ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΣΧΟΛΗ ΕΠΙΣΤΗΜΩΝ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Εισηγητής: Σωτήρης Μπαρσάκης, ΑΜ 238

Επιβλέπων: Γεώργιος Αρακαδάκης

HELLENIC MEDITERRANEAN UNIVERSITY

SCHOOL OF MANAGEMENT AND ECONOMICS SCIENCE

DEPARTMENT OF MANAGMENENT SCIENCE AND TECHNOLOGY

Cryptography in e-commerce

DIPLOMA THESIS

Student : Sotirios Ioannis Barsakis, A.M. 238

Supervisor : Georgios Arakadakis

Υπεύθυνη Δήλωση *: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Διοίκησης Επιχειρήσεων Αγίου Νικολάου του Τ.Ε.Ι. Κρήτης.*

ΠΕΡΙΛΗΨΗ

Οι ραγδαίες τεχνολογικές εξελίξεις στον τομέα της Πληροφορικής σε συνδυασμό με την ταχύτατη εξάπλωση του Internetτα τελευταία χρόνια, έχουν προκαλέσει ουσιαστικά μια επανάσταση στο χώρο του επιχειρείν και έχουν φέρει τις επιχειρήσεις αντιμέτωπες με μια σειρά προκλήσεων. Η χρήση των νέων τεχνολογιών και του Internet (E-Commerce. E- Businessκλπ) προσφέρει στις επιχειρήσεις, μέσα από προσεκτική ανασχεδίαση των επιχειρηματικών διαδικασιών (BusinessProcessReengineering), την ευκαιρία για μεγάλες μειώσεις κόστους, καθιέρωση νέων διαύλων με πελάτες και εταίρους και καλύτερη ολοκλήρωση της εφοδιαστικής αλυσίδας. Τα παραπάνω ενισχύονται. αν ληφθεί υπ όψη η άρση πολλών εμπορικών περιορισμών στα πλαίσια της απελευθέρωσης των αγορών και της παγκοσμιοποίησης, γεγονός όμως που έχει σαν συνέπεια την ένταση του ανταγωνισμού και τη μείωση των' περιθωρίων κέρδους,

Το ηλεκτρονικό εμπόριο (ηλεκτρονικό εμπόριο) είναι η αγορά και πώληση εμπορευμάτων και επιχειρήσεων ή η διαβίβαση περιουσιακών στοιχείων ή πληροφοριών μέσω ηλεκτρονικού δικτύου, κυρίως μέσω διαδικτύου. Αυτές οι επιχειρηματικές ανταλλαγές συμβαίνουν είτε ως b to b (businessto-business), b έως c (από επιχειρήσεις προς καταναλωτές), c έως c (καταναλωτές-καταναλωτές) ή γ-β (καταναλωτές-επιχειρήσεις). σε αντικείμενα ή υπηρεσίες που χρησιμοποιούν δίκτυα υπολογιστών όπως το Internet ή σε απευθείας σύνδεση ανεπίσημες κοινότητες.

Περιλαμβάνει δραστηριότητες, για παράδειγμα, προμήθειες, είσοδο παραγγελιών, επεξεργασία ανταλλαγής, ηλεκτρονική πληρωμή, έλεγχο ταυτότητας, έλεγχο απογραφής, εκτέλεση παραγγελιών, αποστολή και υποστήριξη πελατών. Όταν ένας αγοραστής πληρώνει με μια τραπεζική κάρτα που πετάει μέσα από ένα μαγνητικό stripeader, αυτός ή αυτή ενδιαφέρεται για το ηλεκτρονικό εμπόριο. Η ασφάλεια ηλεκτρονικού εμπορίου είναι ένα κομμάτι του πλαισίου ασφάλειας πληροφοριών και εφαρμόζεται ειδικά στα στοιχεία που επηρεάζουν το ηλεκτρονικό εμπόριο, συμπεριλαμβανομένης της ασφάλειας των δεδομένων και άλλων ευρύτερων πεδίων του πλαισίου ασφάλειας πληροφοριών (Turbanetal, 2006).

Η ασφάλεια ηλεκτρονικού εμπορίου είναι η προστασία των περιουσιακών στοιχείων ηλεκτρονικού εμπορίου από μη εξουσιοδοτημένη πρόσβαση, χρήση, μετατροπή ή καταστροφή. Το ηλεκτρονικό εμπόριο προσφέρει μια μεγάλη ευκαιρία για

τη διαχείριση μιας βιομηχανίας λογαριασμού, αλλά επιπλέον δημιουργεί μια σειρά νέων κινδύνων και ευπάθειας, όπως για παράδειγμα, απειλές για την ασφάλεια, hackings (Δουκίδης & Φραιδάκη, 2010).

