υπογραφεί. Στη συνέχεια η σύνοψη που προκύπτει κρυπτογραφείται με το ιδιωτικό κλειδί του υπογράφοντος σύμφωνα με έναν συγκεκριμένο αλγόριθμο και έτσι προκύπτει μια κρυπτογραφημένη σύνοψη. Αυτή ακριβώς η κρυπτογραφημένη σύνοψη αποτελεί την «ψηφιακή υπογραφή» και αποστέλλεται μαζί με το κείμενο στον παραλήπτη, συνοδευμένη από το δημόσιο κλειδί του αποστολέα.



Σχήμα 8. Επαλήθευση Ψηφιακής Υπογραφής

Η επαλήθευση της ψηφιακής υπογραφής ακολουθεί μια παρόμοια διαδικασία που αποτελείται από δύο υποεργασίες. Στην πρώτη υποεργασία χρησιμοποιείται ο ίδιος αλγόριθμος μαζί με το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφηθεί η σύνοψη. Στη δεύτερη υποεργασία, χρησιμοποιείται η ίδια συνάρτηση κατακερματισμού h(x) που εφαρμόστηκε και κατά την δημιουργία της υπογραφής για να ληφθεί και πάλι η σύνοψη του κειμένου. Στο τελευταίο βήμα συγκρίνονται οι δύο συνόψεις που έχουν προκύψει. Εάν είναι εντελώς όμοιες, τότε η ψηφιακή υπογραφή είναι έγκυρη και άρα είναι όντως υπογεγραμμένη από το συγκεκριμένο αποστολέα και δεν έχει αλλοιωθεί κατά την αποστολή. Εάν οι συνόψεις διαφέρουν τότε η υπογραφή είναι άκυρη.

Οι ψηφιακές υπογραφές χρησιμοποιούνται σε έναν αριθμό υπηρεσιών ασφάλειας. Προσδίδουν έλεγχο αυθεντικότητας ή αυθεντικοποίηση σε ένα μήνυμα, εξασφαλίζοντας ότι αυτό έχει προέλθει από έναν συγκεκριμένο χρήστη, ο οποίος είναι ο μοναδικός κάτοχος του ιδιωτικού κλειδιού. Η ψηφιακή υπογραφή προστατεύει το μήνυμα από μη εξουσιοδοτημένη μεταποίηση προσδίνοντας έναν έλεγχο ακεραιότητας. Παρόλο που από μόνη της η υπογραφή δεν είναι αρκετή για να επιτύχει την υπηρεσία μη-άρνησης συμμετοχής (non-repudiation), μια ψηφιακή υπογραφή κατασκευασμένη σε συνδυασμό με κατάλληλα δεδομένα όπως δεδομένα χρονοσφράγισης μπορεί να παρέχει ένα μέρος της υπηρεσίας μη-άρνησης.

Καταγραφή Δραστηριότητας Χρηστών

Η καταγραφή δραστηριότητας χρηστών αποτελεί ένα επιπλέον αντίμετρο ασφάλειας το οποίο ικανοποιεί την μη άρνηση της ευθύνης καθώς συνδυαζόμενη με μια έγκυρη υπηρεσία χρονοσφράγισης έχει τη δυνατότητα να διατηρεί ένα ιστορικό ενεργειών χρήστη καταγράφοντας όλη τη πλοηγητική του δραστηριότητα μέσα σε ένα ΣΔΗΜ.

Διαθεσιμότητα

Ο βασικός στόχος της διαθεσιμότητας είναι να διασφαλίσει την αδιάκοπη και αξιόπιστη πρόσβαση στις υπηρεσίες και το περιεχόμενο ενός πληροφοριακού συστήματος η-μάθησης.

Σε ένα σενάριο χρήσης της πλατφόρμας για την πραγματοποίηση η-εξετάσεων ενός μαθήματος, η διαθεσιμότητα του συστήματος αποτελεί κρίσιμη προϋπόθεση ομαλής διεξαγωγής τους. Για τη διασφάλιση της αδιάλειπτης παροχής υπηρεσιών ενός τέτοιου συστήματος θα πρέπει να υλοποιηθούν τα παρακάτω:

- Πλάνο ανάκαμψης καταστροφών
- Αποτελεσματική στρατηγική δημιουργίας αντιγράφων ασφαλείας
- Εγκατάσταση και συνεχής ενημέρωση απαραίτητου λογισμικού για την αποφυγή ιών και κακόβουλων λογισμικών.

4.3 Συνοπτικός Οδηγός Εφαρμογής Σχεδίου Πολιτικής Ασφάλειας Πληροφοριών σε Περιβάλλοντα η-Μάθησης

Στον παρακάτω πίνακα φαίνονται συνοπτικά οι συνιστώσες του Πλαισίου Ασφάλειας Πληροφοριών και οι απαραίτητες ενέργειες που τις συνιστούν. Ο συγκεκριμένος πίνακας αποτελεί μια πηγή αναφοράς για την εφαρμογή του Πλαισίου σε ένα περιβάλλον η-μάθησης και αποσκοπεί στην μελλοντική υλοποίηση ενός ολοκληρωμένου οδηγού εφαρμογής του Πλαισίου.

Συνιστώσα Πλαισίου Ασφάλειας Πληροφοριών	Ενέργειες
Διοίκηση Ασφάλειας Πληροφοριών	✓ Πλαίσιο διοίκησης ασφάλειας ✓ Πρόγραμμα σεμιναρίων ενημέρωσης των χρηστών ✓ Αποτελεσματική παρακολούθηση ασφάλειας ✓ Σύστημα διαχείρισης και αντιμετώπισης περιστατικών ασφάλειας
Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών	✓ Ορισμός της ασφάλειας πληροφοριών προσανατολισμένη στους σκοπούς του οργανισμού και του περιβάλλοντος η-μάθησης ✓ Αναφορά στους σκοπούς της διοίκησης έτσι όπως διαμορφώνονται από την υιοθέτηση μηχανισμών ασφάλειας πληροφοριών σύμφωνους με την επιχειρησιακή στρατηγική.

	✓ Συνοπτική περιγραφή και επεξήγηση των πολιτικών, αρχών, προτύπων και διαδικασιών ασφάλειας ✓ Αναφορά των ευθυνών και αρμοδιοτήτων στη διαχείριση ασφάλειας πληροφοριών. ✓ Παραπομπές στην γραπτή τεκμηρίωση της πολιτικής ασφάλειας	
Ευαισθητοποίηση/Ενημέρωση Χρηστών	✓ Ολοκληρωμένο πακέτο τακτικής εκπαίδευσης και ενημέρωσης των χρηστών	
Διαδικασία Διαχείρισης και Αντιμετώπισης Περιστατικών Ασφάλειας	✓ Συγκρότηση ομάδας αντιμετώπισης περιστατικών ασφάλειας ✓ Προτυποποιημένη αναφορά περιστατικών και αδυναμιών ασφάλειας ✓ Ενημέρωση και εκπαίδευση του αρμόδιου προσωπικού ✓ Αναφορά αδυναμιών ασφάλειας με προτυποποιημένη διαδικασία	
Σύστημα Μέτρησης Ασφάλειας ΠΣ	✓ αξιολόγηση των επιδόσεων της ασφάλειας πληροφοριών	
Υιοθέτηση και Υλοποίηση Αντιμέτρων Ασφάλειας (τεχνική συνιστώσα)	**Ταυτοποίηση και Αυθεντικοποίηση**	✓ Μηχανισμοί Κωδικού Πρόσβασης (Password-Based Mechanisms): ✓ Υποδομή Δημόσιου Κλειδιού ✓ Token-based μηχανισμοί ✓ Βιομετρική ✓ Υβριδική Ταυτοποίηση ➢ Βιομετρικές Έξυπνες Κάρτες ➢ Έξυπνες Κάρτες ΥΔΚ
	Εξουσιοδότηση	✓ Έλεγχος πρόσβασης βάσει ιδιοτήτων (ABAC) ✓ Διακριτικός Έλεγχος Πρόσβασης (Discretionary Access Control (DAC)) ✓ Έλεγχος Πρόσβασης βάσει ρόλων (Role-based Access Control) ✓ Αυστηρός Έλεγχος Πρόσβασης (Mandatory Control Access)
	Εμπιστευτικότητα	✓ Υποδομή Δημόσιου Κλειδιού ✓ Πρωτόκολλο ασφάλειας επικοινωνιών SSL (Secure Socket Layer) ✓ Ασφάλεια σε υπηρεσίες ιστού (WS-Security) ➢ XML Κρυπτογράφηση ➢ eXtensible Access Control Markup Language (XACML) ➢ XML Ψηφιακές Υπογραφές ➢ XML Key Management Specification

		(XKMS) ➢ Security Assertion Markup Language (SAML)
	Ακεραιότητα	✓ Message Authentication Code – MAC ✓ Μηχανισμοί ακεραιότητας ΥΔΚ
	Μη Άρνηση Ευθύνης	✓ Ψηφιακές Υπογραφές ✓ Μηχανισμοί ΥΔΚ
	Διαθεσιμότητα	✓ Πλάνο Επιχειρησιακής Συνέχειας ✓ Στρατηγική δημιουργίας αντιγράφων ασφάλειας ✓ Ενημέρωση απαραίτητου λογισμικού

Πίνακας 4. Συγκεντρωτικός Πίνακας Σχεδίου Πολιτικής Ασφάλειας Πληροφοριών σε Περιβάλλοντα η-Μάθησης

Αρχιτεκτονική Ασφαλών η-Εξετάσων μέσω Ιστού - SWBES[16]

Στο παρόν κεφάλαιο, έχοντας το Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών ως οδηγό, θα προταθεί μια Αρχιτεκτονική Ασφαλών η-λεκτρονικών Εξετάσεων σε περιβάλλοντα η-μάθησης το οποίο έχει ως στόχο τη διασφάλιση της διαδικασίας των η-εξετάσεων στο σύνολό της αλλά και την αντιστοίχιση/εφαρμογή του Σχεδίου Πολιτικής Ασφάλειας σε ένα πραγματικό σενάριο χρήσης.

Τόσο η εξέταση ενός μαθήματος όσο και η συνολική αξιολόγηση ενός εκπαιδευόμενου αποτελούν ίσως τις πιο κρίσιμες υπηρεσίες που προσφέρει ένα ΣΔΗΜ. Στο κεφάλαιο 3, καταγράφηκαν οι απειλές ασφάλειας που εμφανίζονται κατά τη διαδικασία εξέτασης και αξιολόγησης καθώς και οι μηχανισμοί που υλοποιούνται σε ένα από τα πιο αναγνωρισμένα ΣΔΗΜ όπως το Moodle

Για τους σκοπούς του παρόντος κεφαλαίου αναπτύχθηκε η εφαρμογή η-εξετάσεων SWBES η οποία αποτελεί τον πυρήνα της προτεινόμενης Αρχιτεκτονικής και υλοποιεί μηχανισμούς ασφάλειας σύμφωνους με το Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών. Πιο συγκεκριμένα, απευθύνεται στους βασικούς χρήστες των ΣΔΗΜ (Εκπαιδευτής/Εξεταστής, Εκπαιδευόμενος/Εξεταζόμενος, Διαχειριστής), οι οποίοι έχουν τη δυνατότητα μετάβασης από ένα περιβάλλον μάθησης σε ένα ασφαλές περιβάλλον εξέτασης ενσωματώνοντας τη διαδικασία εξέτασης μέσα σε κάποιο μάθημα. Η προσέγγιση της υλοποίησης του SWBES ήταν να χρησιμοποιηθεί με τους παρακάτω τρόπους ως:

- Αυτόνομο εργαλείο το οποίο συμμετέχει στην εκπαιδευτική διαδικασία ως εξωτερική υπηρεσία χωρίς καμία αλληλεπίδραση με το ΣΔΗΜ.
- Ολοκληρωμένη υπηρεσία η-εξετάσεων ενσωματωμένη και πλήρως διαλειτουργική με το ΣΔΗΜ, προσβάσιμη μέσα από το περιβάλλον η-μάθησης Moodle.

Τα βασικά λειτουργικά χαρακτηριστικά του SWBES είναι τα εξής:

1. Διαχείριση διαδικασίας εξετάσεων (παρακολούθηση διαδικασίας)
2. Αυτοματοποιημένη συγγραφή η-εγγράφων εξετάσεων
3. Εξέταση εκπαιδευόμενων
4. Αυτόματη βαθμολόγηση η-εγγράφων εξέτασης

Γίνεται αντιληπτό ότι το SWBES διαχειρίζεται ευαίσθητες και κρίσιμες πληροφορίες οι οποίες θα πρέπει να διασφαλίζονται κατά τη μεταφορά τους, αποθήκευση τους και πρόβολη τους μόνο σε εξουσιοδοτημένους χρήστες έτσι ώστε να καλύπτονται οι βασικές απαιτήσεις όπως αναφέρονται στην τεχνική συνιστώσα ασφάλειας του Σχεδίου.

Στη συνέχεια του κεφαλαίου θα γίνει η περιγραφή της προτεινόμενης αρχιτεκτονικής ασφαλών η-εξετάσεων, η λειτουργική περιγραφή του SWBES και τέλος θα γίνει συγκριτική αξιολόγηση ασφάλειας της προτεινόμενης αρχιτεκτονικής (όπως ορίζονται από το Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών) με τους μηχανισμούς που αναπτύχθηκαν.

[16] Secure Web-Based Exam System (SWBES)

5.1 Αρχιτεκτονική Ασφαλών η-Εξετάσεων μέσω Ιστού σε Περιβάλλοντα η-Μάθησης

Όπως ήδη αναφέρθηκε, στόχος του κεφαλαίου είναι η πρόταση μιας ευρύτερης Αρχιτεκτονικής ασφαλών η-εξετάσεων σε περιβάλλοντα η-μάθησης. Για να μπορέσουμε να οδηγηθούμε σε μια ολοκληρωμένη αρχιτεκτονική, θα πρέπει να ερευνήσουμε το αντικείμενο των η-εξετάσεων έτσι ώστε να καταγράψουμε όλες τις απαραίτητες λειτουργικές ανάγκες και απαιτήσεις.

5.1.1 Διαδικασία Αξιολόγησης Εκπαιδευόμενου

Ένα από τα βασικά και κρίσιμα λειτουργικά χαρακτηριστικά ενός ΣΔΗΜ αποτελεί η διαδικασία αξιολόγησης των εκπαιδευόμενων. Η διαδικασία αυτή περιλαμβάνει τρεις βασικές φάσεις:

- Συγγραφή και επιλογή θεμάτων εξέτασης
- Διεξαγωγή των εξετάσεων από τους εκπαιδευόμενους
- Βαθμολόγηση εξεταζόμενων

Οι τρεις παραπάνω φάσεις υλοποιούνται από μηχανισμούς που διαχειρίζονται ευαίσθητα και κρίσιμα δεδομένα. Όπως γίνεται αντιληπτό, η διασφάλιση της διαδικασίας κρίνεται απαραίτητη. Κάθε ΣΔΗΜ υλοποιεί τους μηχανισμούς αυτούς με διαφορετικό τρόπο καθώς η γλώσσα προγραμματισμού στην οποία είναι υλοποιημένοι, προσφέρει και διαφορετικές δυνατότητες. Όμως η διασφάλιση της διαδικασίας αξιολόγησης θα πρέπει να είναι ανεξάρτητη και να λειτουργήσει καθολικά ως μοντέλο αξιολόγησης των εκπαιδευόμενων.

Όπως ήδη αναφέρθηκε στο κεφάλαιο 3, το Moodle υλοποιεί τα απολύτως αναγκαία αντιμέτρα ασφάλειας με στόχο την εγκυρότητα της αξιολόγησης των εκπαιδευόμενων, ικανοποιώντας στο ελάχιστο τις απαιτήσεις ασφάλειας που ορίζονται από την τεχνική συνιστώσα του Σχεδίου. Θέλοντας να γενικεύσουμε την εφαρμογή του Σχεδίου Ασφάλειας σε όλα τα διαθέσιμα ΣΔΗΜ της αγοράς, είναι δύσκολο να βρούμε ένα σύστημα που να υλοποιεί όλα τα προτεινόμενα αντίμετρα ασφάλειας έτσι ώστε να είναι σύμφωνο με το Σχέδιο καθώς το προγραμματιστικό κόστος αυξάνει όσο περισσότεροι και πολυπλοκότεροι μηχανισμοί ασφάλειας ενσωματώνονται σε ένα ΣΔΗΜ.

Για την επίλυση τέτοιων προβλημάτων ανομοιογένειας σε θέματα ασφάλειας μεταξύ των ΣΔΗΜ και την εξάλειψη των απειλών ασφάλειας που δημιουργούνται κατά τη δραστηριότητα των χρηστών μέσα στο περιβάλλον η-μάθησης (και συγκεκριμένα κατά τη διαδικασία αξιολόγησης), προτείνεται η υιοθέτηση μιας **Αρχιτεκτονικής Ασφαλών η-Εξετάσεων μέσω ιστού σε περιβάλλοντα η-Μάθησης**. Οι πυλώνες προσέγγισης της Αρχιτεκτονικής αυτής είναι οι εξής:

- Η Αρχιτεκτονική θα πρέπει να περιλαμβάνει όλα τα αντίμετρα ασφάλειας με στόχο την απόλυτη εναρμόνιση του με το Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών που περιγράφηκε στο κεφάλαιο 4.
- Η Αρχιτεκτονική θα πρέπει να αποτελέσει ολιστική λύση στο πρόβλημα της ανομοιογένειας στη διαδικασία αξιολόγησης μέσα σε ένα περιβάλλον η-μάθησης. Η

ανεξαρτησία τεχνολογιών θα πρέπει να αποτελέσει κίνητρο στην υιοθέτηση της αρχιτεκτονικής από όλα τα ΣΔΗΜ.

5.1.2 Λειτουργικές Απαιτήσεις

Η καταγραφή των λειτουργικών απαιτήσεων αποτελεί απαραίτητη προϋπόθεση για την ανάπτυξη οποιουδήποτε πληροφοριακού συστήματος καθώς θέτει τις αρχικές προδιαγραφές λειτουργίας βάσει των οποίων θα υλοποιηθούν οι κατάλληλοι μηχανισμοί που θα τις ικανοποιούν.

Η διαδικασία αξιολόγησης αποτελεί από μόνη της λειτουργική απαίτηση ενός ΣΔΗΜ όταν αυτή ενσωματώνεται στον πυρήνα του πληροφοριακού συστήματος. Μεταβαίνοντας όμως σε μια ολιστική προσέγγιση της διαδικασίας αξιολόγησης θα πρέπει οι η-εξετάσεις να αποτελούν εξωτερική υπηρεσία με στόχο την ανεξαρτησία τους από το εκάστοτε ΣΔΗΜ, μέσω μιας προτυποποιημένης επικοινωνίας μεταξύ του ΣΔΗΜ και της υπηρεσίας. Συνεπώς δημιουργούνται καινούριες λειτουργικές απαιτήσεις οι οποίες ορίζονται με σαφήνεια παρακάτω:

1. **Δημιουργία ενότητας η-εξετάσεων ως εξωτερική υπηρεσία μέσα στη δομή μαθήματος μέσα στο περιβάλλον η-μάθησης.** Ο εκπαιδευτής θα πρέπει να έχει τη δυνατότητα να ενεργοποιήσει την υπηρεσία η-εξετάσεων (διαδικασία αξιολόγησης) και να την ενσωματώσει στη δομή του η-μαθήματος. Επιπλέον θα έχει τη δυνατότητα
    a. να ρυθμίσει το χρονικό διάστημα στο οποίο θα είναι ενεργοποιημένη η υπηρεσία
    b. να ορίσει αν η υπηρεσία θα είναι ορατή ή όχι.
2. **Προτυποποιημένη σύνδεση περιβάλλοντος η-μάθησης με περιβάλλον η-εξετάσεων.** Η επικοινωνία των δύο συστημάτων συνιστά απαίτηση διαλειτουργικότητας και καθιστά απαραίτητη τη σύνδεση των συστημάτων μέσα από το περιβάλλον η-μάθησης για την ομαλότερη και φιλικότερη στο χρήστη μετάβαση από το ένα σύστημα στο άλλο. Η επικοινωνία αυτή θα πρέπει να εγκαθιδρύεται μέσω ενός προτύπου διαλειτουργικότητας.
3. **Σύστημα η-εξετάσεων μέσω ιστού ως εξωτερική υπηρεσία.** Το σύστημα θα πρέπει να ικανοποιεί τις εξής λειτουργικές απαιτήσεις:
    a. *Είσοδος χρήστη στο περιβάλλον ασφαλών η-εξετάσεων με τα διαπιστευτήρια του περιβάλλοντος η-μάθησης.* Ο χρήστης θα συνδέεται στο περιβάλλον η-εξετάσεων με το ίδιο όνομα χρήστη και κωδικό πρόσβασης που χρησιμοποιεί στο περιβάλλον η-μάθησης. Από τη συγκεκριμένη απαίτηση προκύπτει η ανάγκη για προγραμματισμένο συγχρονισμό του μητρώου χρηστών μεταξύ των δύο συστημάτων.
    b. *Κατηγοριοποίηση χρηστών.* Οι κατηγορίες χρηστών ενός περιβάλλοντος η-μάθησης θα πρέπει να διατηρούνται και στο περιβάλλον η-μάθησης με διαφορετική διεπαφή χρήσης για κάθε κατηγορία. Οι κατηγορίες του εκπαιδευόμενου και του εκπαιδευτή αντιστοιχίζονται σε αυτές του εξεταζόμενου και του εξεταστή αντίστοιχα.
    c. *Ολοκληρωμένη υπηρεσία η-εξετάσεων.* Πρόκειται για τον πυρήνα της διαδικασίας αξιολόγησης η οποία θα πρέπει να ικανοποιεί τις παρακάτω απαιτήσεις ανά κατηγορία χρήστη:

Εξεταζόμενος

- *Προβολή μαθημάτων στα οποία είναι εγγεγραμμένος.*
- *Αίτηση εξέτασης σε κατ'επιλογήν μάθημα.*
- *Αρχειοθέτηση αιτήσεων εξέτασης ανά μάθημα.*
- *Εξέταση μαθήματος.*
- *Αρχείο βαθμολόγησης ανά μάθημα .*

Εξεταστής

- *Προβολή μαθημάτων στα οποία είναι εγγεγραμμένος .*
- *Προβολή αιτήσεων εξέτασης ανά μάθημα, με δυνατότητα έγκρισης ή απόρριψης.*
- *Αρχειοθέτηση αιτήσεων εξέτασης.*
- *Δημιουργία διαφορετικού η-εγγράφου εξέτασης ανά μαθητή/εγκεκριμένη αίτηση εξέτασης.*
- *Αρχειοθέτηση ενεργών αιτήσεων προς εξέταση.*
- *Βαθμολόγηση απαντημένων η-εγγράφων εξέτασης.*
- *Αρχειοθέτηση βαθμολογημένων η-εγγράφων εξέτασης .*

Διαχειριστής

- *Παρακολούθηση/Επίβλεψη διαδικασίας η-εξετάσεων.*
- *Προβολή ενεργών εξετάσεων ανά μάθημα.*
- *Δυνατότητα συγχρονισμού μητρώου χρηστών.*

4. **Δυνατότητα αλληλεπίδρασης του συστήματος η-εξετάσεων με το περιβάλλον η-μάθησης, μέσω του προτύπου επικοινωνίας/διαλειτουργικότητας**. Η συγκεκριμένη απαίτηση κρίνεται απαραίτητη για τη μεταφορά των βαθμολογιών από το σύστημα η-εξετάσεων στο ΣΔΗΜ και ενημέρωση των στοιχείων του εκπαιδευόμενου.

Ύστερα από την καταγραφή των λειτουργικών απαιτήσεων ακολουθεί η ανάλυση κινδύνων ασφάλειας στη διαδικασία αξιολόγησης βάσει των προδιαγραφών λειτουργίας που περιγράφηκαν παραπάνω.

5.1.3 Απειλές Ασφάλειας

Η δραστηριότητα των χρηστών και η κρισιμότητα των δεδομένων σε ένα περιβάλλον η-εξετάσεων, εκθέτει το σύστημα σε απειλές ασφάλειας οι οποιοι θα πρέπει να αντιμετωπιστούν με τους κατάλληλους μηχανισμούς έτσι ώστε η διαδικασία να διασφαλιστεί. Πριν την υλοποίηση των μηχανισμών ασφάλειας, θα πρέπει αρχικά να καταγράψουμε και να αναλύσουμε τις απειλές ασφάλειας που μπορεί να δεχτεί η διαδικασία αξιολόγησης.

1. **Απειλές ασφάλειας στις υποδομές και στην επικοινωνία μεταξύ των συστημάτων**

a. Η αμφίδρομη επικοινωνία μεταξύ του ΣΔΗΜ και του συστήματος η-εξετάσεων αποτελεί πρόκληση καθώς μεταφέρονται ευαίσθητα δεδομένα όπως διαπιστευτήρια χρήστη και βαθμολογίες. Συνεπώς η μη-ασφαλής και μη-προτυποποιημένη επικοινωνία μπορεί να

αποτελέσει ευπάθεια του συστήματος και να οδηγήσει σε κίνδυνο ασφάλειας (υποκλοπή, τροποποίηση, πλαστογράφηση).

b. Ενδεχόμενη διακοπή της υπηρεσίας η-εξετάσεων μπορεί να οδηγήσει σε άγνωστη και αβέβαιη κατάσταση συστήματος και θα επηρεάσει με αρνητικό τρόπο την αξιοπιστία της διαδικασίας.

2. Απειλές ασφάλειας για τον εκπαιδευτή

a. Αλλοίωση η-εξετάσεων: πρόσβαση στα θέματα πριν από την έναρξη των εξετάσεων, τροποποίηση ερωτήσεων εξέτασης, διαγραφή της ενεργής η-εξέτασης, συμμετοχή σε εξετάσεις από μη εξουσιοδοτημένο άτομο ή κακόβουλο εκπαιδευόμενο.

b. Προβολή, τροποποίηση και διαγραφή απαντήσεων η-εξετάσεων και εργασιών από μη εξουσιοδοτημένο χρήστη

c. Τροποποίηση βαθμολόγησης εργασιών και η-εξετάσεων

3. Απειλές ασφάλειας για τον εκπαιδευόμενο

a. Αλλοίωση η-εξετάσεων: Χρήση προσωπικών στοιχείων ταυτοποίησης και αυθεντικοποίησης για να συμμετέχει εκ μέρους του εκπαιδευόμενου ένα μη εξουσιοδοτημένο άτομο σε η-εξετάσεις.

b. Πρόσβαση σε εργασίες του εκπαιδευόμενου με στόχο την τροποποίηση, διαγραφή και υποκλοπή τους.

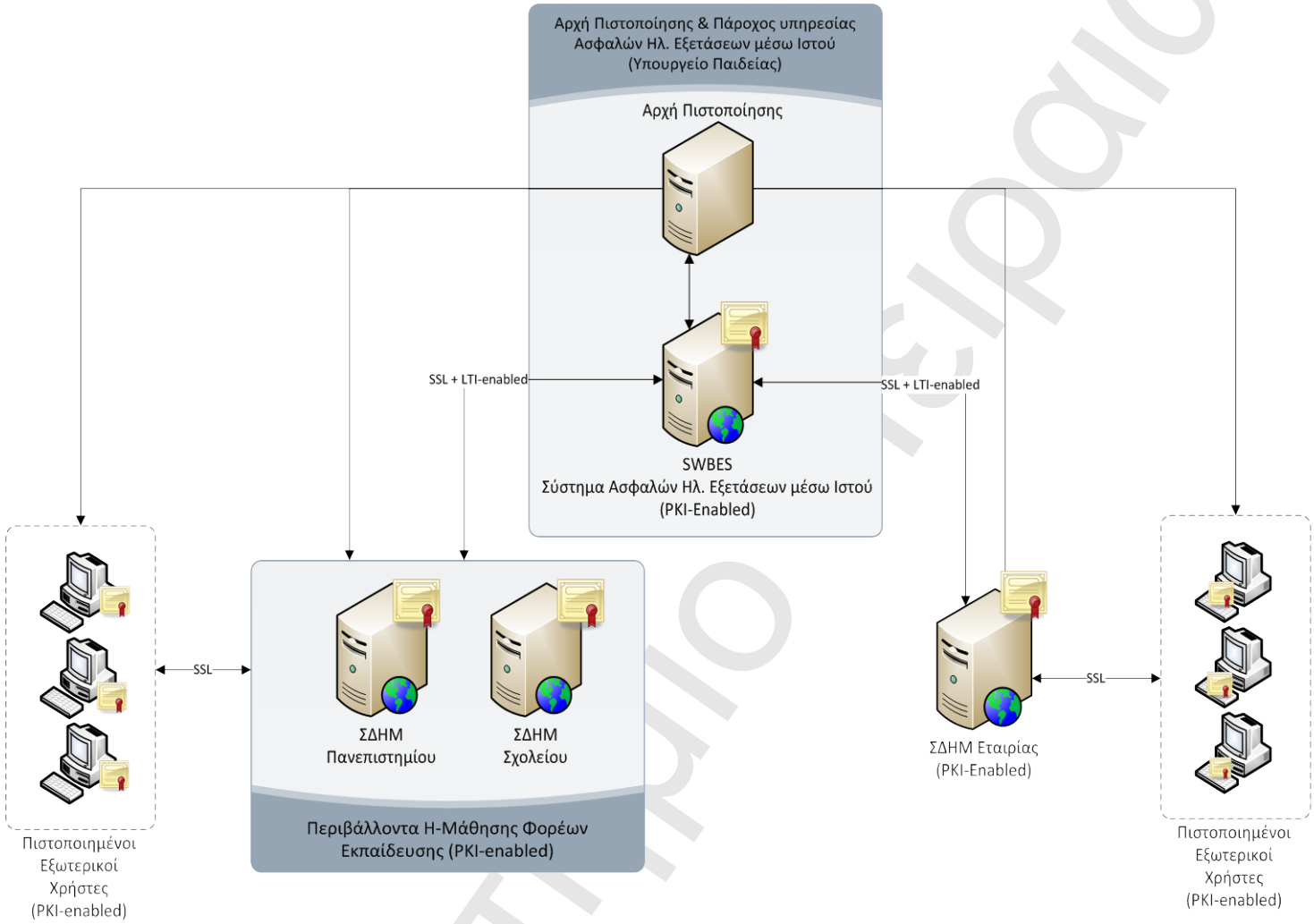
c. Πρόσβαση σε βαθμολογίες του εκπαιδευόμενου με στόχο την τροποποίηση κα διαγραφή τους.

Λαμβάνοντας υπόψη τις λειτουργικές απαιτήσεις της διαδικασίας αξιολόγησης αλλά και τους δυνητικούς κινδύνους ασφάλειας που θα πρέπει να αντιμετωπιστούν με τους κατάλληλους μηχανισμούς, ακολουθεί η περιγραφή της προτεινόμενης Αρχιτεκτονικής Ασφαλών η-Εξετάσεων μέσω ιστού.

5.1.4 Προτεινόμενη Αρχιτεκτονική

Η προτεινόμενη Αρχιτεκτονική Ασφαλών η-Εξετάσεων έχει ως στόχο την ολιστική αντιμετώπιση της διαδικασίας αξιολόγησης εκπαιδευομένων ενός ΣΔΗΜ λαμβάνοντας υπόψη τόσο τις λειτουργικές απαιτήσεις όσο και τις απειλέςασφάλειας μιας τέτοιας διαδικασίας.

Αρχιτεκτονική Ασφαλών η-Εξετάσεων μέσω Ιστού σε Περιβάλλοντα η-Μάθησης



Σχήμα 9. Αρχιτεκτονική Ασφαλών η-Εξετάσεων μέσω Ιστού

Στο Σχήμα 9 φαίνεται η προτεινόμενη Αρχιτεκτονική Ασφαλών η-Εξετάσεων το οποίο βασίζεται στην Υποδομή Δημόσιου Κλειδιού ως ομπρέλα ασφάλειας και αποτελείται από τις παρακάτω οντότητες

- **Αρχή Πιστοποίησης & Πάροχος Υπηρεσίας Ασφαλών η-Εξετάσεων μέσω Ιστού**

  Αποτελούν μια ενιαία οντότητα αναλαμβάνοντας το ρόλο της έκδοσης πιστοποιητικών και της υπηρεσίας η-εξετάσεων. Με κριτήρια επιλογής τη μεγαλύτερη αξιοπιστία στη διαδικασία αξιολόγησης και τη σχετικότητα με το φυσικό αντικείμενο της προτεινόμενης Αρχιτεκτονικής, το ρόλο αυτό αναλαμβάνει μια δημόσια αρχή του κράτους όπως το Υπουργείο Παιδείας. Οι αρμοδιότητες του είναι οι εξής:

  - Υπηρεσίες Υποδομής Δημόσιου Κλειδιού: Έγγραφή, Πιστοποίηση, Κατάλογος, Χρονοσφράγιση.

Το υπουργείο αναλαμβάνει την έκδοση πιστοποιητικών προς τα εμπλεκόμενα μέρη της διαδικασίας αξιολόγησης όπως επίσης τον έλεγχο της εγκυρότητάς τους.

- Σύστημα Ασφαλών η-Εξετάσεων μέσω ιστού – Secure Web-based Exam System (SWBES)

  Πρόκειται για τον πυρήνα της διαδικασίας αξιολόγησης αφού υλοποιεί το σύνολο των μηχανισμών η-Εξετάσεων και των μηχανισμών ασφάλειας για κάθε ΣΔΗΜ που συνδέεται σε αυτό. Κάθε ΣΔΗΜ δημιουργεί ένα δικό του αντίγραφο του SWBES στον εξυπηρετητή. Το Υπουργείο Παιδείας είναι υπεύθυνο για τη συντήρηση και αδιάλειπτη λειτουργία του SWBES.

- **Πιστοποιημένα Συστήματα Διαχείρισης η-Μάθησης φορέων εκπαίδευσης και εταιριών**

  Τα ΣΔΗΜ που θέλουν να χρησιμοποιήσουν την υπηρεσία η-εξετάσεων θα πρέπει να πιστοποιηθούν από το Υπουργείο Παιδείας και στη συνέχεια χρησιμοποιώντας το πρότυπο διαλειτουργικότητας μαθησιακών εργαλείων (LTI – Learning Tool Interoperability), συνδέονται με το SWBES.

- **Πιστοποιημένοι Χρήστες ΣΔΗΜ**

  Οι χρήστες που συνδέονται με το SWBES μέσω ενός ΣΔΗΜ θα πρέπει να είναι πιστοποιημένοι για την ασφαλή χρήση της υπηρεσίας. Η έκδοση των πιστοποιητικών τους γίνεται κατά την είσοδο τους στο SWBES.

Η επικοινωνία όλων εμπλεκομένων μερών της Αρχιτεκτονικής διέπεται από το πρωτόκολλο ασφάλειας επικοινωνίας SSL (Secure Socket Layer) για την κρυπτογράφηση των μηνυμάτων κατά τη μεταφορά τους.

5.1.5 SWBES - Σύστημα Ασφαλών η-Εξετάσεων μέσω ιστού

Το SWBES σύμφωνα με την προτεινόμενη Αρχιτεκτονική, αποτελεί τον πυρήνα της διαδικασίας αξιολόγησης. Όπως αναφέρθηκε, κάθε ΣΔΗΜ που συνδέεται στον εξυπηρετητή του SWBES, δημιουργεί ένα δικό του αντίγραφο της εφαρμογής, χρησιμοποιώντας τους πόρους του αντιγράφου κατ'αποκλειστικότητα.

Για τις ανάγκες του κεφαλαίου υλοποιήθηκε ένα αντίγραφο του SWBES για το Moodle λαμβάνοντας υπόψη όλες τις λειτουργικές απαιτήσεις και απαιτήσεις ασφάλειας που αναφέρθηκαν στις ενότητες 4.2.2 και 4.2.3 . Στην ενότητα αυτή θα γίνει αναλυτική περιγραφή του Συστήματος η-Εξετάσεων μέσω ιστού παρουσιάζοντας μέσω διαγραμμάτων UML όλες τις φάσεις της διαδικασίας αξιολόγησης. Αρχικά θα αναφερθούν οι τεχνολογίες που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής.

Τεχνολογίες

Πριν περάσουμε στην περιγραφή της υλοποίησης, θα πρέπει να καταγράψουμε τις τεχνολογίες που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής. Πιο συγκεκριμένα:

- Η εφαρμογή ασφαλών η-εξετάσεων μέσω ιστού αναπτύχθηκε εξ'ολοκλήρου σε γλώσσα προγραμματισμού **PHP (Hypertext Preprocessor)** υλοποιώντας τους βασικούς μηχανισμούς ασφάλειας με τις συναρτήσεις του **OpenSSL**[17] (υλοποιημένες σε PHP) για τη δημιουργία και επαλήθευση ψηφιακών υπογραφών όπως επίσης την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων.
- Η εφαρμογή χρησιμοποιεί τη γλώσσα **XML (Extensible Markup Language)** για τη δημιουργία και αποθήκευση των η-εγγράφων εξετάσεων θέλοντας να αξιοποιήσει τις δυνατότητες που παρέχει η δομή ενός XML εγγράφου.
- Για την αποθήκευση ευαίσθητων πληροφοριών στη Βάση Δεδομένων χρησιμοποιούνται **συναρτήσεις κατακερματισμού** υλοποιημένες σε PHP. Για παράδειγμα ο αλγόριθμος **MD5 (Message Digest Algorithm)** χρησιμοποιείται κατά την αποθήκευση του κωδικού πρόσβασης ενός χρήστη.
- Για την κρυπτογράφηση του καναλιού επικοινωνίας χρησιμοποιήθηκε το πρωτόκολλο ασφάλειας **SSL (Secure Socket Layer)** προκειμένου να διασφαλίσουμε την μεταφορά των δεδομένων μεταξύ πελάτη και εξυπηρετητή. Κατά τη λειτουργία μιας τέτοιου είδους εφαρμογής, δημιουργούνται αμφίδρομες επικοινωνίες, τα μηνύματα των οποίων είναι απαραίτητο να κρυπτογραφηθούν. Συνεπώς, το πρωτόκολλο SSL χρησιμοποιήθηκε για τη δημιουργία ενός ιδιωτικού καναλιού μεταξύ των εμπλεκομένων μερών. Οι ελάχιστη απαίτηση για την εδραίωση ενός τέτοιου πρωτοκόλλου είναι η απόκτηση ενός πιστοποιητικού από την πλευρά του εξυπηρετητή, το οποίο θα έχει ως στόχο την αυθεντικοποίηση του στον πελάτη. Όμως στην περίπτωση των ασφαλών η-εξετάσεων θα πρέπει να αυθεντικοποιούνται όλα τα εμπλεκόμενα μέρη (Εξεταστής, Εξεταζόμενος, ΣΔΗΜ, SWBES) μέσω έγκυρων πιστοποιητικών ασφάλειας.
- Η βάση δεδομένων στην οποία αποθηκεύονται προσωπικά στοιχεία χρηστών και λειτουργικά δεδομένα της εφαρμογής έχει υλοποιηθεί σε **MySQL** (Σύστημα Διαχείρισης Σχεσιακών βάσεων Δεδομένων ανοιχτού κώδικα) χρησιμοποιώντας αλγορίθμους κρυπτογράφησης για τα ερωτήματα προς τη ΒΔ.
- Για την εξυπηρέτηση των http αιτήσεων και την εδραίωση του πρωτοκόλλου SSL χρησιμοποιήθηκε σταθερή έκδοση του δημοφιλέστερου εξυπηρετητή ιστού της **Apache**.
- **Moodle**. Όπως αναφέρθηκε και στο κεφάλαιο 2, αποτελεί ίσως το πιο δημοφιλές σύστημα διαχείρισης η-μάθησης ανοιχτού κώδικα το οποίο είναι υλοποιημένο σε γλώσσα προγραμματισμού PHP. Χρησιμοποιήθηκε για τους σκοπούς του SWBES με στόχο την αναβάθμιση του στον τομέα της ασφάλειας σχετικά με τις η-εξετάσεις.

[17] Το OpenSSL αποτελεί την πιο διαδεδομένη ανοιχτού κώδικα εργαλειοθήκη που υλοποιεί τα πρωτόκολλα ασφάλειας SSL (Secure Socket Layer) και TLS (Transport Layer Security) όπως επίσης προσφέρει την πιο δυνατή γενικού τύπου κρυπτογραφική βιβλιοθήκη.