Ως εκ τούτου, αποτελεί ουσιαστική διοικητική και τεχνική απαίτηση για αποτελεσματικές και αποτελεσματικές δραστηριότητες ανταλλαγής πληρωμών μέσω του Διαδικτύου. Ακόμα και τα ψώνια μέσω του ηλεκτρονικού εμπορίου έχουν διεισδύσει σε όλα τα τμήματα των εμπορευμάτων που πηγαίνουν από παντοπωλεία σε ηλεκτρονικά προϊόντα και ακόμη και οχήματα. Η ταχεία εξέλιξη στις τεχνολογίες κινητής τηλεφωνίας και αλληλογραφίας διευκόλυνε την πανταχού παρούσα χρήση του ηλεκτρονικού εμπορίου. Το βασικό εμπόδιο στην ανάπτυξη του ηλεκτρονικού εμπορίου είναι η ψευδής παρουσίαση του κυβερνοχώρου και η κλοπή ταυτότητας. Οι χάκερ είναι άνθρωποι που ολοκληρώνουν το έγκλημα στον κυβερνοχώρο. Ως εκ τούτου, η κακή ασφάλεια στους διακομιστές ιστού του ηλεκτρονικού εμπορίου και στους υπολογιστές του χρήστη είναι βασικό ζήτημα που πρέπει να επιλυθεί για την ταχεία ανάπτυξη του ηλεκτρονικού εμπορίου.

Λέξεις Κλειδιά: Ηλεκτρονικό Εμπόριο, Κρυπτογράφηση, ηλεκτρονικά καταστήματα, ιστοσελίδες, υπογραφή

SUMMARY

The rapid technological developments in the field of Informatics combined with the rapid spread of the Internet in recent years, have caused a real revolution in the field of business and have brought businesses facing a number of challenges. The use of new technologies and the Internet (E-Commerce. E-Business, etc.) offers businesses, through careful redesign of business processes (Business Process Reengineering), the opportunity for large cost reductions, the introduction of new channels with customers and partners and better integration supply chain. The above are reinforced. taking into account the removal of many trade restrictions in the context of market liberalization and globalization, but which has the effect of intensifying competition and reducing profit margins,

E-commerce (e-commerce) is the buying and selling of goods and businesses or the transmission of assets or information through an electronic network, mainly through the Internet. These business exchanges occur as either b to b (businessto-business), b to c (from business to consumers), c to c (consumers-consumers) or c-b (consumers-businesses). in objects or services that use computer networks such as the Internet or online informal communities.

It includes activities, for example, procurement, order entry, batch processing, electronic payment, authentication, inventory verification, order execution, shipping and customer support. When a buyer pays with a bank card that flies through a magnetic stripeader, he or she is interested in e-commerce. E-commerce security is a part of the information security framework and applies specifically to elements that affect e-commerce, including data security and other broader areas of the information security framework (Turbanetal, 2006).

E-commerce security is the protection of e-commerce assets from unauthorized access, use, conversion or destruction. E-commerce offers a great opportunity to manage an account industry, but also creates a number of new risks and vulnerabilities, such as security threats, hackings (Doukidis & Fraidaki, 2010).

It is therefore an essential administrative and technical requirement for effective and efficient online payment activities. Even e-commerce shopping has penetrated all segments of goods ranging from grocery stores to electronic products and even vehicles. The rapid development of mobile and mail technologies has facilitated the ubiquitous use of e-commerce. The main obstacle to the development of e-commerce is the false presentation of cyberspace and identity theft. Hackers are people who commit cybercrime. Therefore, poor security on e-commerce web servers and user computers is a key issue that needs to be addressed for the rapid development of e-commerce.

Keywords: e-shop, ssl, cryptography, e-commerce, encrypted key

Πίνακας περιεχομένων

ΚΕΦΑΛΑΙΟ 1- ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

1.1. Ηλεκτρονικό Εμπόριο

Οι σύγχρονες επικοινωνιακές τεχνολογίες και τεχνολογίες πληροφοριών μπορούν να επιτρέψουν την αλλαγή των οργανωτικών δομών και των επιχειρηματικών διαδικασιών και επηρεάζουν το ανταγωνιστικό πλεονέκτημα των επιχειρήσεων. Κάτω από τις επιρροές τους οι αγορές αποκτούν όλο και μεγαλύτερη σημασία ως μορφή συντονισμού. Αλλά και οι εκδηλώσεις εντός της δομής της αγοράς και της αγοράς αντιμετωπίζουν αλλαγές εξαιτίας της αυξανόμενης χρήσης των σύγχρονων τηλεπικοινωνιακών μέσων (Δουκίδης & Φραιδάκη, 2010).