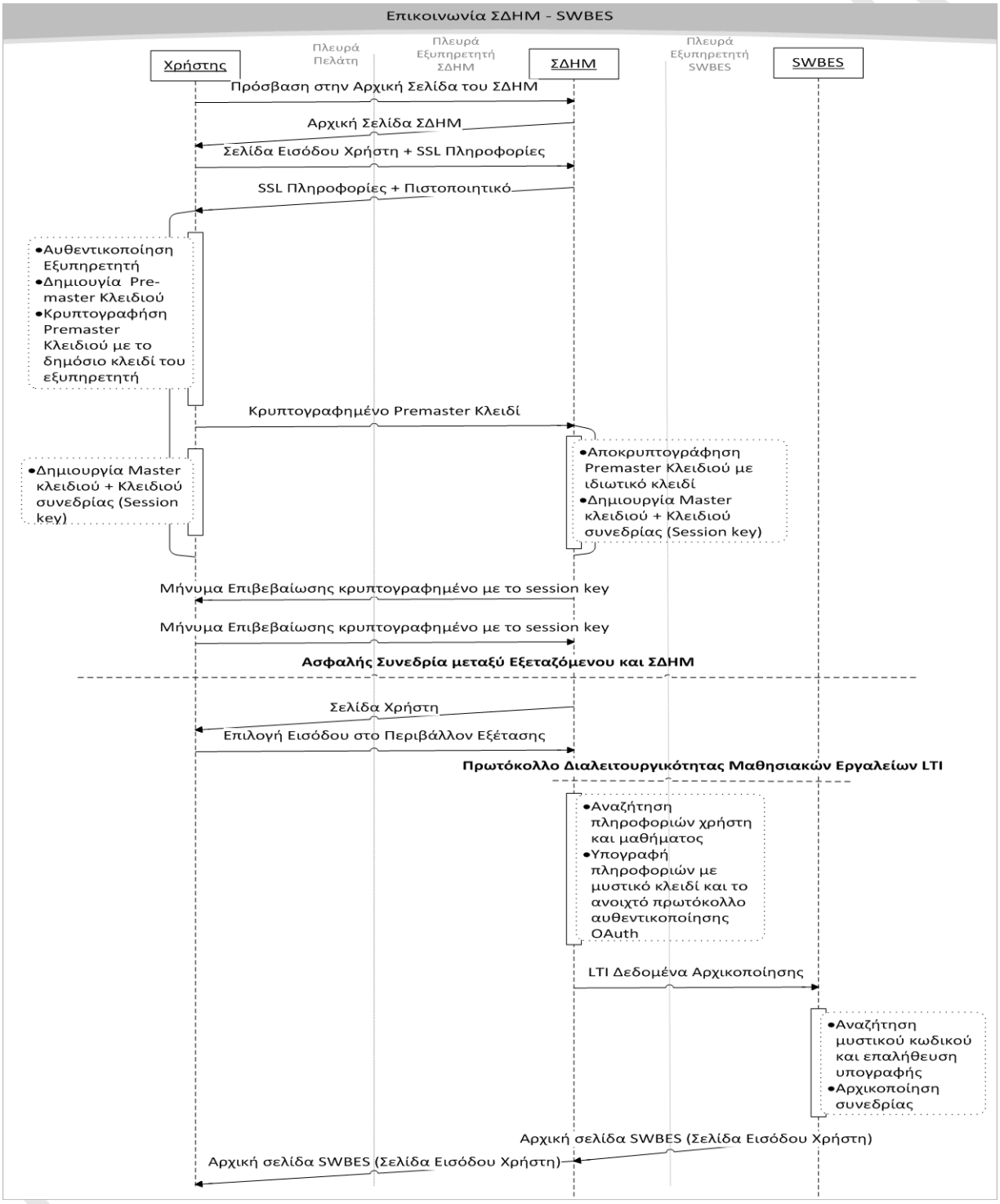
- Βασική πρόκληση της υλοποίησης αποτελεί η διαλειτουργικότητα μιας εφαρμογής η-εξετάσεων με το Moodle. Όπως αναφέρθηκε, το SWBES μπορεί να χρησιμοποιηθεί ως ενσωματωμένη υπηρεσία σε ένα ΣΔΗΜ με στόχο την αποτελεσματικότερη αλληλεπίδραση τους. Για να μπορέσει το SWBES να επικοινωνήσει με το Moodle, χρησιμοποιήσαμε το **πρότυπο διαλειτουργικότητας εκπαιδευτικών εργαλείων LTI (Learning Tools Interoperability standard)** του οργανισμού IMS Global Consortium. Πρόκειται για ένα πρότυπο συμβατότητας στην επικοινωνία και διαλειτουργικότητα μεταξύ εκπαιδευτικών εργαλείων και ΣΔΗΜ. Πρόκειται για ένα πρότυπο το οποίο προσδίδει τα παρακάτω λειτουργικά χαρακτηριστικά σε ένα ΣΔΗΜ:
  - Άμεση ενσωμάτωση μεγάλης ποικιλίας εκπαιδευτικών εργαλείων, εφαρμογών και περιεχομένου μέσα σε ένα ΣΔΗΜ
  - Οι χρήστες ενός ΣΔΗΜ έχουν τη δυνατότητα να έχουν πρόσβαση στο εκπαιδευτικό εργαλείο μέσα από το περιβάλλον η-μάθησης (single sign-on)
  - Ανταλλαγή δεδομένων μεταξύ του εκπαιδευτικού εργαλείου και του ΣΔΗΜ με στόχο τη χρήση τους από τις ενδογενείς υπηρεσίες του ΣΔΗΜ (π.χ. τη βαθμολογία των εξεταζόμενων)
  - Κάθε εφαρμογή έχει την ίδια διεπαφή με το ΣΔΗΜ, μειώνοντας το προγραμματιστικό κόστος που απαιτείται για κάποιο εργαλείο να προσαρμοστεί στην τεχνολογία του κάθε ΣΔΗΜ.
  - Ένα ΣΔΗΜ έχει τη δυνατότητα να προσφέρει υπηρεσίες και εργαλεία προς τη κοινότητα του χωρίς περιορισμούς.

Παρουσίαση SWBES

Στο σενάριο χρήσης που θα περιγραφεί παρακάτω μέσω διαγραμμάτων, οι χρήστες ενός ΣΔΗΜ όπως το Moodle έχουν τη δυνατότητα να χρησιμοποιήσουν την υπηρεσία ασφαλών η-εξετάσεων ως εξωτερικό εργαλείο αξιολόγησης. Πιο συγκεκριμένα, ένας χρήστης με ρόλο εκπαιδευτή στο Moodle έχει τη δυνατότητα να ενεργοποίησει για συγκεκριμένο χρονικό διάστημα την υπηρεσία η-εξετάσεων για τις ανάγκες αξιολόγησης των εκπαιδευόμενων ενός μαθήματος (λειτουργική απαίτηση 1). Ταυτόχρονα, κάνει ορατή την ενότητα των εξετάσεων στους εκπαιδευόμενους (λειτουργική απαίτηση 1). Μέσα στο ενεργό χρονικό διάστημα, οι εκπαιδευόμενοι, αφού συνδεθούν στο SWBES μέσα από το Moodle, έχουν τη δυνατότητα να κάνουν αίτηση εξέτασης μαθήματος, να εξεταστούν στο μάθημα και να βαθμολογηθούν (λειτουργική απαίτηση 3). Αντίστοιχα οι εκπαιδευτές έχουν τη δυνατότητα να εγκρίνουν ή να απορρίψουν μια αίτηση, να δημιουργήσουν ένα η-έγγραφο εξετάσεων και να βαθμολογήσουν τους εξεταζόμενους (λειτουργική απαίτηση 3). Για την ολοκληρωμένη κατανόηση της διαδικασίας εξέτασης, θα παρουσιαστεί σχηματικά η ροή της πληροφορίας στις διακριτές φάσεις που την ορίζουν.

Φάση Α': Επικοινωνία ΣΔΗΜ-SWBES

Αρχικά, στο παρακάτω UML διάγραμμα ακολουθίας, εμφανίζεται αναλυτικά η επικοινωνία μεταξύ ΣΔΗΜ (Moodle) και SWBES κατά τη σύνδεση ενός χρήστη (εκπαιδευτή ή εκπαιδευόμενου) στο περιβάλλον εξέτασης μέσω του Moodle.



Σχήμα 10. Επικοινωνία μεταξύ ΣΔΗΜ και SWBES

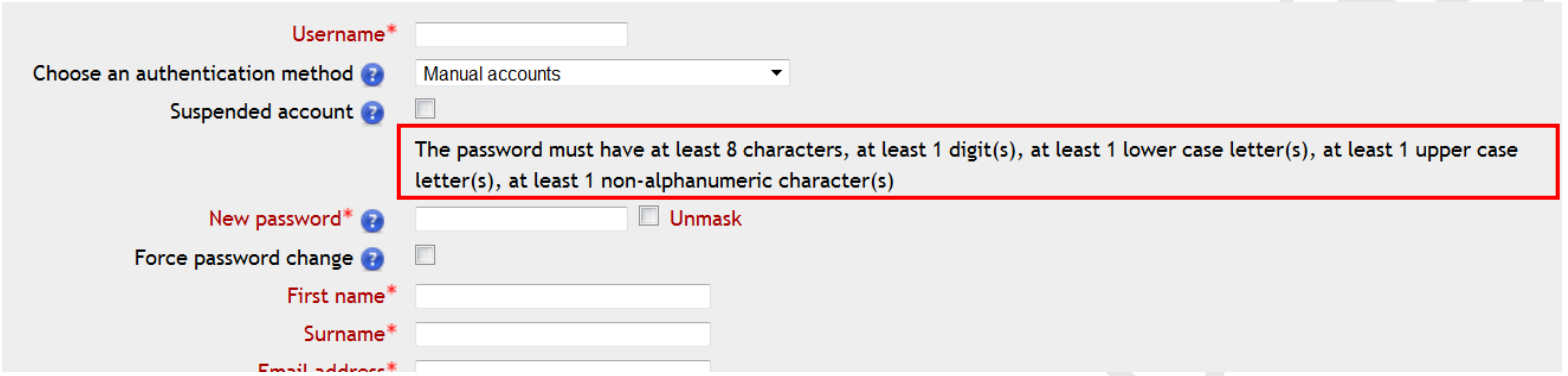
Βασικά στοιχεία της εδραίωσης επικοινωνίας μεταξύ του ΣΔΗΜ και του SWBES σύμφωνα με το Σχήμα 10 είναι τα παρακάτω:

- Η επικοινωνία μεταξύ ΣΔΗΜ και χρήστη (φυλλομετρητής χρήστη) είναι κρυπτογραφημένη σύμφωνα με το πρωτόκολλο ασφάλειας SSL. Το πρωτόκολλο SSL ενεργοποιείται στη σελίδα εισόδου χρήστη όπου ο χρήστης λαμβάνει το πιστοποιητικό του ΣΔΗΜ. Σύμφωνα με την προτεινόμενη Αρχιτεκτονική ασφαλών εξετάσεων, το πιστοποιητικό εκδίδεται από το αρχή πιστοποίησης (Υπουργείο Παιδείας). Συνεπώς, το πιστοποιητικό που αποστέλλεται στο χρήστη, ελέγχεται από την υπεύθυνη αρχή για την εγκυρότητα του.

Η διαδικασία εδραίωσης SSL επικοινωνίας έχει ως εξής:

1. Αποστέλλεται το πιστοποιητικό στο χρήστη (φυλλομετρητή), αυθεντικοποιείται το ΣΔΗΜ, δημιουργείται ένα προσωρινό κλειδί, κρυπτογραφείται με το δημόσιο κλειδί του ΣΔΗΜ και αποστέλλεται στο ΣΔΗΜ όπου αποκρυπτογραφείται με το ιδιωτικό κλειδί του ΣΔΗΜ.
2. Το ΣΔΗΜ και ο χρήστης (φυλλομετρητής) δημιουργούν το Master κλειδί επικοινωνίας και αποστέλλουν μήνυμα επιβεβαίωσης κρυπτογραφημένο με το κλειδί συνεδρίας μεταξύ τους.
3. Εδραίωση SSL επικοινωνίας. Κάθε μήνυμα αποστέλλεται κρυπτογραφημένο, ασφαλίζοντας το κανάλι επικοινωνίας. Το πρωτόκολλο συνεχίζει να υφίσταται και μετά την είσοδο του χρήστη για όσο χρονικό διάστημα διαρκέσει η συνεδρία.

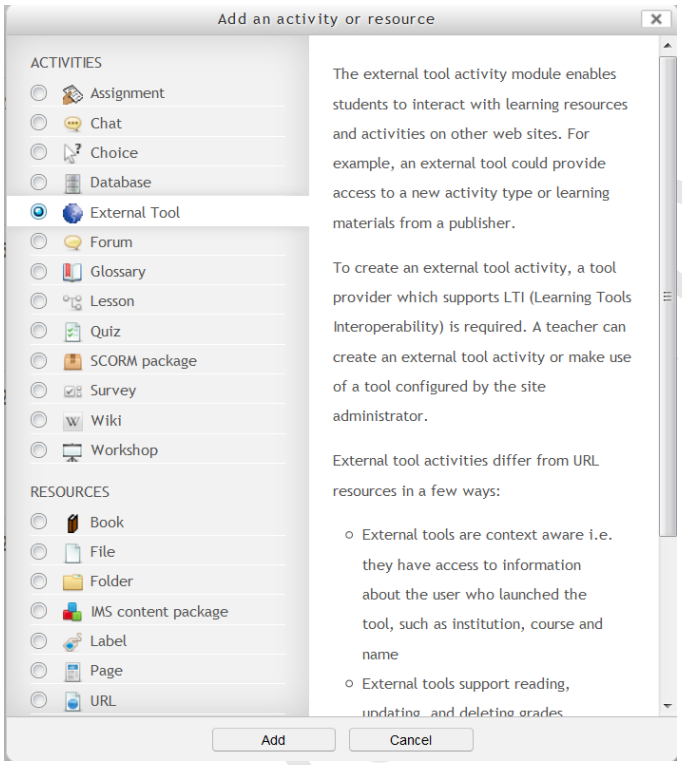
- Κατά την υποβολή των στοιχείων χρήστη, username και password, τα στοιχεία κατακερματίζονται με αλγόριθμο md5 σε συνδυασμό με ένα αλφαριθμητικό salt. Το ίδιο ισχύει και κατά την εγγραφή ενός χρήστη στο Moodle. Ο κατακερματισμός με salt του κωδικού πρόσβασης μειώνει το ενδεχόμενο υποκλοπής στοιχείων πρόσβασης. Επίσης η πολιτική κωδικού πρόσβασης κατά την εγγραφή ενός χρήστη είναι η χρήση κωδικού που αποτελείται από τουλάχιστον 8 χαρακτήρες, ειδικούς χαρακτήρες, αριθμούς , κεφαλαία και μικρά γράμματα. Αυτό μειώνει το ενδεχόμενο πρόβλεψης το κωδικού πρόσβασης από κάποιο κακόβουλο λογισμικό.
- Η επικοινωνία μεταξύ του ΣΔΗΜ και του SWBES εκτός από το πρωτόκολλο SSL, βασίζεται στο πρωτόκολλο διαλειτουργικότητας μαθησιακών εργαλείων LTI (λειτουργική απαίτηση 2,4). Αφού ο χρήστης επιλέξει την είσοδο του στο περιβάλλον εξέτασης του SWBES, καλείται ο μηχανισμός του LTI για την εδραίωση της επικοινωνίας μεταξύ του Moodle και μαθησιακού εργαλείου, δηλ. του SWBES. Κατά την εδραίωση αυτή, το ΣΔΗΜ αναζητά πληροφορίες χρήστη και μαθήματος τις οποίες υπογράφει με ένα μυστικό κλειδί μέσω του ανοιχτού πρωτοκόλλου αυθεντικοποίησης OAuth. Στη συνέχεια το υπογεγραμμένο ψηφιακά μήνυμα αποστέλλεται στο SWBES όπου επαληθεύεται η υπογραφή. Αν η υπογραφή είναι έγκυρη, αρχικοποιείται η συνεδρία και αποστέλλεται στο ΣΔΗΜ η αρχική σελίδα του SWBES.



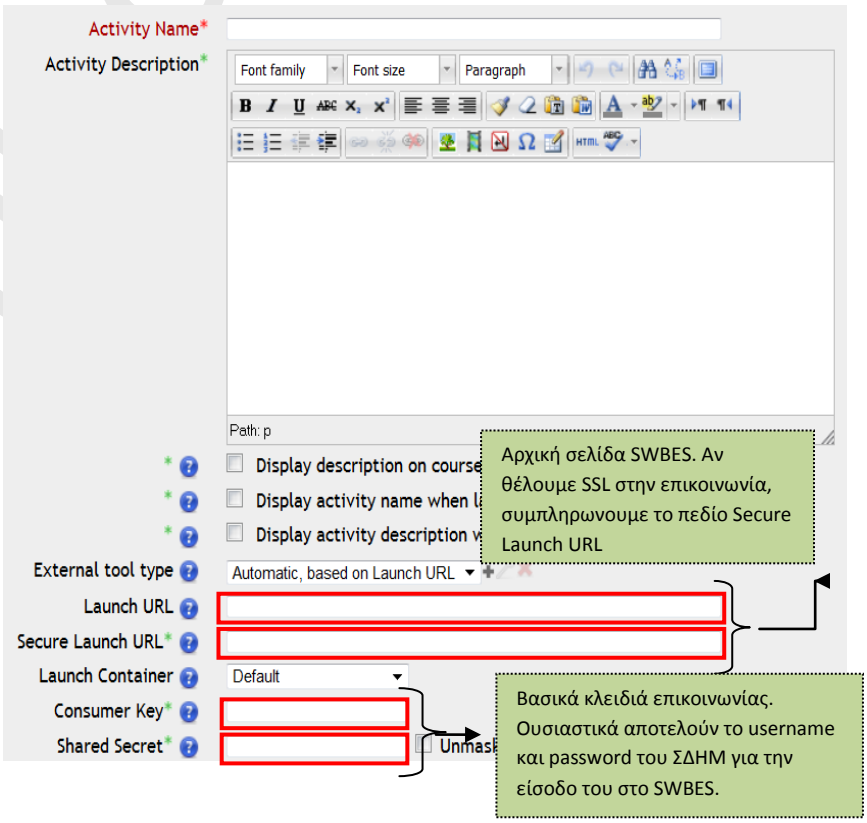
Εικόνα 1. Στιγμιότυπο κατά την εγγραφή χρήστη.

Στην Εικόνα 1 βλέπουμε στιγμιότυπο από την εγγραφή ενός χρήστη στο Moodle. Η πολιτική κωδικού πρόσβασης αναφέρεται ρητά όπως φαίνεται επισημασμένο κείμενο.

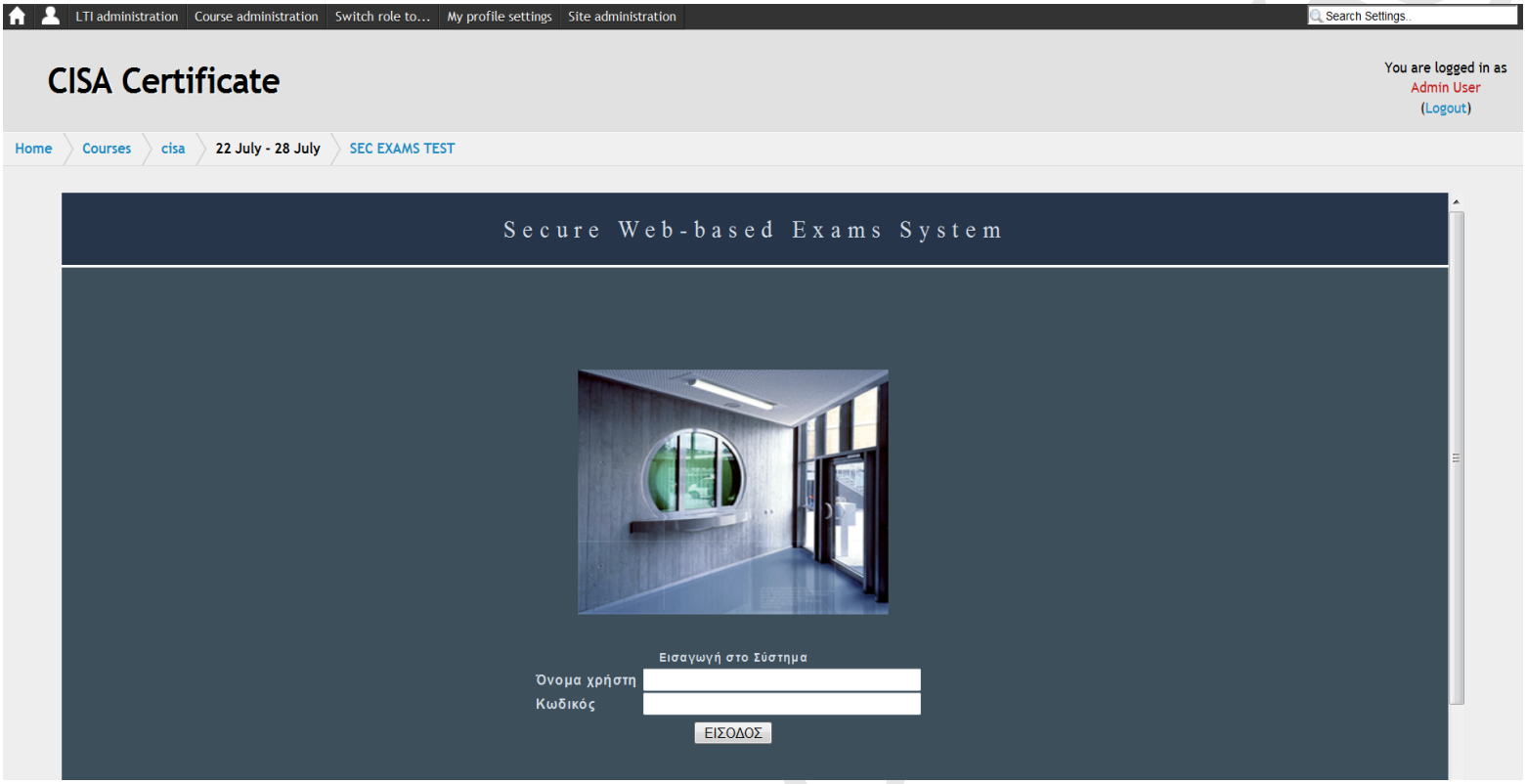
Στην **Εικόνα 2** και **Εικόνα 3** βλέπουμε τις οθόνες κατά την προσθήκη ενός εξωτερικού μαθησιακού εργαλείου ως ενότητα του μαθήματος. Συγκεκριμένα στην **Εικόνα 3** φαίνονται τα πεδία που πρέπει να συμπληρωθούν για την αρχικοποίηση του εξωτερικού μαθησιακού εργαλείου όπως το SWBES.



Εικόνα 2. Προσθήκη εξωτερικού εργαλείου ως ενότητα του μαθήματος



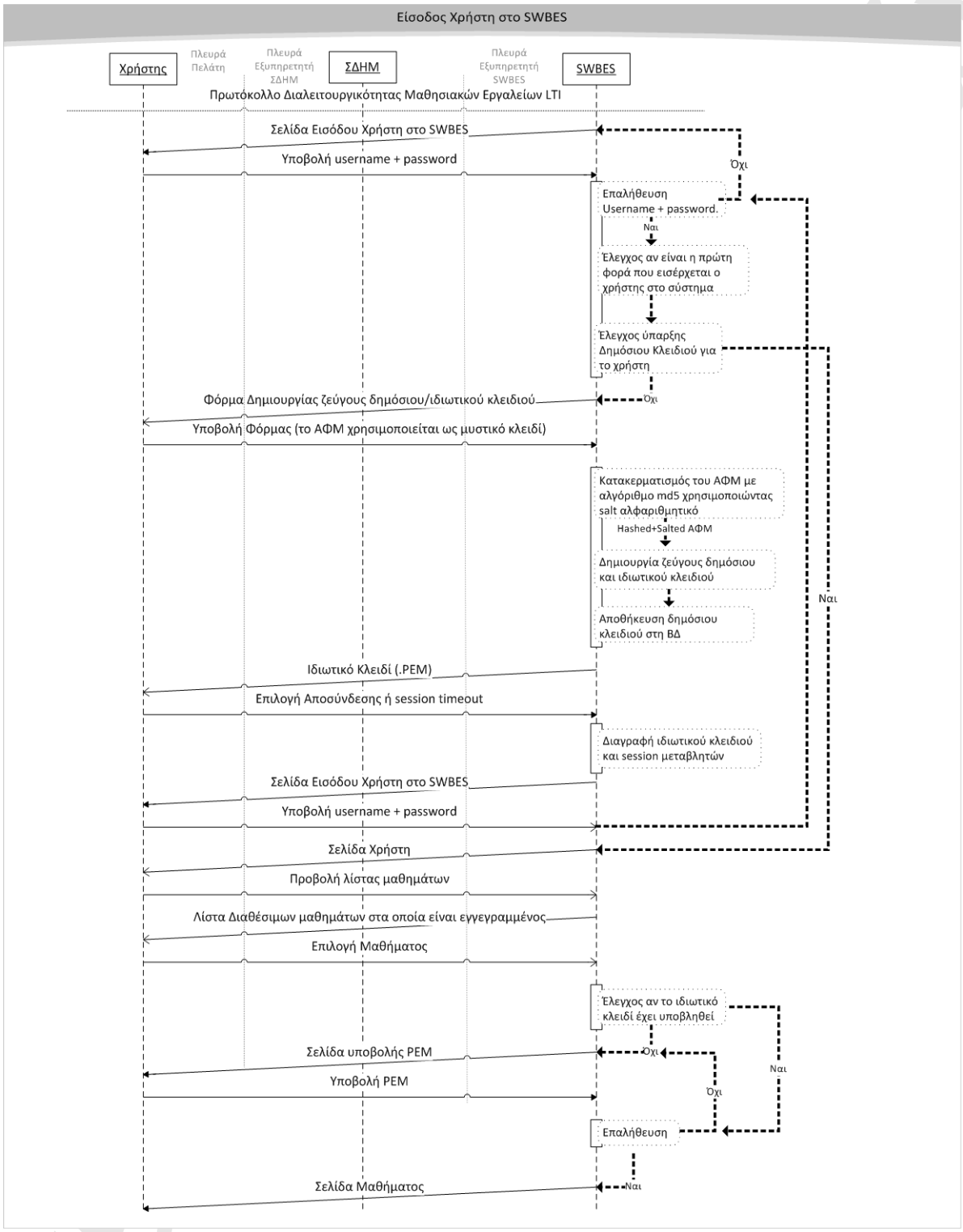
Εικόνα 3. Ρυθμίσεις εξωτερικού μαθησιακού εργαλείου



Εικόνα 4. Αρχική σελίδα SWBES μέσα από το περιβάλλον του Moodle

Φάση Β': Είσοδος Χρήστη στο SWBES

Κατά την είσοδο στο SWBES, ο χρήστης εισάγει εκ νέου το username και password που χρησιμοποιεί για το Moodle. Για την πλήρη αντιστοιχία των απαραίτητων πληροφοριών μεταξύ Moodle και SWBES, έχει δημιουργηθεί ένας μηχανισμός συγχρονισμού δεδομένων μεταξύ των ΒΔ των δύο συστημάτων, ο οποίος εκτελείται χρονοπρογραμματισμένα για την αδιάλειπτη ενημέρωση των συσχετισμένων πινάκων του SWBES. Οι πληροφορίες που ανταλάσσονται είναι σχετικά με τους χρήστες και τα μαθήματα στα οποία είναι εγγεγραμμένα ο καθένας ως εκπαιδευόμενος ή ως εκπαιδευτής. Οι ευαίσθητες πληροφορίες αποθηκεύονται κατακερματισμένες και τα ερωτήματα προς τη βάση του Moodle είναι κωδικοποιημένα με base64. Στο Σχήμα 11 φαίνεται η ροή πληροφορίας κατά την είσοδο του χρήστη στο SWBES. Αρχικά ο χρήστης εισάγει τα διαπιστευτήρια του και τα αποστέλλει στο SWBES. Αφού επαληθευτεί η ύπαρξη του username και password, το σύστημα ελέγχει αν έχει δημιουργηθεί δημόσιο κλειδί για το χρήστη. Η δημουργία ζεύγους δημόσιου/ιδιωτικού είναι απαραίτητη για κάθε χρήστη που εισέρχεται στο SWBES καθώς για την ανταλλαγή μηνυμάτων μεταξύ εξεταζόμενου και εξεταστή χρησιμοποιείται κρυπτογραφία δημόσιου κλειδιού. Αν ο χρήστης δεν έχει καταχωρημένο δημόσιο κλειδί, οδηγείται σε σελίδα συμπλήρωσης φόρμας για τη δημιουργία ζεύγους δημόσιου/ιδιωτικού κλειδιού.

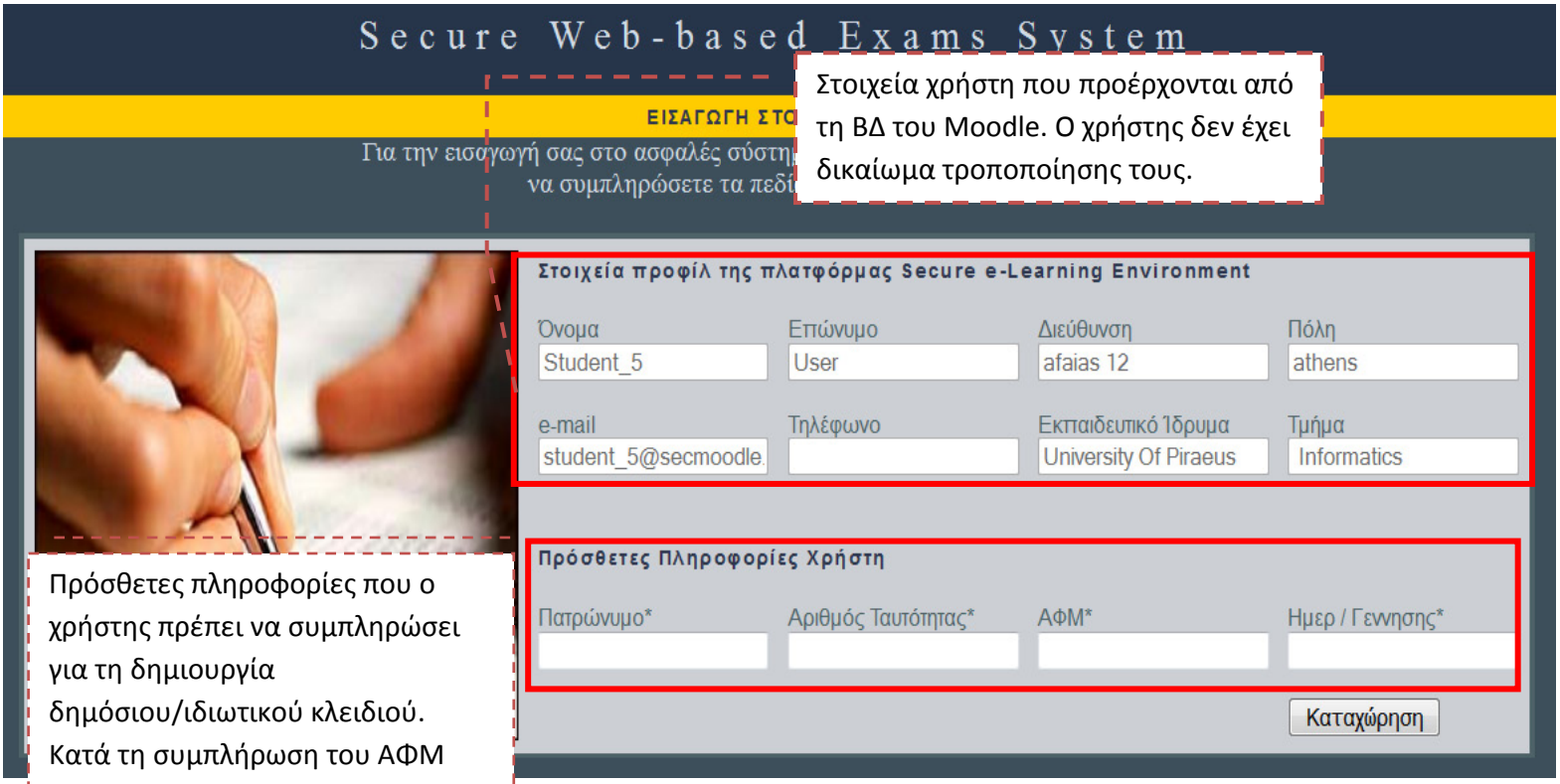


Σχήμα 11. Είσοδος χρήστη στο SWBES

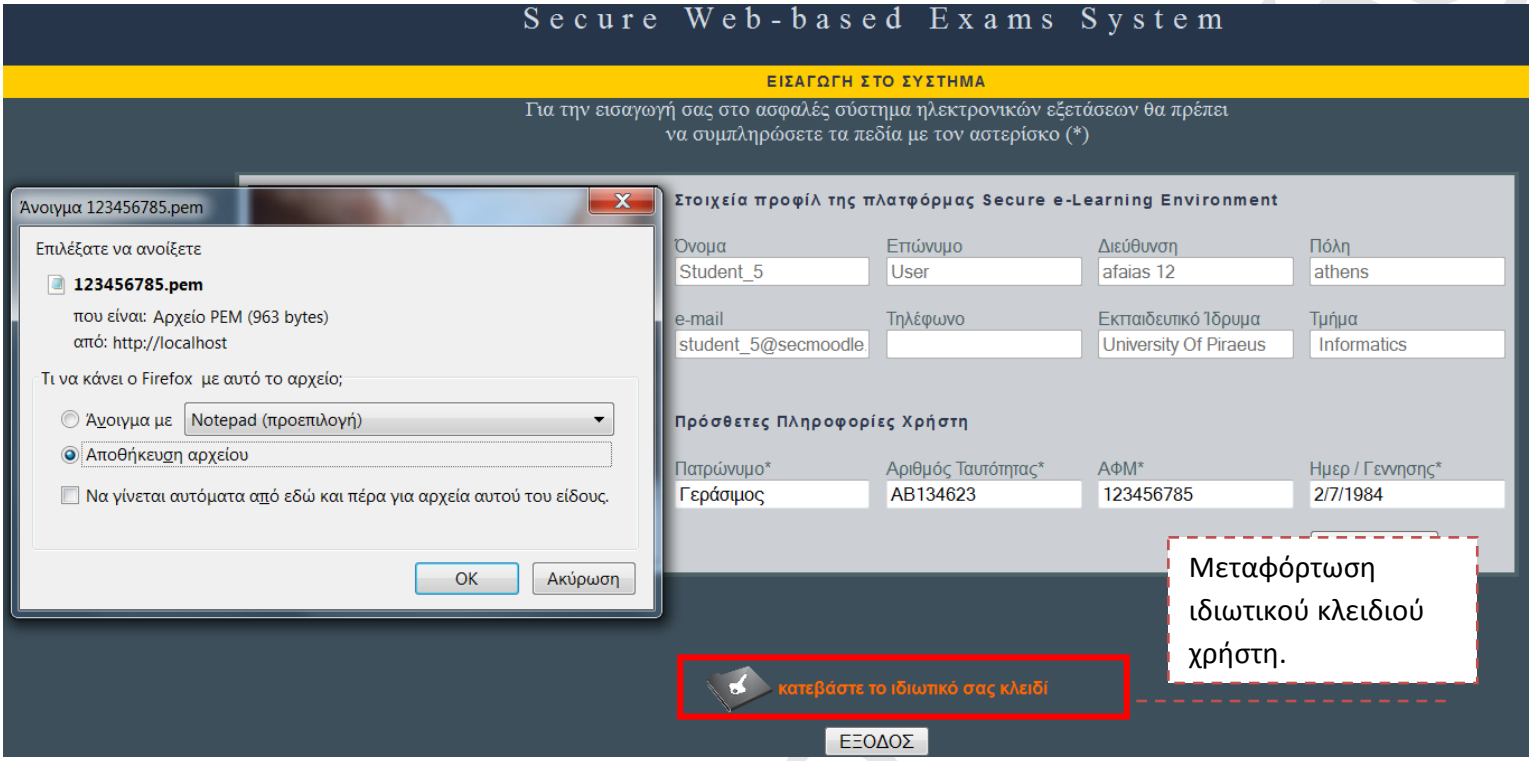
Συνοψίζοντας τα βασικά σημεία του παραπάνω σχήματος:

- Επαλήθευση διαπιστευτηρίων χρήστη (username,password). Έλεγχος ύπαρξης δημόσιου κλειδιού κατά την είσοδο του χρήστη.

- Αν ο χρήστης εισέρχεται για πρώτη φορά, οδηγείται σε φόρμα συμπλήρωσης βασικών στοιχείων. Το κατακερματισμένο ΑΦΜ (md5 και salt) αποτελεί τον κωδικό δημιουργίας του ζεύγους δημόσιου/ιδιωτικού κλειδιού. Το ΑΦΜ έχει τις ιδιότητες της μοναδικότητας και μυστικότητας για κάθε χρήστη συνεπώς μπορεί να χρησιμοποιηθεί ως μυστικός κωδικός δημιουργίας του ζεύγους.
- Αφού υποβληθούν τα στοιχεία, δημιουργείται μοναδικό ζεύγος δημόσιου/ιδιωτικού κλειδιού για κάθε χρήστη με τη χρήση των συναρτήσεων κρυπτογραφίας του openssl. Συγκεκριμένα χρησιμοποιούνται οι συναρτήσεις openssl_get_privatekey(), openssl_get_publickey() .
- Το δημόσιο κλειδί αποθηκεύεται στη ΒΔ του SWBES και το ιδιωτικό κλειδί αποστέλλεται στο χρήστη σε αρχείο PEM για να το κατεβάσει.
- Κατά την αποσύνδεση του χρήστη, το ιδιωτικό κλειδί διαγράφεται από τον εξυπηρετητή του SWBES όπως επίσης και όλες οι μεταβλητές συνεδρίας.
- Για την είσοδο ενός χρήστη στη σελίδα ενός επιλεγμένου μαθήματος, θα πρέπει να υποβληθεί το ιδιωτικό κλειδί. Αν επαληθευτεί, ο χρήστης οδηγείται στη σελίδα μαθήματος.



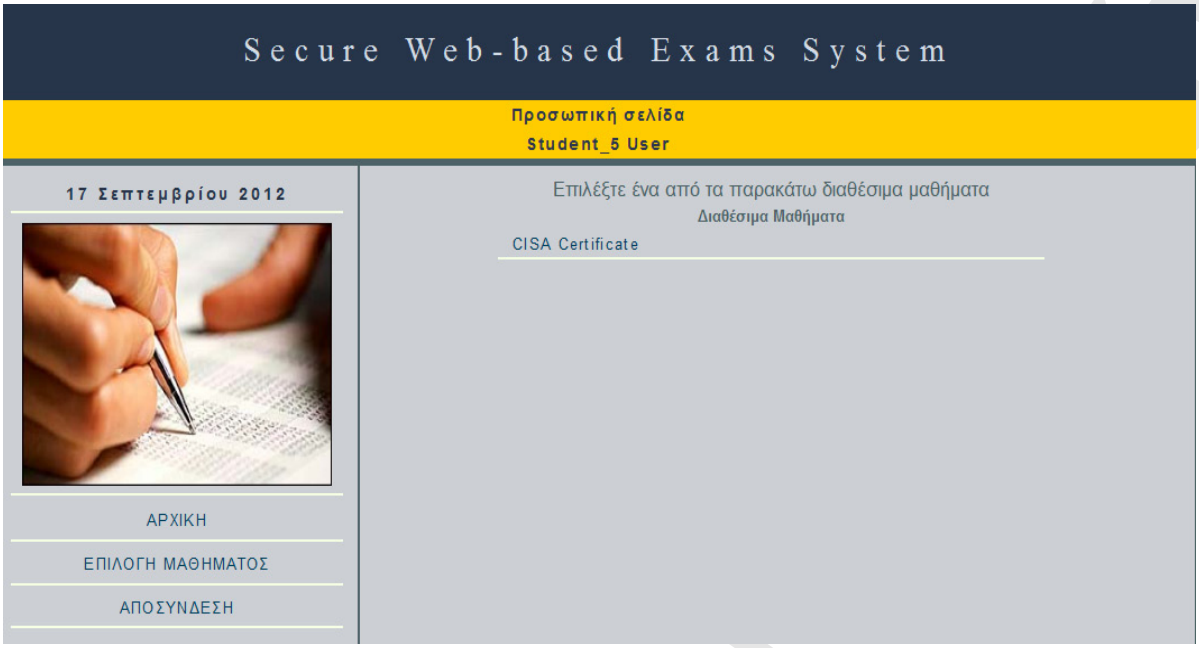
Εικόνα 5. Φόρμα δημιουργίας ζεύγους δημόσιου/ιδιωτικού κλειδιού



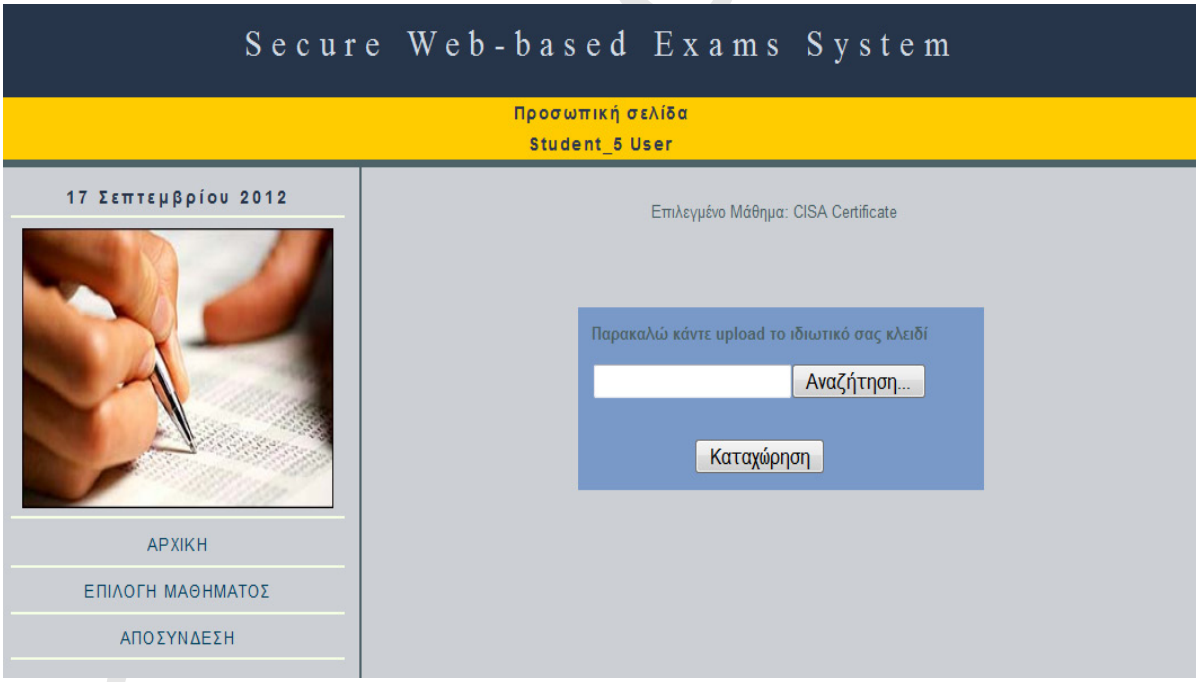
Εικόνα 6. Μεταφόρτωση ιδιωτικού κλειδιού

Δημόσιο Κλειδί	Ιδιωτικό Κλειδί
-----BEGIN CERTIFICATE----- MIIDGjCCAoOgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBqTELMAkGA1UEBhMCR1Ix DzANBgNVBAgMBmF0aGVuczESMBAGA1UEBwwJYWZhaWFzIDEyMR4wHAYDVQQKDBVV bml2ZXJzaXR5IE9mIFBpcmFldXMxFTATBgNVBAsMDCBJbmZvcm1hdGljczEXMBUG A1UEAwwOU3R1ZGVudF81IFVzZXIxJTAjBgkqhkiG9w0BCQEWFnN0dWRlbnRfNUBz ZWNtb29kbGUuZ3IwHhcNMTIwOTE2MjEyODMzWhcNMTMwOTE2MjEyODMzWjCBqTEL MAkGA1UEBhMCR1IxDzANBgNVBAgMBmF0aGVuczESMBAGA1UEBwwJYWZhaWFzIDEy MR4wHAYDVQQKDBVVbml2ZXJzaXR5IE9mIFBpcmFldXMxFTATBgNVBAsMDCBJbmZv cm1hdGljczEXMBUGA1UEAwwOU3R1ZGVudF81IFVzZXIxJTAjBgkqhkiG9w0BCQEW FnN0dWRlbnRfNUBzZWNtb29kbGUuZ3IwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ AoGBAPFLuHwvtWuxfnl+g8mSQ7Mkhi9zWjzlS316TktN5cknwJgZahSpXCQEZjj4 3Jt3CAj9lXDeac3UkDYmvpyt42IZJlxLr0m6HrsgCN7OOlQF0C2WAMuNnXbDMWio WIBrr1VH8xXMgHgsNNQ/4soRLbAQxQwk1Z+J6aw40UiuF4bXAgMBAAGjUDBOMB0G A1UdDgQWBBT3O+kHmcsv548/FJEUDry7iHq9uzAfBgNVHSMEGDAWgBT3O+kHmcsv 548/FJEUDry7iHq9uzAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBAUAA4GBAB6l 02D2VvIGsK7gJFPgZeomGBH2LOjMVMKVQearkKKbuwSyCxITvlGN0HuJo4Pi3Qx9 s7DLtnfD1+YPZXhpnhQ/FwgjH02nMkfXhdbwo3Hf4jDGVB48EY8itOD8Geu9paoH njckgZOIpKpM7lubMJntv/B7xr7gZijQWY6yEIXE -----END CERTIFICATE-----	-----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,E81DAE525573DFD9 enrQEbBaxSzh4xQFfEDMqtqjTZiZTy50a0Ftr5YNZiKeG0K1YI/Rxep3e4kGku57 OxoBmoS/T1fDK7zMnM/w0/eOdMnSQZJ3M9qN8NtoUYztfMCosT2y+0NCkjR2mB2q Kr/XVUkXBXUUgmAt6+IDqeagYAF//96KOgkW6qv5FtJOf4JXkJ4hZF60hi2Nk77P 7PH4RliX6vtFRQdvXDSpMx68q4a+bMwiVdfIhi1KDnSz377WI5h1wSdGgVNBNyaS Nnzg2/LH2RgK6v2AD37e6bkbnmFqM72tBp8onBQ6cXGHqoR4wSGAsicpRxbxuQ5a GpLwbIh1Y9/4SMdDZintMfzDiPoH27lctRB6JhJ27Cv4ALhM8axzPJX9shDNk5MX aT8Utyos0InDDckg4LN4ylAbwapeCk675tKs4Epxf/6gnKmq+NzNbKaAItC8cw19 x+MrNey8wa+HQqkG1HiQ6BMXhVZRRWeNvoRJtN0nHfNa0nH5DPHZEi9+oBvjfC5e 0JuOtmI8u8dkxYpV4AtUWpE4BZWaWxQeU2sjRFTe++rjkC17fINkpSQnPx0Bkomj ABV7tivln1LWPhXMdqFUn6OFB1NacB0jUsuLc+cl3sNpM0F5DjTNL6VJcaeHUAu2 UvvBReoya3ssb7XAuxAsmqKjGmMx/PpabTJ7ZRkoiHYve8woiec4bCWYC8/FJPdg S0XAAIRivqV9LTd4DlyBxnBsCcQQkNGVzYtv9ofC+6VkZJeHyjD2WH1cVmu5/oc6 zeSkEOellx54jFkEZHwCo0ilu5J2JoCs/28pvidkadr1NdVcj0PUzA== -----END RSA PRIVATE KEY-----

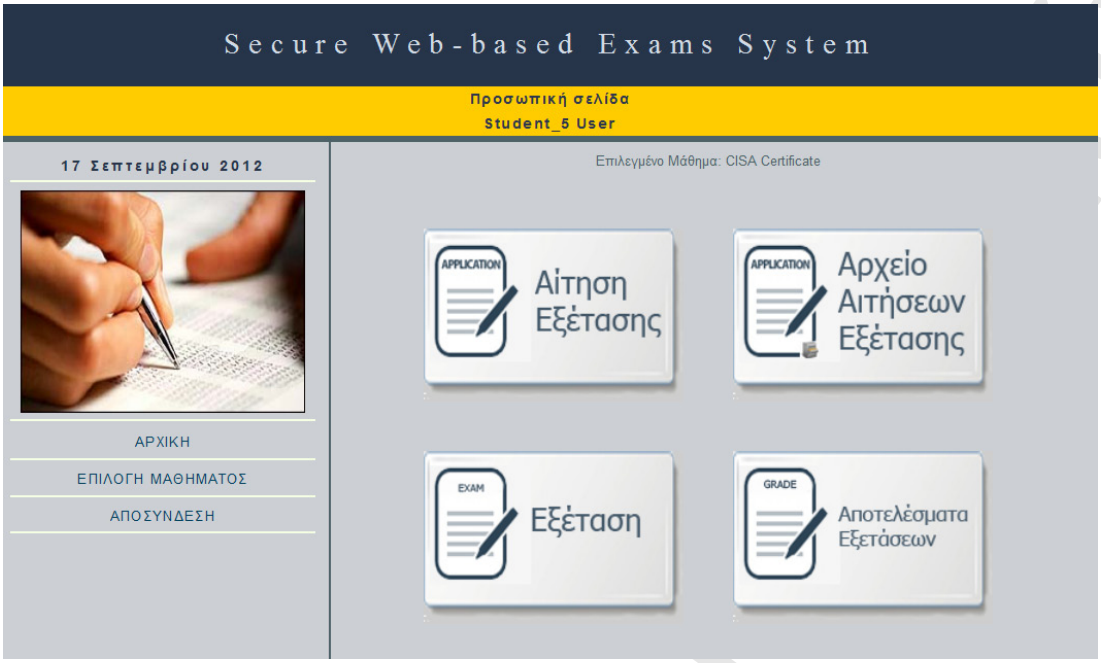
Πίνακας 5. Ζεύγος Δημόσιου/Ιδιωτικού κλειδιού



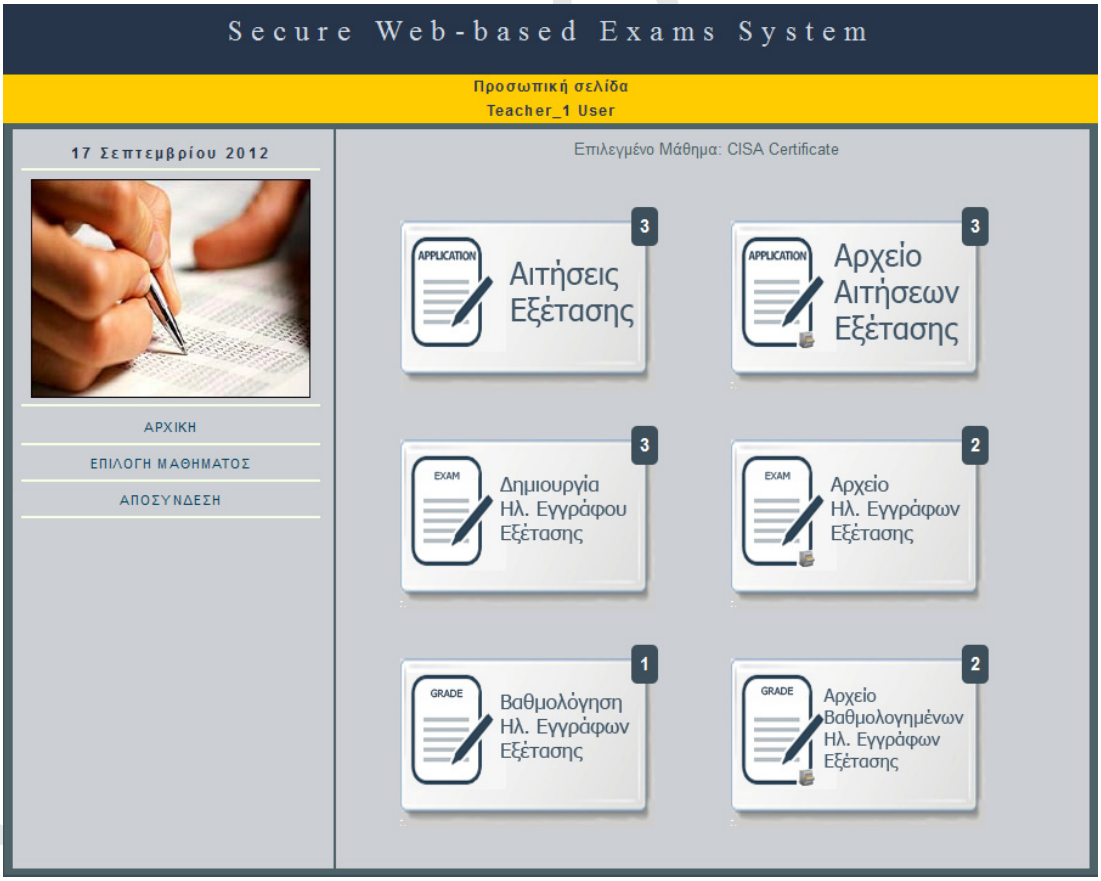
Εικόνα 7. Επιλογή Μαθήματος



Εικόνα 8. Υποβολή ιδιωτικού κλειδιού



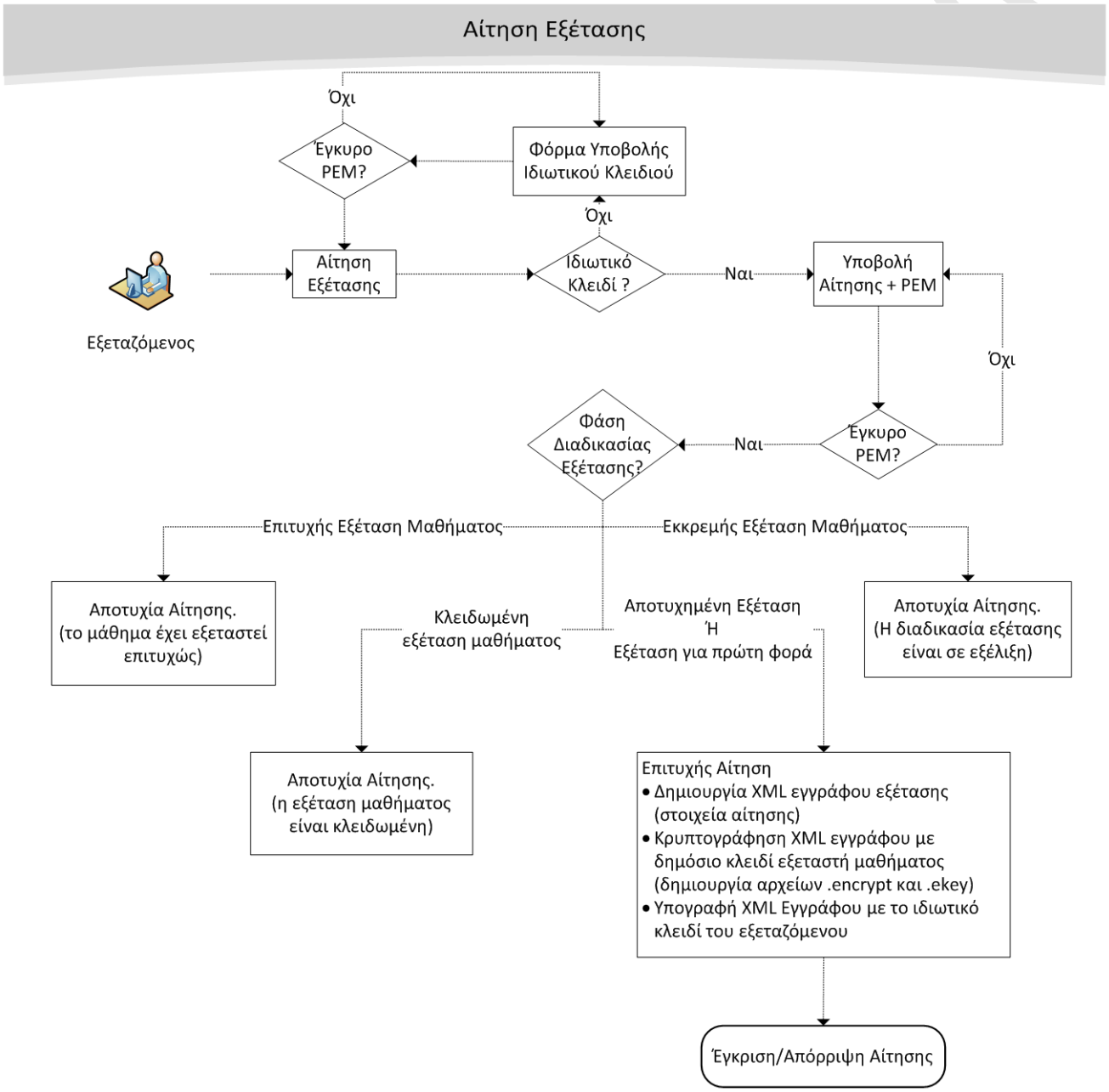
Εικόνα 9. Περιβάλλον Εξεταζόμενου - Σελίδα Μαθήματος



Εικόνα 10. Περιβάλλον Εξεταστή – Σελίδα Μαθήματος

Φάση Γ' : Αίτηση Εξέτασης

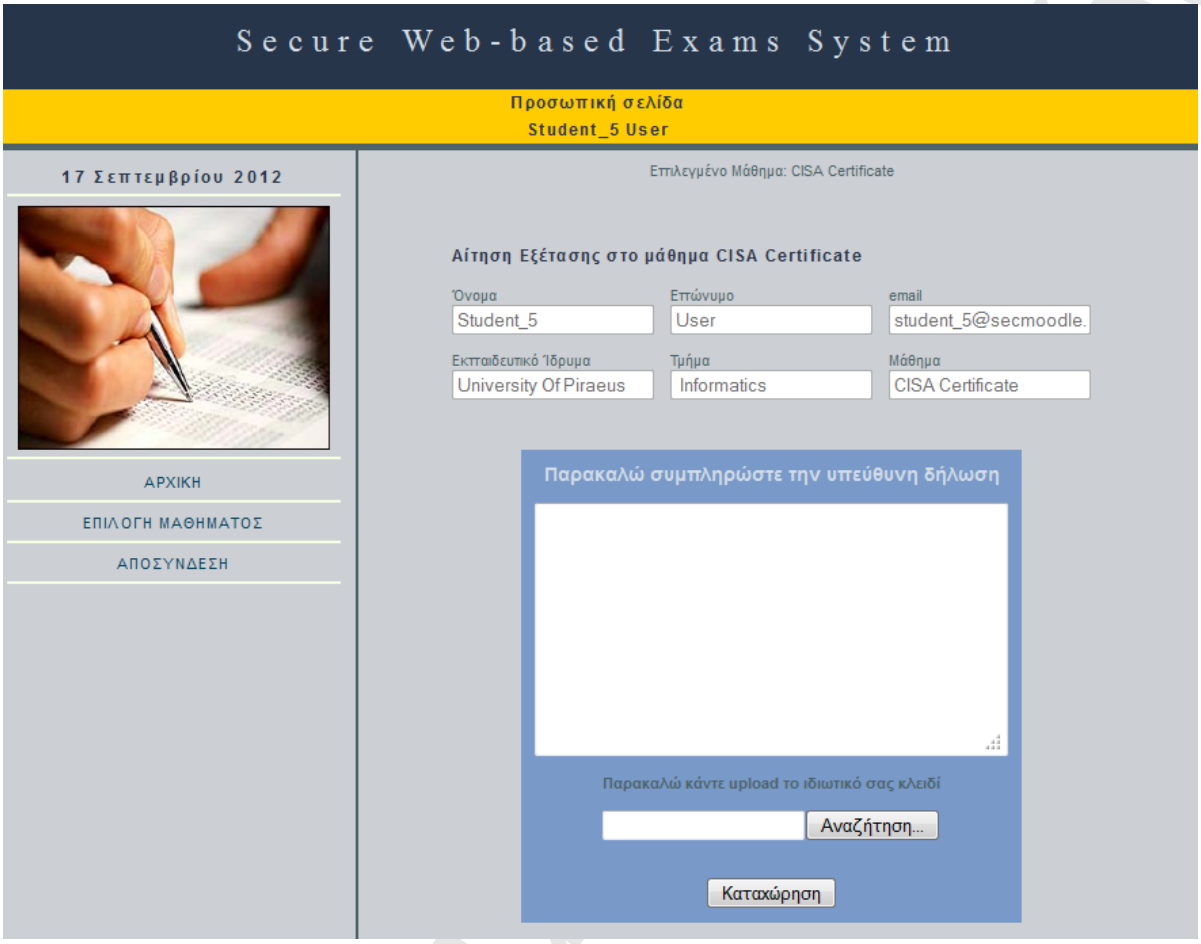
Ένας εξεταζόμενος για να μπορέσει να εξεταστεί σε ένα επιλεγμένο μάθημα, θα πρέπει αρχικά να κάνει αίτηση εξέτασης. Το παρακάτω διάγραμμα ροής παρουσιάζει τη διαδικασία αίτησης εξέτασης.



Σχήμα 12. Αίτηση Εξέτασης

Βασικά σημεία του παραπάνω διαγράμματος είναι τα εξής:

- Για την είσοδο στη σελίδα αίτησης εξέτασης γίνεται έλεγχος αν το ιδιωτικό κλειδί είναι στον εξυπηρετητή. Αν το ιδιωτικό κλειδί είναι έγκυρο, ο εξεταζόμενος οδηγείται στη σελίδα αίτησης όπως φαίνεται στην **Εικόνα 11**.



Εικόνα 11. Αίτηση Εξέτασης

- Κατά την υποβολή της αίτησης, καταχωρεί εκ νέου το ιδιωτικό κλειδί. Στη συνέχεια, αφού επαληθευτεί το ιδιωτικό κλειδί ότι είναι έγκυρο, ακολουθούν μια σειρά από διαδοχικοί έλεγχοι σχετικά με την εγκυρότητα της αίτησης.

Ο εξεταζόμενος δεν μπορεί να υποβάλλει αίτηση αν:

- Έχει εξεταστεί επιτυχώς στο επιλεγμένο μάθημα.
- Η διαδικασία εξέτασης είναι σε εκκρεμότητα. Πιο συγκεκριμένα,
  - η αίτηση έχει υποβληθεί αλλά δεν έχει εγκριθεί ή απορριφθεί.
  - η αίτηση έχει εγκριθεί αλλά δεν έχει δημιουργηθεί η-έγγραφο εξέτασης.
  - η αίτηση έχει εγκριθεί, έχει δημιουργηθεί η-έγγραφο εξέτασης αλλά δεν έχει απαντηθεί από τον εξεταζόμενο.
  - Η αίτηση έχει εγκριθεί, έχει δημιουργηθεί η-έγγραφο εξέτασης, έχει απαντηθεί αλλά δεν έχει βαθμολογηθεί.
- Η διαδικασία εξέτασης έχει κλειδωθεί για το επιλεγμένο μάθημα.

Ο εξεταζόμενος μπορεί να υποβάλλει αίτηση αν :

- Είναι η πρώτη αίτηση εξέτασης για το επιλεγμένο μάθημα.
- Έχει εξεταστεί ανεπιτυχώς για το επιλεγμένο μάθημα.
- Η αίτηση έχει απορριφθεί από τον εξεταστή.

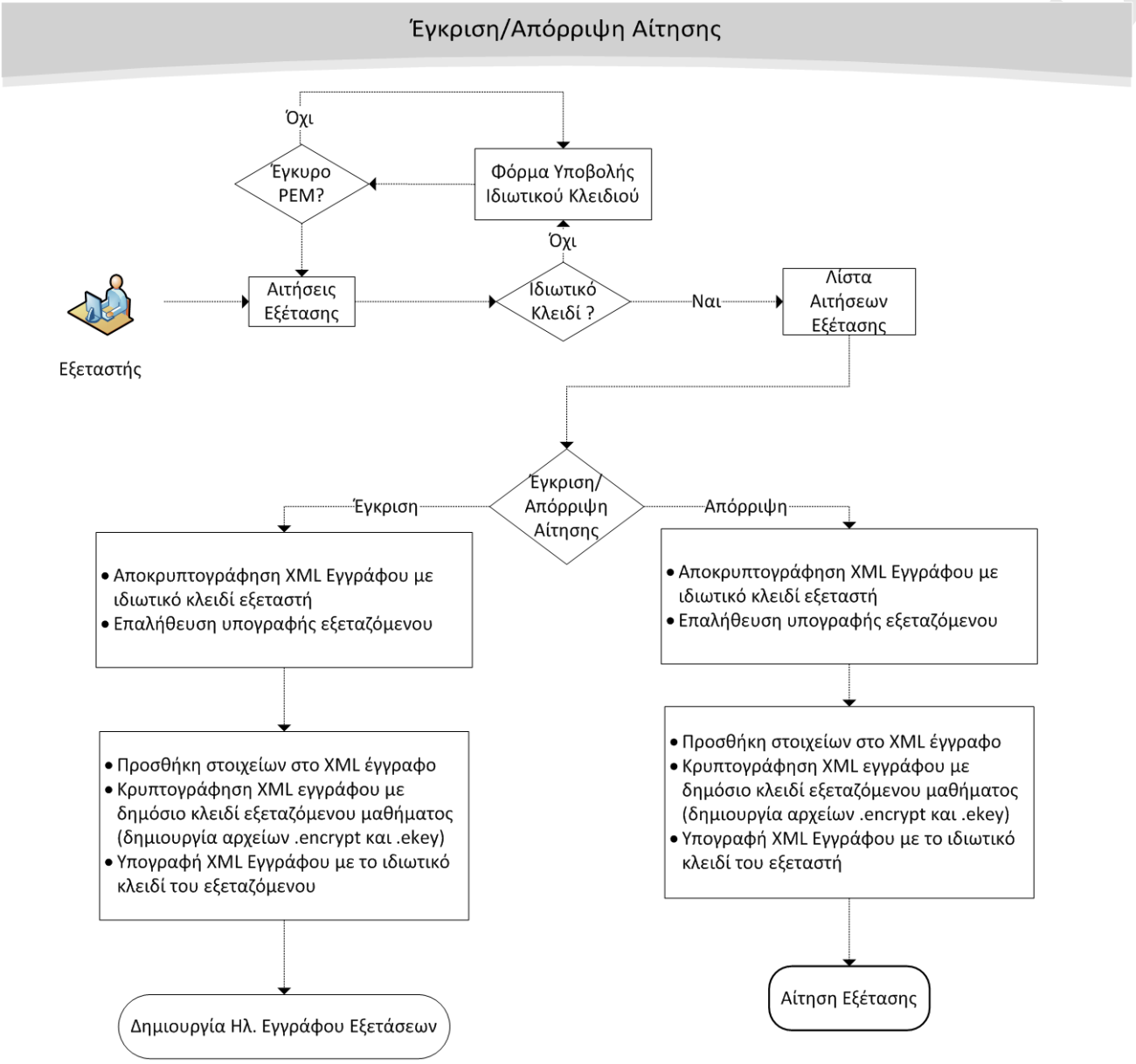
- Κατά την επιτυχή αίτηση εξέτασης, δημιουργείται ένα XML έγγραφο με τις απαραίτητες πληροφορίες του εξεταζόμενου. Το έγγραφο αυτό κρυπτογραφείται με το δημόσιο κλειδί του εξεταστή και υπογράφεται με το ιδιωτικό κλειδί του εξεταζόμενου. Οι συναρτήσεις openssl που υλοποιούν την κρυπτογράφηση δημόσιου κλειδιού και την ψηφιακή υπογραφή, είναι οι **openssl_seal()** και **openssl_sign()** αντίστοιχα. Πιο συγκεκριμένα, η συνάρτηση **openssl_seal()** δημιουργεί δύο αρχεία με κατάληξη **.encrypt** και **.ekey** . Το αρχείο **.encrypt** περιέχει το κρυπτογραφημένο XML έγγραφο και το αρχείο **.ekey** είναι απαραίτητο για τον παραλήπτη κατά την αποκρυπτογράφηση. Η συνάρτηση **openssl_sign()** υπογράφει ψηφιακά το xml έγγραφο με το ιδιωτικό κλειδί του εξεταζόμενου.

Ένα παράδειγμα xml εγγράφου που παράγεται σε κάθε αίτηση εξεταζόμενου είναι το παρακάτω:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<aitisi>
        <date_aitisis>15-09-2012</date_aitisis>
        <examinee_id>13</examinee_id>
        <examinee_onoma>Student_3</examinee_onoma>
        <examinee_eponimo>User</examinee_eponimo>
        <examinee_patronimo>test</examinee_patronimo>
        <examinee_dieythinsi>afaias 51</examinee_dieythinsi>
        <examinee_tilefono/>
        <examinee_birthday>test</examinee_birthday>
        <examinee_taytotita>test</examinee_taytotita>
        <examinee_afm>7036e33cf53cfe89cd67d954a8770d81</examinee_afm>
        <examinee_poli>athens</examinee_poli>
        <examinee_email>student_3@secmoodle.gr</examinee_email>
        <course_id>2</course_id>
        <examinee_comments/>
</aitisi>
```

- Μετά την επιτυχή αίτηση εξέτασης, η διαδικασία εξέτασης περνάει στη φάση έγκρισης/απόρριψης αίτησης.

Φάση Δ': Έγκριση/Απόρριψη Αίτησης

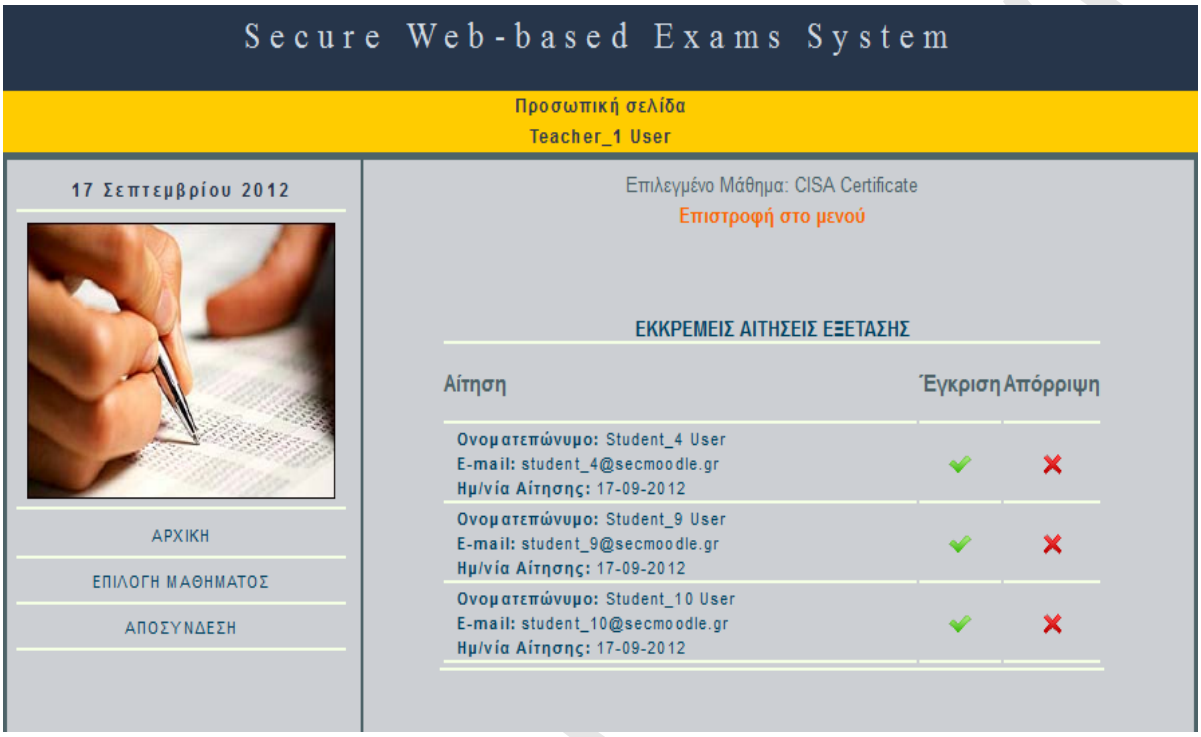


Σχήμα 13. Έγκριση/Απόρριψη Αίτησης Εξέτασης

Η φάση Δ' αναφέρεται στον εξεταστή ο οποίος θα πρέπει να εγκρίνει ή να απορρίψει την αίτηση εξέτασης έτσι ώστε να προχωρήσει η διαδικασία. Πιο συγκεκριμένα:

- Κατά την έγκριση ή απόρριψη μιας αίτησης, το κρυπτογραφημένο XML έγγραφο αποκρυπτογραφείται με το ιδιωτικό κλειδί του εξεταστή και επαληθεύεται η υπογραφή του εξεταζόμενου που έκανε την αίτηση. Στη συνέχεια, το XML έγγραφο εμπλουτίζεται με την ημερομηνία έγκρισης/απόρριψης, κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη εξεταζόμενου και υπογράφεται με το ιδιωτικό κλειδί του εξεταστή.

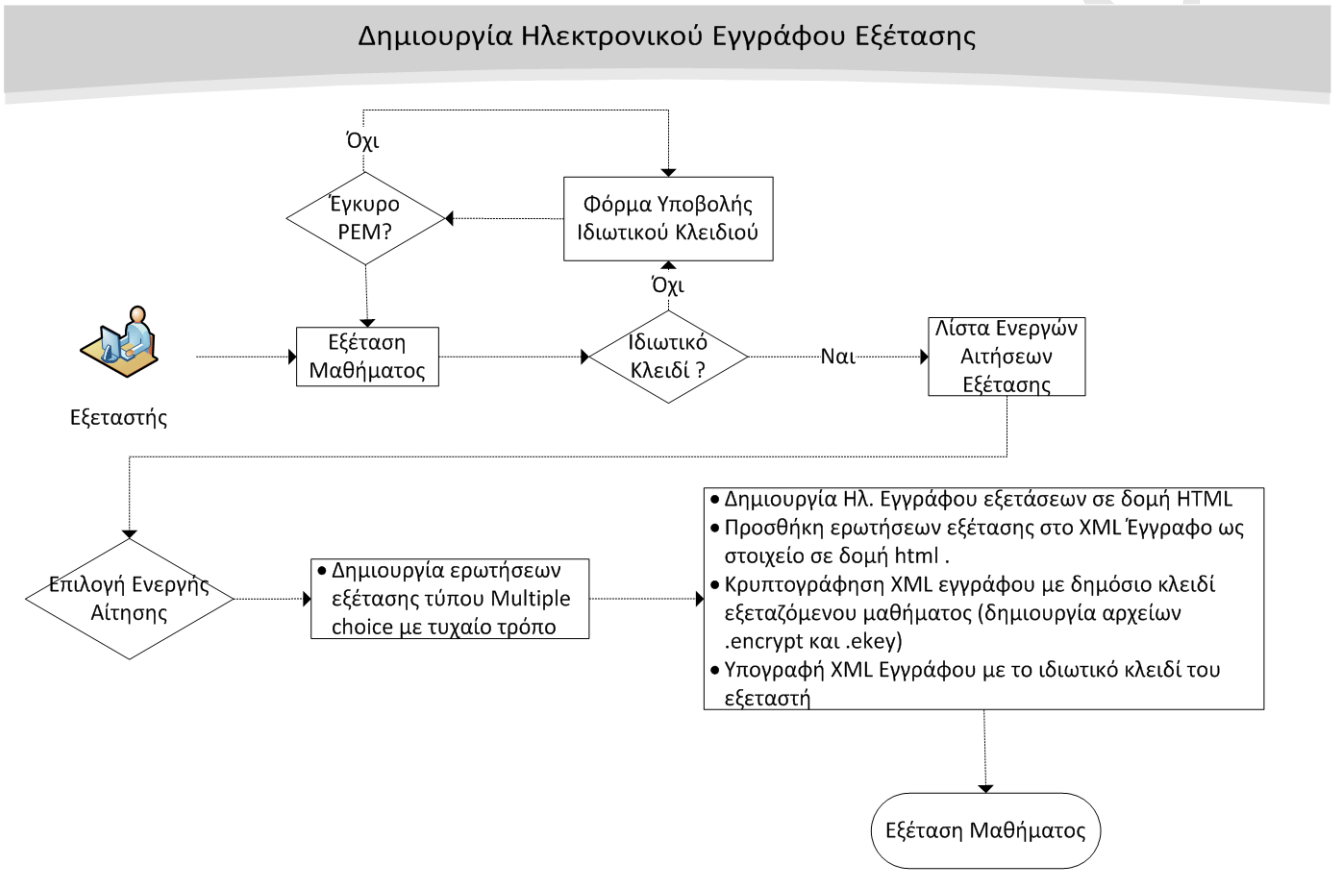
- Αν η αίτηση εγκριθεί, η διαδικασία περνάει στη φάση δημιουργίας η-εγγράφου εξετάσεων. Αν η αίτηση απορριφθεί, ο εξεταζόμενος οδηγείται εκ νέου στη φάση αίτησης εξέτασης όπου μπορεί να υποβάλλει ξανά αίτηση.



Εικόνα 12. Έγκριση/Απόρριψη Αίτησης Εξέτασης

Φάση Ε' : Δημιουργία η-Εγγράφου Εξέτασης

Στη φάση αυτή, ο εξεταστής δημιουργεί το η-έγγραφο εξέτασης το οποίο περιέχει τις ερωτήσεις στις οποίες ο εξεταζόμενος θα κληθεί να απαντήσει. Όπως και στις προηγούμενες φάσεις, η κρυπτογράφηση δημόσιου κλειδιού αποτελεί το βασικό μηχανισμό ασφάλειας. Στο παρακάτω διάγραμμα ροής φαίνονται τα βήματα που ακολουθούνται για τη μέχρι τη δημιουργία του η-εγγράφου εξέτασης.



Σχήμα 14. Δημιουργία η-Εγγράφου Εξέτασης

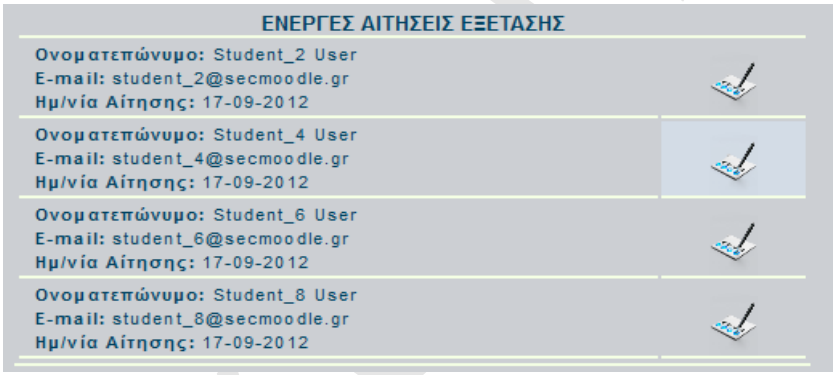
Το SWBES είναι τροφοδοτημένο με ένα σύνολο ερωτήσεων του μαθήματος, το οποίο αποτελεί την τράπεζα ερωτήσεων εξέτασης. Για τη δημιουργία του η-εγγράφου εξέτασης υλοποιήθηκε μηχανισμός σύμφωνα με τον οποίο:

1. Επιλέγεται τυχαία μια δεκάδα ερωτήσεων πολλαπλής επιλογής.
2. Η επιλεγμένη δεκάδα εμφανίζεται στον εξεταστή. Επειδή οι ερωτήσεις είναι πολλαπλής επιλογής εμφανίζονται οι ερωτήσεις και οι πιθανές απαντήσεις. Ο εξεταστής έχει τη δυνατότητα να αλλάξει τη δεκάδα ερωτήσεων επιλέγοντας την ανανέωση των ερωτήσεων .
3. Αν ο εξεταστής καταχωρήσει τη δεκάδα ερωτήσεων, δημιουργείται ένα XML έγγραφο με στοιχεία τις βασικές πληροφορίες της αίτησης και τις ερωτήσεις προς εξέταση.

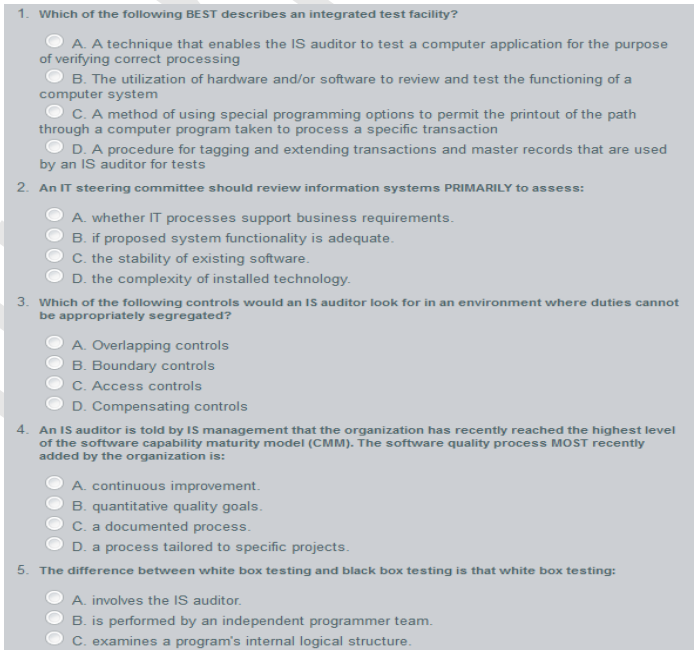
4. Οι ερωτήσεις εξέτασης αποθηκεύονται στο XML έγγραφο ως δομή HTML. Συγκεκριμένα παράγεται μια ολοκληρωμένη html σελίδα η οποία περιέχει τις ερωτήσεις, τις πιθανές απαντήσεις των ερωτήσεων, χρονόμετρο, τον απαραίτητο μηχανισμό υποβολής απαντήσεων και στυλ μορφοποίησης της html σελίδας. Επειδή η html περιέχει δεσμευμένους χαρακτήρες της XML, για την εγγραφή html μέσα σε ένα xml θα πρέπει το στοιχείο να μετατραπεί σε τύπο CDATA έτσι ώστε να μην υπάρχει δυνατότητα σάρωσης από έναν XML σαρωτή. Με αυτό τον τρόπο ο σαρωτής αγνοεί την ύπαρξη δεσμευμένων χαρακτήρων και το έγγραφο γίνεται έγκυρο.
5. Η τελική html σελίδα αποθηκεύεται ως στοιχείο του XML.

Το τελικό η-έγγραφο εξέτασης κρυπτογραφείται με το δημόσιο κλειδί του εξεταζόμενου και υπογράφεται με το ιδιωτικό κλειδί του εξεταστή. Συνεπώς ο εξεταστής παράγει για κάθε εξεταζόμενο ένα κρυπτογραφημένο xml έγγραφο εξέτασης το οποίο μπορεί να αποκρυπτογραφηθεί μόνο από τον κάθε εξεταζόμενο (με το ιδιωτικό κλειδί).

Χαρακτηριστικά στιγμιότυπα της φάσης Ε' φαίνονται παρακάτω.

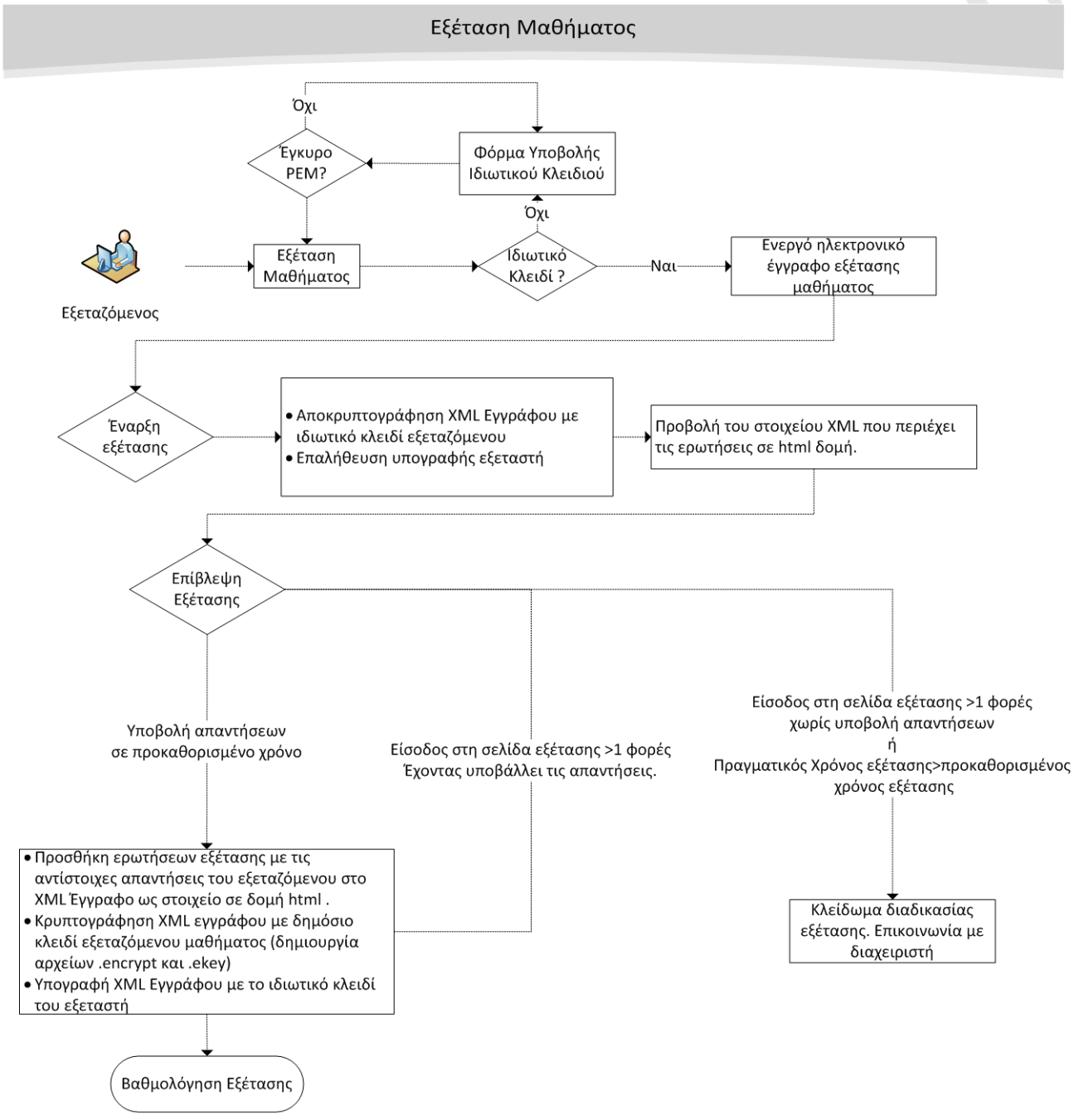


Εικόνα 13. Λίστα ενεργών αιτήσεων για δημιουργία η-εγγράφου εξετάσεων



Εικόνα 14. Δείγμα ερωτήσεων πολλαπλής επιλογής που καταχωρούνται στο XML έγγραφο

Φάση Στ': Εξέταση Μαθήματος



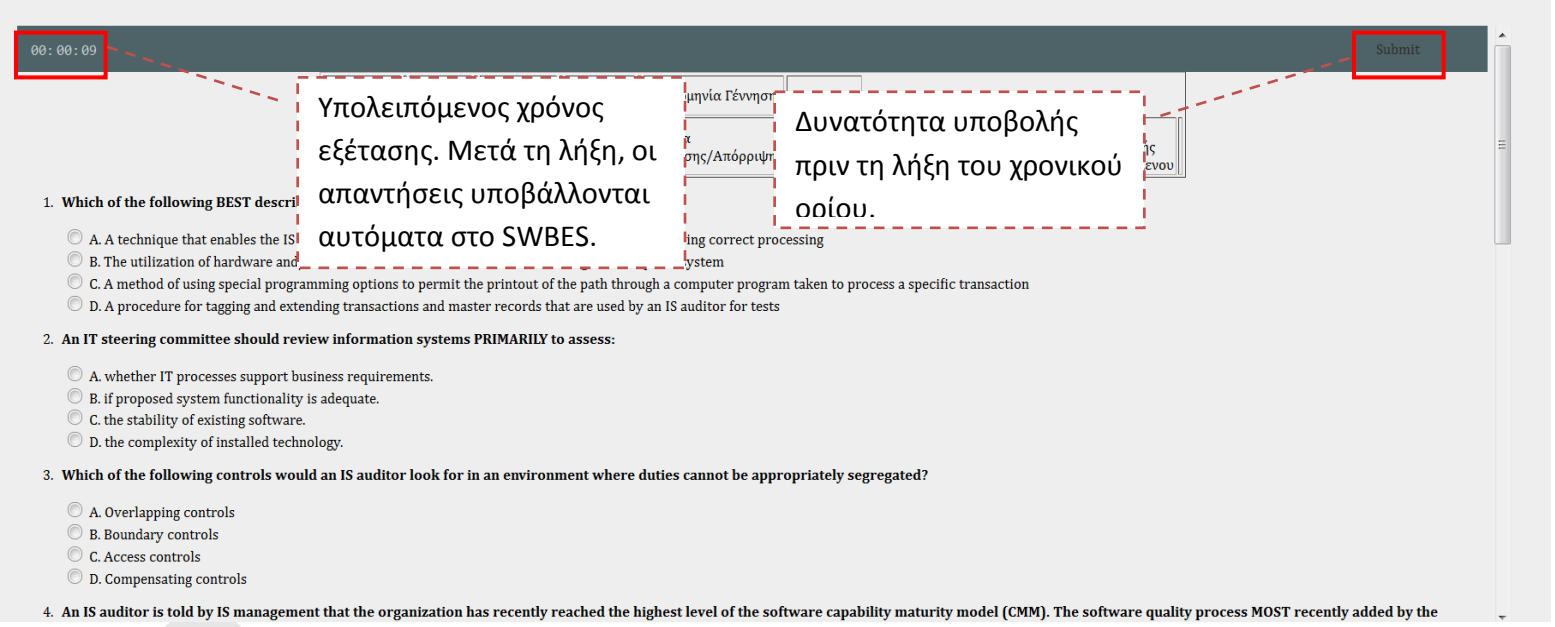
Σχήμα 15. Εξέταση Μαθήματος

Κατά την εξέταση του μαθήματος ο εξεταζόμενος αποκρυπτογραφεί το XML η-έγγραφο εξέτασης, επαληθεύει την υπογραφή του εξεταστή και οδηγείται στην html σελίδα εξέτασης που είναι αποθηκευμένη μέσα στο XML. Στην Εικόνα 15 φαίνεται η σελίδα εξέτασης που προβάλλεται στο εξεταζόμενο. Θα πρέπει να σημειωθεί ότι κατά τη εξέταση υπάρχουν

διαδοχικοί έλεγχοι προκειμένου να αποκλειστεί το ενδεχόμενο ο εξεταζόμενος να αλλοιώσει το αποτέλεσμα εξέτασης. Πιο συγκεκριμένα η διαδικασία εξέτασης κλειδώνεται στις παρακάτω περιπτώσεις:

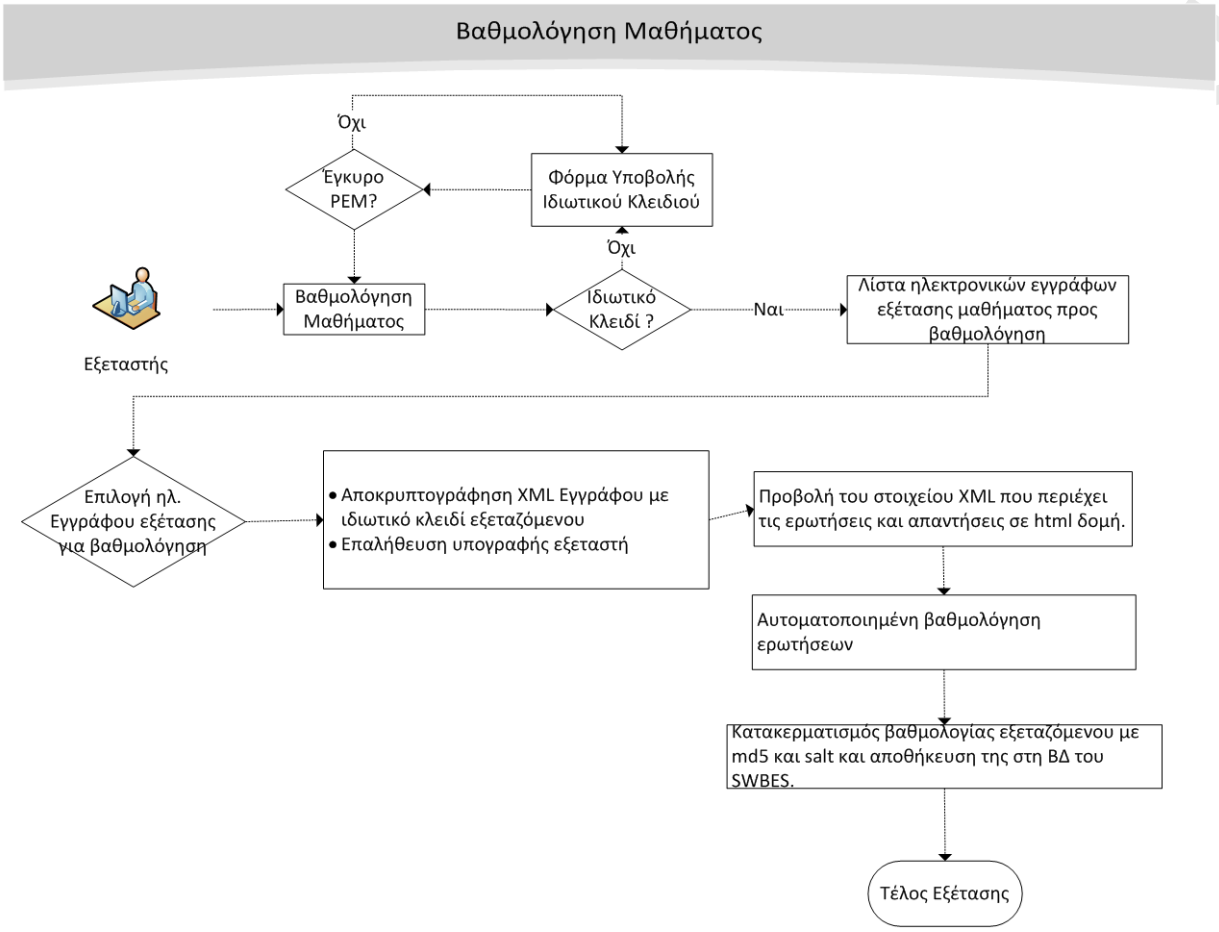
- Αν η πραγματική διάρκεια εξέτασης υπερβαίνει το δοσμένο επιτρεπτό χρονικό όριο. Ο εξεταζόμενος οφείλει να υποβάλει τις απαντήσεις των ερωτήσεων σε προκαθορισμένο χρονικό διάστημα το οποίο δηλώνεται ρητά μέσω χρονόμετρου στη σελίδα εξέτασης. Ο έλεγχος του χρόνου υποβολής γίνεται με μηχανισμό χρονοσφράγισης. Ο μηχανισμός επιτηρεί το χρόνο έναρξης και χρόνο λήξης της εξέτασης. Αν ο χρόνος που υπολογίζεται υπερβαίνει το επιτρεπτό χρονικό όριο εξέτασης, τότε η διαδικασία κλειδώνεται.
- Αν ο εξεταζόμενος προσπελάσει τη σελίδα εξέτασης περισσότερες από μια φορές χωρίς να έχει υποβάλλει τις απαντήσεις.

Κατά την υποβολή των απαντήσεων, δημιουργείται κρυπτογραφημένο XML έγγραφο το οποίο περιέχει τις απαραίτητες πληροφορίες εξεταζόμενου και τις απαντήσεις σε δομή html. Ουσιαστικά, χρησιμοποιείται ο ίδιος μηχανισμός αποθήκευσης html δομής μέσα σε XML με τη διαφορά ότι σε αυτή τη φάση, εκτός από τις ερωτήσεις, αποθηκεύονται και οι απαντήσεις του εξεταζόμενου σε html δομή. Επιπλέον, επειδή οι ερωτήσεις είναι πολλαπλής επιλογής, κατά τη αποθήκευση της html δομής μέσα στο xml, απενεργοποιούνται οι υπόλοιπες πιθανές απαντήσεις των ερωτήσεων, έχοντας ενεργοποιημένες μόνο τις απαντήσεις του εξεταζόμενου. Η απενεργοποίηση αυτή γίνεται έτσι ώστε ο εξεταστής να μη έχει τη δυνατότητα αλλαγής των απαντήσεων του εξεταζόμενου κατά την προβολή του εγγράφου εξέτασης στη φάση Στ’.



Εικόνα 15. HTML σελίδα εξέτασης

Φάση Ζ': Βαθμολόγηση Εξέτασης Μαθήματος



Σχήμα 16. Βαθμολόγηση Μαθήματος

Η τελευταία φάση της διαδικασίας εξέτασης περιλαμβάνει τη βαθμολόγηση του εξεταζόμενου. Σύμφωνα με το παραπάνω διάγραμμα ροής, κατά την επιλογή ενός η-εγγράφου για βαθμολόγηση, το XML έγγραφο αποκρυπτογραφείται με το ιδιωτικό κλειδί του εξεταστή και προβάλλεται η html δομή των ερωτήσεων και απαντήσεων του εξεταζόμενου. Όπως αναφέρθηκε και παραπάνω οι υπόλοιπες πιθανές απαντήσεις των ερωτήσεων είναι απενεργοποιημένες.

Κατά τη βαθμολόγηση, ενεργοποιείται μηχανισμός αυτόματης βαθμολόγησης της δεκάδας ερωτήσεων. Το SWBES είναι τροφοδοτημένο με τις σωστές απαντήσεις των ερωτήσεων βάσει των οποίων, ο μηχανισμός καταχωρεί τη βαθμολογία στη ΒΔ. Ταυτόχρονα, η βαθμολογία εμφανίζεται στο αρχείο βαθμολογημένων εγγράφων του εξεταστή αλλά και στη σχετική περιοχή του περιβάλλοντος του εξεταζόμενου.

5.2 Εφαρμογή Σχεδίου Πολιτικής Ασφάλειας Πληροφοριών στην Αρχιτεκτονική Ασφαλών η-Εξετάσεων μέσω Ιστού.

Στόχος της ενότητας είναι η αξιολόγηση της προτεινόμενης αρχιτεκτονικής εφαρμόζοντας το Σχέδιο Ασφάλειας Πληροφοριών που περιγράφηκε στο κεφάλαιο 4. Λαμβάνοντας υπόψη την τεχνική συνιστώσα του Σχεδίου, θα γίνει αντιστοίχιση των αντιμέτρων ασφάλειας που χρησιμοποιούνται στην προτεινόμενη Αρχιτεκτονική με τις βασικές απαιτήσεις ασφάλειας της τεχνικής συνιστώσας.

Όπως αναφέρθηκε και στο κεφάλαιο 4, η τεχνική συνιστώσα του Σχεδίου Ασφάλειας Πληροφοριών αποτελείται από τις τεχνικές προδιαγραφές που υλοποιούν τις έξι βασικές απαιτήσεις ασφάλειας: Ταυτοποίηση και Αυθεντικοποίηση, Εξουσιοδότηση, Εμπιστευτικότητα, Ακεραιότητα, μη Άρνηση της Ευθύνης και Διαθεσιμότητα. Στη συνέχεια γίνεται καταγραφή των μηχανισμών που αναπτύχθηκαν και ικανοποιούν αυτές τις απαιτήσεις.

Ταυτοποίηση και Αυθεντικοποίηση

Η διαδικασία αξιολόγησης της προτεινόμενης Αρχιτεκτονικής χρησιμοποιεί μηχανισμούς αυθεντικοποίησης σε διάφορα σημεία.

- Κατά την είσοδο χρήστη στο ΣΔΗΜ (Moodle)
  - **Μηχανισμός κωδικού πρόσβασης**. Για ισχυρή αυθεντικοποίηση, το σύστημα υποχρεώνει το χρήστη να χρησιμοποίησει ένα συνδυασμό ειδικών χαρακτήρων, αριθμών, κεφαλαίων και μικρών γραμμάτων.
- Κατά την επικοινωνία του ΣΔΗΜ (Moodle) με το SWBES
  - **Υποδομή Δημόσιου Κλειδιού**. Κάθε ΣΔΗΜ πιστοποιείται από την Αρχή Πιστοποίησης (Υπουργείο Παιδείας) και αυθεντικοποιείται από το SWBES. Αντίστοιχα, το SWBES διαθέτει έγκυρο πιστοποιητικό για την αυθεντικοποίηση του στα συνδεόμενα ΣΔΗΜ.
  - **Πρότυπο Διαλειτουργικότητας Μαθησιακών Εργαλείων LTI**. Κατά τη σύνδεση του ΣΔΗΜ με το SWBES χρησιμοποιείται το πρωτόκολλο αυθεντικοποίησης OAuth.
- Κατά την είσοδο χρήστη στο SWBES μέσω του ΣΔΗΜ (Moodle)
  - **Μηχανισμός κωδικού πρόσβασης**. Χρησιμοποιείται αντίγραφο του μηχανισμού αυθεντικοποίησης του Moodle.
- Κατά την είσοδο του χρήστη στο μενού μαθήματος
  - **Μηχανισμός επαλήθευσης ιδιωτικού κλειδιού** με χρήση κρυπτογραφίας δημόσιου κλειδιού.

Εξουσιοδότηση

Για την ανάθεση δικαιωμάτων στους χρήστες της προτεινόμενης Αρχιτεκτονικής:

- Περιβάλλον η-μάθησης του Moodle

- **Μηχανισμός Ελέγχου Πρόσβασης βασισμένος σε ρόλους** (Role-based Access Control). Κάθε ρόλος έχει διαφορετικά δικαιώματα.

- Περιβάλλον εξέτασης του SWBES
  - Οι ρόλοι κληρονομούνται στο περιβάλλον εξέτασης του SWBES και κάθε χρήστης, συναρτήσει του ρόλου του, έχει πρόσβαση σε διαφορετικό περιβάλλον και με διαφορετικές λειτουργίες.

Εμπιστευτικότητα

Στην επίτευξη της εμπιστευτικότητας στην προτεινόμενη Αρχιτεκτονική συμβάλλουν οι μηχανισμοί αυθεντικοποίησης όπως επίσης και η ύπαρξη μηχανισμού εξουσιοδότησης. Επιπλέον ισχύουν:

- Στην επικοινωνία μεταξύ χρήστη και ΣΔΗΜ (Moodle)
  - **Κρυπτογράφηση καναλιού επικοινωνίας με το πρωτόκολλο ασφάλειας SSL**. Απαραίτητη προϋπόθεση είναι η εγκυρότητα του πιστοποιητικού του ΣΔΗΜ από την Αρχή Πιστοποίησης.
- Στην επικοινωνία ΣΔΗΜ (Moodle) και SWBES
  - Κρυπτογράφηση καναλιού επικοινωνίας με το πρωτόκολλο ασφάλειας SSL. Απαραίτητη προϋπόθεση είναι η εγκυρότητα των πιστοποιητικού του ΣΔΗΜ και του SWBES.
- ΣΔΗΜ (Moodle)
  - **Κλειδί εγγραφής σε η-μάθημα**. Κάθε χρήστης για να συμμετέχει στην εκπαιδευτική διαδικασία (είτε ως εκπαιδευόμενος είτε ως εκπαιδευτής) απαιτείται ένα κλειδί εγγραφής για το η-μάθημα. Συνεπώς πρόσβαση στο εκπαιδευτικό υλικό έχουν όσοι είναι εγγεγραμμένοι στο μάθημα.
  - **Χρήση αλγόριθμου κατακερματισμού md5** με salt για την αποθήκευση κωδικών πρόσβασης
- Περιβάλλον εξέτασης του SWBES
  - **Κρυπτογράφηση δημόσιου κλειδιού**. Τα δεδομένα του αποστολέα κρυπτογραφούνται με το δημόσιο κλειδί του παραλήπτη και αποκρυπτογραφούνται με το ιδιωτικό κλειδί τουπαραλήπτη. Χαρακτηριστικό παράδειγμα είναι η αποστολή του η-εγγράφου εξέτασης από τον εξεταστή, κρυπτογραφημένο με το δημόσιο κλειδί του εξεταζόμενου. Ο εξεταζόμενος αποκρυπτογραφεί το έγγραφο με το ιδιωτικό κλειδί. Κάθε εξεταστής και εξεταζόμενο διαθέτει ένα μοναδικό ζεύγος δημόσιου και ιδιωτικού κλειδιού.
  - **Χρήση αλγόριθμου κατακερματισμού md5** με salt για την αποθήκευση κωδικών πρόσβασης και μυστικού κωδικού δημιουργίας ζεύγους δημόσιου/ιδιωτικού κλειδιού.
  - **Χρήση αλγόριθμου κωδικοποίησης base64** για τα ερωτήματα στη ΒΔ του Moodle κατά το συγχρονισμό των πανομοιότυπων πινάκων μεταξύ Moodle και ΣΔΗΜ.

Ακεραιότητα

Για την προστασία του περιεχομένου από τη μη εξουσιοδοτημένη τροποποίησή ή διαγραφή του κατά τη μεταφορά των δεδομένων στη διαδικασία αξιολόγησης χρησιμοποιούνται οι παρακάτω μηχανιμοί:

- **Χρήση ψηφιακών υπογραφών**. Τα δεδομένα μεταξύ εξεταστή και εξεταζόμενου υπογράφονται ψηφιακά όταν αποστέλλονται. Ο μηχανισμός που ικανοποιεί την ακεραιότητα είναι κατά τη σύγκριση της σύνοψης που αποστέλλεται με τη σύνοψη που δημιουργεί ο παραλήπτης από τα δεδομένα αν υπογραφούν ψηφιακά με το ιδιωτικό κλειδί του αποστολέα.
- **Υποδομή Δημόσιου Κλειδιού**. Μηχανισμοί ακεραιότητας κατά τη μεταφορά των δεδομένων ελέγχοντας τα δεδομένα κατά την είσοδο στο κανάλι επικοινωνίας και κατά την έξοδο τους.

Μη άρνηση της ευθύνης

- **Αρχείο καταγραφής δραστηριότητας χρηστών.** Ο μηχανισμός χρησιμοποιεί χρονοσφράγιση για την καταγραφή της δραστηριότητας των χρηστών.
- **Χρήση ψηφιακών υπογραφών**. Τα δεδομένα υπογράφονται ψηφιακά. Η επαλήθευση της υπογραφής από τον παραλήπτη, αυθεντικοποιεί τον αποστολέα.
- **Υποδομή Δημόσιου Κλειδιού**. Η Αρχή Εγγραφής εγγυάται την εγκυρότητα του δημόσιου κλειδιού για κάθε εμπλεκόμενο μέρος.

Διαθεσιμότητα

Η διαθεσιμότητα της υπηρεσίας ασφαλών εξετάσεων εξαρτάται άμεσα από τη διαθεσιμότητα των ΣΔΗΜ και SWBES. Οι υπεύθυνες ομάδες των συστημάτων έχουν ως βασική αρμοδιότητα την υλοποίηση διαδικασίας ανάκαμψης καταστροφών των υπηρεσιών και την εφαρμογή πολιτικής δημιουργίας αντιγράφων ασφαλείας.

5.3 Συγκριτική Αξιολόγηση Ασφάλειας

Αξιολογώντας την ασφάλεια της προτεινόμενης Αρχιτεκτονικής θα πρέπει να τη συγκρίνουμε με τη διαδικασία αξιολόγησης έτσι όπως υλοποιείται σε ένα ΣΔΗΜ όπως το Moodle. Στον παρακάτω πίνακα γίνεται άμεση σύγκριση των μηχανισμών ασφάλειας που υλοποιούνται στις δύο περιπτώσεις με σενάριο χρήσης τη διαδικασία αξιολόγησης.

Απαίτηση Ασφάλειας	Moodle	Αρχιτεκτονική Ασφαλών η-Εξετάσεων μέσω ιστού
Ταυτοποίηση και Αυθεντικοποίηση	*Είσοδος χρήστη στο Moodle* 1. Μηχανισμός κωδικού πρόσβασης	*Είσοδος χρήστη στο ΣΔΗΜ (Moodle)* 1. Μηχανισμός κωδικού πρόσβασης *Επικοινωνία ΣΔΗΜ (Moodle) με SWBES*

		1. Υποδομή Δημόσιου Κλειδιού 2. Πρότυπο Διαλειτουργικότητας Μαθησιακών Εργαλείων LTI *Είσοδος χρήστη στο SWBES μέσω του ΣΔΗΜ (Moodle)* 1. Μηχανισμός κωδικού πρόσβασης. *Είσοδος χρήστη στο μενού μαθήματος (SWBES)* 1. Μηχανισμός επαλήθευσης ιδιωτικού κλειδιού
Εξουσιοδότηση	Μηχανισμός Ελέγχου Πρόσβασης βασισμένος σε ρόλους	Μηχανισμός Ελέγχου Πρόσβασης βασισμένος σε ρόλους
Εμπιστευτικότητα	1. Πρωτόκολλο ασφάλειας SSL κατά την επικοινωνία χρήστη και Moodle 2. Κλειδί εγγραφής σε μάθημα 3. Αλγόριθμος Κατακερματισμού md5	*Επικοινωνία χρήστη-ΣΔΗΜ, ΣΔΗΜ-SWBES* 1. Πρωτόκολλο ασφάλειας SSL *ΣΔΗΜ (Moodle)* 1. Κλειδί εγγραφής σε μάθημα 2. Αλγόριθμος Κατακερματισμού md5 *SWBES* *1.* Κρυπτογράφηση δημόσιου κλειδιού *2.* Αλγόριθμος Κατακερματισμού md5 *3.* Κωδικοποίηση base64 ερωτημάτων προς τη βάση δεδομένων του SWBES
Ακεραιότητα	-	*1.* Ψηφιακές υπογραφές *2.* Υποδομή Δημόσιου Κλειδιού
Μη άρνηση ευθύνης	Αρχείο καταγραφής δραστηριότητας χρηστών	1. Αρχείο καταγραφής δραστηριότητας χρηστών 2. Ψηφιακές υπογραφές 3. Υποδομή Δημόσιου Κλειδιού
Διαθεσιμότητα	Μηχανισμός προγραμματισμένης δημιουργίας αντιγράφων ασφάλειας	Οι υπεύθυνες ομάδες των συστημάτων έχουν ως βασική αρμοδιότητα την υλοποίηση διαδικασίας ανάκαμψης καταστροφών της υπηρεσίας εξετάσεων και την εφαρμογή πολιτικής δημιουργίας αντιγράφων ασφαλείας
Επιπλέον λειτουργικά χαρακτηριστικά ασφάλειας	Ρυθμίσεις Χρόνου • Διαθεσιμότητα εξέτασης για συγκεκριμένο χρονικό διάστημα. • Χρονικό όριο υποβολής εξέτασης. Ρυθμίσεις Εξέτασης • Ρύθμιση μέγιστου αριθμού προσπαθειών υποβολής εξέτασης. • Τυχαία παραγωγή ερωτήσεων εξέτασης. • Αυτόματη υποβολή εξέτασης μετά το πέρας του χρονικού ορίου.	Ρυθμίσεις Χρόνου • Διαθεσιμότητα εξέτασης για συγκεκριμένο χρονικό διάστημα (μέσω του ΣΔΗΜ). • Χρονικό όριο υποβολής εξέτασης (μέσω του SWBES) Ρυθμίσεις Εξέτασης • Υποβολή εξέτασης μόνο μια φορά. Αν ο εξεταζόμενος δεν υποβάλλει την εξέταση και εισέλθει για δεύτερη φορά στις ερωτήσεις, υπάρχει αυτόματο κλείδωμα της διαδικασίας. • Τυχαία παραγωγή ερωτήσεων εξέτασης.

		• Αυτόματη υποβολή εξέτασης μετά το πέρας του χρονικού ορίου.

Πίνακας 6. Συγκριτικός Πίνακας μηχανισμών ασφάλειας Moodle και SWBES

Όπως φαίνεται από τον παραπάνω πίνακα, την προτεινόμενη Αρχιτεκτονική βελτιώνει αισθητά το βαθμό ασφάλειας στη διαδικασία αξιολόγησης καθώς οι βασικές απαιτήσεις της τεχνικής συνιστώσας του Σχεδίου Ασφάλειας ικανοποιούνται με έγκυρους μηχανισμούς ασφάλειας οι οποίοι προτάθηκαν στην ενότητα 3.3.6 . Η πολυπλοκότητα της προτεινόμενης Αρχιτεκτονικής είναι αυξημένη καθώς τα εμπλεκόμενα μέρη που συμμετέχουν στη διαδικασία χρησιμοποιούν διαφορετικές τεχνολογίες, όμως η Αρχιτεκτονική αποτελεί μια ολιστική λύση στη διαδικασία αξιολόγησης με χαρακτηριστικά γνωρίσματα την ανεξαρτησία τεχνολογιών και την εφαρμογή του Σχεδίου Ασφάλειας Πληροφοριών.

Συμπεράσματα - Προτάσεις

Βασικός στόχος της διατριβής ήταν η ενίσχυση της ασφάλειας πληροφοριών στα συστήματα διαχείρισης η-μάθησης και πιο συγκεκριμένα στη διαδικασία αξιολόγησης των εκπαιδευόμενων σε περιβάλλοντα η-μάθησης. Το **Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών για τα περιβάλλοντα η-μάθησης** και την **Αρχιτεκτονική Ασφαλών η-Εξετάσεων μέσω Ιστού** (Secure Web-Based Exam Schema) και το **Σύστημα Ασφαλών η-Εξετάσεων μέσω Ιστού (SWBES** – Secure Web-Based Exam System**)** αποτελούν τα παραδοτέα της διατριβής.

Αρχικά, ερευνήθηκαν και καταγράφηκαν οι απειλές ασφάλειας που δημιουργούνται από τη δραστηριότητα των χρηστών μέσα σε ένα περιβάλλον η-μάθησης. Στη συνέχεια καταγράφηκαν οι μηχανισμοί ασφάλειας που χρησιμοποιεί ένα γνωστό Σύστημα Διαχείρισης η-Μάθησης όπως το Moodle και προτάθηκε το **Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών για περιβάλλοντα η-μάθησης** το οποίο έρχεται να ενισχύσει την ασφάλεια στα συστήματα διαχείρισης η-μάθησης καθώς συνιστά έναν οδηγό αναφοράς ασφάλειας για τους οργανισμούς που επιθυμούν την ενσωμάτωση της τεχνολογίας στην εκπαιδευτική διαδικασία μέσω ενός ασφαλούς ΣΔΗΜ. Βασίζεται στο πρότυπο 27002 του Διεθνούς Οργανισμού Προτυποποίησης και αποτελείται από τις παρακάτω συνιστώσες ασφάλειας:

1. Διοίκηση Ασφάλειας Πληροφοριών
2. Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών
3. Ευαισθητοποίηση/Ενημέρωση Χρηστών
4. Διαδικασία Διαχείρισης και Αντιμετώπισης Περιστατικών Ασφάλειας
5. Σύστημα Μέτρησης Ασφάλειας ΠΣ
6. Υιοθέτηση και Υλοποίηση Αντιμέτρων Ασφάλειας (τεχνική συνιστώσα)

Η επίτευξη της ασφάλειας σε ένα ΣΔΗΜ αποτελεί μια πολυδιάστατη θεμελίωση η οποία απαιτεί την υλοποίηση ενός **κατάλληλου** συνόλου αντιμέτρων που περιλαμβάνει πολιτικές ασφάλειας, διαδικασίες, τρόπους ενέργειας, οδηγούς και πρακτικές αντιμετώπισης κινδύνων, οργανωτικές δομές όπως επίσης και τη συμβολή του λογισμικού και του υλικού. Τα αντίμετρα αυτά μπορούν να είναι διαχειριστικής, διοικητικής, νομικής και τεχνικής φύσης πράγμα το οποίο καθιστά εύκολο να αντιληφθούμε ότι κατά την επίτευξη της ασφάλειας σε ένα πληροφοριακό σύστημα, όπως ένα e-LMS, θα πρέπει να λάβουμε υπόψη όλες τις συνιστώσες ασφάλειας και όχι μόνο την τεχνική.

Οι παραπάνω συνιστώσες ασφάλειας αποτελούν σύμφωνα με το ISO 27002 τους κρίσιμους παράγοντες επίτευξης ενός ασφαλούς πληροφοριακού συστήματος και ταυτόχρονα ορίζουν ένα Πλαίσιο Ασφάλειας Πληροφοριών το οποίο μπορεί να εφαρμοστεί στα Συστήματα Διαχείρισης η-Μάθησης.

Η **Αρχιτεκτονική Ασφαλών Ηλεκτρονικών Εξετάσεων μέσω Ιστού** αποτελεί μια ολιστική λύση ασφάλειας στη διαδικασία αξιολόγησης των συστημάτων διαχείρισης η-μάθησης, τα βασικά γνωρίσματα του οποίου είναι τα εξής:

- Η **Αρχιτεκτονική** περιλαμβάνει όλα τα αντίμετρα ασφάλειας με στόχο την απόλυτη εναρμόνιση του με το Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών για περιβάλλοντα η-μάθησης.
- Η **Αρχιτεκτονική** έχει την δυνατότητα να υιοθετηθεί από οποιοδήποτε ΣΔΗΜ καθώς η ανεξαρτησία τεχνολογιών συμβάλλει στην ομαλή διαλειτουργικότητα των εμπλεκόμενων μερών.

Τα **Σύστημα Ασφαλών η-Εξετάσεων μέσω Ιστού (SWBES)** αποτελεί τον πυρήνα της Αρχιτεκτονικής καθώς υλοποιεί το μεγαλύτερο μέρος της διαδικασίας αξιολόγησης, τους μηχανισμούς ασφάλειας και τη διεπαφή εξέτασης. Στο πλαίσιο της διατριβής υλοποιήθηκε ένα αντίγραφο του συστήματος, πλήρως συμβατό με το Moodle, αναπτύσσοντας τους μηχανισμούς ασφάλειας που προτείνονται από το Πλαίσιο Ασφάλειας Πληροφοριών για τα περιβάλλοντα η-μάθησης.

Εφαρμόζοντας το Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών στην προτεινόμενη Αρχιτεκτονική, αποδείχτηκε ότι η διαδικασία αξιολόγησης ενισχύθηκε αισθητά στον τομέα της ασφάλειας συγκριτικά με τη διαδικασία αξιολόγησης έτσι όπως υλοποιείται σε ένα ΣΔΗΜ όπως το Moodle.

Μελλοντική Έρευνα και Προτάσεις Βελτίωσης

Το Σχέδιο Πολιτικής Ασφάλειας Πληροφοριών για περιβάλλοντα η-μάθησης αποτελεί μια αρχή για την προτυποποίηση της ασφάλειας σε οργανισμούς που χρησιμοποιούν Συστήματα διαχείρισης η-μάθησης. Ταυτόχρονα όμως δημιουργεί τις παρακάτω ερευνητικές ευκαιρίες και προτάσεις βελτίωσης:

- Εμπλουτισμός και Επέκταση Σχεδίου με συνιστώσες περισσότερο προσανατολισμένες στην η-μάθηση.
- Δημιουργία οδηγού εφαρμογής του Πλαισίου.
- Προτυποποίηση του τρόπου αξιολόγησης ασφάλειας των ΣΔΗΜ στα οποία εφαρμόζεται το Πλαίσιο.
- Δημιουργία web εργαλείου για την εφαρμογή του Σχεδίου.

Η προτεινόμενη Αρχιτεκτονική Ασφαλών η-Εξετάσεων μέσω Ιστού αποτελεί μια προσέγγιση ασφάλειας στη διαδικασία αξιολόγησης των εκπαιδευόμενων ενός ΣΔΗΜ. Μερικές προτάσεις βελτίωσης είναι οι παρακάτω:

- Δημιουργία μηχανισμού αυτόματης δημιουργίας αντιγράφου SWBES για κάθε ΣΔΗΜ που συμμετέχει στην Αρχιτεκτονική
- Μεταφορά δεδομένων μέσω του προτύπου διαλειτουργικότητας μαθησιακών εργαλείων LTI, από το SWBES προς το ΣΔΗΜ.
- Δημιουργία έκδοσης του LTI προσανατολισμένη στη διαδικασία αξιολόγησης.
- Βελτίωση τρόπου παρουσίασης δεδομένων μέσα από τη διεπαφή εξέτασης του SWBES.
- Πιλοτική εφαρμογή της Αρχιτεκτονικής Ασφαλών η-Εξετάσεων μέσω Ιστού.

- Εφαρμογή του αναθεωρημένου Σχεδίου Πολιτικής Ασφάλειας Πληροφοριών για περιβάλλοντα η-μάθησης και αξιολόγηση ασφάλειας της Αρχιτεκτονικής μέσω προτυποποιημένης διαδικασίας.

Βιβλιογραφία

[1] Aimeur, E., Hage, H., and Onana, F. S. M., "Anonymous Credentials for Privacy-Preserving E-learning," in *International MCETECH Conference on e-Technologies*, Montreal,Canada, 2008.

[2] Alwi, N. H. M. and Fan, I., "E-Learning and Information Security Management," *International Journal of Digital Society (IJDS)*, vol. 1, no. 2, pp. 148-156, 2010.

[3] Argles, D., Marais, E., and Von Solms, S. H., "Security Issues Specific to e-Assessment," in *8th Annual Conference on WWW Applications*, Bloemfontein, 2006.

[4] Brotby, K., Bayuk, J., and Coleman, C., *Information Security Governance: Guidance for Boards of Directors and Executive Management*. United States of America: IT Governance Institute, 2006. [Online]. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx

[5] Calder, A. and Watkins, S., *IT Governance, A Manager's Guide to Data Security and ISO27001/ISO 27002*. London and Philadelphia: Kogan Page Ltd., 2008.

[6] Chang, J. F. and Wang, S. J., "Smart card based Secure Password authentication Scheme," *Computers and Security*, vol. 15, no. 3, pp. 231-237, 1996.

[7] Chan, Y., Leung, C. H., and Liu, J. K., "Evaluation on Security and Privacy of Web-Based Learning Systems," in *The 3rd IEEE International Conference on Advanced Learning Technologies (ICALT'03)*, Ahens,Greece, 2003.

[8] Choules, A. P., "The use of elearning in medical education: a review of the current situation," *Postgraduate Medical Journal*, vol. 83, no. 978, pp. 212-216, 2007.

[9] Clayton, J. and Elliott, R., "Using e-learning to build workforce capability: A review of activities," 2008.

[10] Dietinger, T., "Aspects of e-Learning Environments," Institute for Information Systems and Computer Media (IICM), Faculty of Computer Science at Graz University of Technology, Austria, PhD Thesis 2003.

[11] Eastlake, D., Reagle, J., and Solo, D. (2002, March) XML-Signature Syntax and Processing, , . IETF RFC 3275. [Online]. http://www.ietf.org/rfc/rfc3275

[12] Eibl, C. J., "Privacy and Confidentiality in E-Learning Systems," in *Fourth International Conference on Internet and Web Applications and Services (ICIW)*, Venice/Mestre, Italy, 2009.

[13] Eibl, C. J., Von Solms, S. H., and Schubert, S., "A Framework for Evaluating the Information Security of E-learning Systems," in *2nd International Conference on Information in secondary Schools: Evolution and Perspectives (ISSEP2006)*, Vilnius, Lithuania, 2006.

[14] El-Khatib, K., Korba, L., Xu, Y., and Yee, G., "Privacy and Security in E-Learning," *International Journal of Distance Education*, vol. 1, no. 4, 2003.

[15] ENISA. (2010, December) Good Practice Guide for Incident Management. [Online]. http://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management

[16] Frankl, G., Schartner, P., and Zebedin, G., "The "Secure Exam Environment" for Online Testing," in *World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education (ELEARN) 2011*, Honolulu, Hawaii, USA, 2011, pp. 1201-1211.

[17] Gehrke, M., Mayer, M., and Schafer, W. An Architectural Framework for distributed E-Learning Systems. [Online]. http://www.campussource.de/org/projects

[18] Gelbord, B., "On the Use of PKI Technologies For Secure and Private e-learning Environments," in *International Conference on Computer Systems and Technologies-CompSysTech'2003*, Sofia, Bulgaria, 2003.

[19] Graf, F., "Providing security for eLearning," *Computers & Graphics*, vol. 26, no. 2, pp. 355-365, 2002.

[20] Gualberto, T. D. M., Abib, S., and Zorzo, S. D., "INCA: A Security Service for Collaborative Learning Environments," in *International Conference on Education Technology and Computer*, Singapore, 2009.

[21] Gualberto, T. D. M. and Zorzo, S. D., "Service for secure and protected Applications in Collaborative Learning Environments," in *IEEE International Conference on Systems, Man, and Cybernetics - SMC*, Istanbul,Turkey, 2010.

[22] Hallam-Baker, P. and Mysore, S. H. (2005, June) XML Key Management Specification (XKMS 2.0). W3C Recommendation. [Online]. http://www.w3.org/TR/xkms2/

[23] *ISO/IEC1779:2005(E) Information Technology – Security Technique - Code of Practice for Information Security Management*..

[24] *IT Governance Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management*. United State of America: IT Governance Institute, 2006.

[25] ITC-Council, "International Guidelines on Computer-Based and Internet Delivered Testing," 2005.

[26] Jalal, A. and Zeb, M. A., "Security Enhancement for E-Learning Portal," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 8, no. 3, pp. 41-45, 2008.

[27] Kritzinger, E. and Von Solms, S. H., "E-Learning: Incorporating Information Security

Governances," *Issues in informing Science and Information Technology*, vol. 3, pp. 319-326, 2006.

[28] Kumar, S., Gankotiya, A. K., and Dutta, K., "A Comparative Study of MOODLE with other e-Learning Systems," in *3rd International Conference on Electronics Computer Technology(ICECT 2011)*, Kanyakumari, India, 2011.

[29] Lambrinoudakis, C., Gritzalis, S., Dridi, F., and Pernul, G., "Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy," *Computer Communications*, vol. 26, no. 16, pp. 1873–1883, 2003.

[30] Lim, C. C. and Jin, J. S., "A Study on Applying Software Security to Information Systems: E-Learning Portals," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 6, no. 3B, pp. 162-166, 2006.

[31] Masadeh, S. R., Turab, N., and Obisat, F., "A secure model for building e-learning systems," *Network Security*, vol. 2012, no. 1, pp. 17–20, 2012.

[32] Miletić, D., *Moodle Security*. Birmingham: Packt Publishing Ltd., 2011.

[33] Moodle.org. (2012, September) Moodle 2.3 documentation. [Online]. http://docs.moodle.org/23/en/?lang=en

[34] Myrick, J., *Moodle 1.9 Testing and Assessment*. Birmingham: Packt Publishing, 2010.

[35] Nickolov, E. and Nickolova, M., "Threat Model for User Security in E-Learning Systems," *Information Technologies and Knowledge*, vol. 1, pp. 341-347, 2007.

[36] OASIS. (2002, May) Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML). Committee Specification. [Online]. http://www.oasis-open.org/committees/security/docs/

[37] OASIS. (2005, February) eXtensible Access Control Markup Language (XACML) Version 2.0. [Online]. http://docs.oasis-open.org/xacml/2.0/.

[38] OASIS. (2004, July) Security Assertion Markup Language (SAML) 2.0 Technical Overview. [Online]. http://www.oasis-open.org/committees/security/docs/.

[39] Polemi, D., *Security of IT systems (Notes for Undergraduate/Graduate Courses)*. Greece: University of Piraeus, 2005.

[40] Raitman, R., Ngo, L., Augar, N., and Zhou, W., "Security in the Online E-learning Environment," in *Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05)*, Washington, DC, USA, 2005, pp. 702-706.

[41] Rice, W., *Moodle E-Learning Course Development: A complete guide to successful learning using Moodle*. Birmingham, UK: Packt Publishing Ltd., 2006.

[42] Sessink, O., Beeftink, R., Tramper, J., and Hartog, R., "Securing Web-Based Exams," *Journal of Universal Computer Science*, vol. 10, no. 2, pp. 145-157, 2004.

[43] Siddiqui, B. (2002, March) Exploring XML Encryption, Part 1. IBM DeveloperWorks. [Online]. http://www-128.ibm.com/developerworks/xml/library/x-encrypt

[44] Siddiqui, B. (2002, March) Exploring XML Encryption, Part 2. IBM DeveloperWorks. [Online]. http://www-128.ibm.com/developerworks/xml/library/x-encrypt2

[45] Stapić, Z., Orehovački, T., and Đanić, M., "Determination of optimal security settings for LMS Moodle," in *31st MIPRO International Convention on Information Systems Security*, Opatija, Croatia, 2008.

[46] Suilleabhain, G. O., "Principles, structure and framework of e-learning," DEIS Department for Education Development at the Cork Institute of Technology, Ireland, MSc 2003.

[47] Virvou, M., Polemi, N., and Kabassi, K., "Completeness, Security and Privacy in User Modelling for Web-Based Learning," in *Web Information Systems and Technologies - WEBIST*, Setubal,Portugal, 2006.

[48] Von Solms, S. H., "Corporate Governance & information Security," *Computers and Security*, vol. 20, no. 3, pp. 215-218, 2001.

[49] Von Solms, S. H., "Information Security – A Multidimensional Discipline," *Computers and Security*, vol. 20, no. 6, pp. 504-508, 2001.

[50] Von Solms, S. H., "Information Security Governance in ICT based Educational systems," in *4th International Conference on ICT and Higher Education*, Bangkok, Thailand, 2005.

[51] Weippl, E., *Security in E-Learning*. United States of America: Springer, 2005.

[52] Weippl, E. and Ebner, M., "Security & Privacy Challenges in E-Learning 2.0," in *E-Learn*, Las Vegas, 2008.

[53] Wikipedia. e-Learning. [Online]. http://en.wikipedia.org/wiki/E-learning

[54] Wikipedia. Learning management system. [Online]. http://en.wikipedia.org/wiki/Learning_management_system

[55] Wikipedia. Security risk. [Online]. http://en.wikipedia.org/wiki/Security_risk

[56] Yong, J., "Security and Privacy Preservation for Mobile E-Learning via Digital Identity Attributes," *Journal of Universal Computer Science*, vol. 17, no. 2, pp. 296-310, 2011.