Οι οδηγοί, η φύση και τα μεγέθη αυτών των αλλαγών είναι τα βασικά σημεία και οι δυνατότητες του ηλεκτρονικού εμπορίου και εξετάζονται σε αυτή τη συμβολή. Το ηλεκτρονικό εμπόριο είναι μια σχετικά νέα ιδέα και έχει φτάσει στο επιχειρηματικό λεξιλόγιο όχι νωρίτερα από τη δεκαετία του '70. Αντιμετωπίζουμε πολλές οικονομικές δραστηριότητες που βρίσκουν ηλεκτρονική υποστήριξη. Ο λογοτεχνικός και εμπορικός τύπος τείνει να μην περιγράφει σαφώς μεταξύ «ηλεκτρονικών επιχειρήσεων», «ηλεκτρονικού εμπορίου», «ηλεκτρονικών αγορών», και συναφών όρων. Ίσως δεν πρέπει να εκπλαγούμε, καθώς ο τομέας του ηλεκτρονικού εμπορίου και των οργανωτικών διαδικασιών υπόκειται σε γρήγορες και συχνά δραματικές και εξωτερικά προκαλούμενες τεχνολογικές αλλαγές. Η ευρεία χρήση των προσωπικών υπολογιστών, σε συνδυασμό με τον πολλαπλασιασμό των τηλεπικοινωνιακών δικτύων και του Διαδικτύου, καθώς και με την κοινή τους ολοκλήρωση, κατέστησε πραγματικότητα το εμπόριο χωρίς χαρτί, ακόμη και για τους κοινούς πολίτες (Chaffey, 2007).

Σε ευρεία έννοια, το ηλεκτρονικό εμπόριο περιλαμβάνει οποιαδήποτε μορφή οικονομικής δραστηριότητας διεξάγονται μέσω ηλεκτρονικών συνδέσεων. Το εύρος ζώνης του «ηλεκτρονικού εμπορίου» εκτείνεται από τις ηλεκτρονικές αγορές έως τις ηλεκτρονικές ιεραρχίες και περιλαμβάνει επίσης ηλεκτρονικά υποστηριζόμενα επιχειρηματικά δίκτυα και συνεργατικές διευθετήσεις (ηλεκτρονικά δίκτυα). Ο μηχανισμός συντονισμού της αγοράς είναι το κοινό τους χαρακτηριστικό. Οι υπηρεσίες στον τομέα του τουρισμού, της χρηματοδότησης ή της ασφαλιστικής βιομηχανίας, αλλά

και η διανομή προϊόντων και οι υπηρεσίες πελατών αποτελούν τυπικά πεδία εφαρμογής. Η οριοθέτηση μεταξύ των διαφόρων μορφών ηλεκτρονικών αγορών γίνεται ακόμα πιο δύσκολη, καθώς:

- Τα οργανωτικά όρια μεταβάλλονται ή εξαφανίζονται και, ως μορφές συντονισμού της αγοράς, μπορούν επίσης να βρουν μια θέση μέσα στις ίδιες τις οργανώσεις.
- Οι αλυσίδες προστιθέμενης αξίας αλλάζουν και οι δραστηριότητες προστιθέμενης αξίας διανέμονται πρόσφατα.
- Οι πελάτες γίνονται μέρος της αλυσίδας προστιθέμενης αξίας και οι ιδιώτες πολίτες γίνονται επιχειρηματίες από μόνα τους.

Η ηλεκτρονική ανταλλαγή δεδομένων (EDI) και το ηλεκτρονικό ταχυδρομείο, για παράδειγμα, αποτελούν κεντρικά επιχειρηματικά εργαλεία που στηρίζουν τη λειτουργία του ηλεκτρονικού εμπορίου. Ωστόσο, είναι αδύνατο να πραγματοποιηθεί συναλλαγή μέσω της EDI χωρίς συμβατική συμφωνία. Τόσο το EDI όσο και το ηλεκτρονικό ταχυδρομείο σήμερα μπορούν να θεωρηθούν υπηρεσίες δικτύου προστιθέμενης αξίας και επιτρέπουν στον χρήστη να υποκαταστήσει ηλεκτρονικά έντυπα για τους ομολόγους τους με βάση το χαρτί (Koponen, 2006).

1.2. Πλεονεκτήματα και μειονεκτήματα του Ηλεκτρονικού εμπορίου

Πλεονεκτήματα του ηλεκτρονικού εμπορίου

Μια επιχείρηση μπορεί να χρησιμοποιήσει το ηλεκτρονικό εμπόριο για να φτάσει σε στενά τμήματα της αγοράς που είναι ευρέως διάσπαρτα γεωγραφικά. Το διαδίκτυο και ο ιστός είναι ιδιαίτερα χρήσιμα στη δημιουργία εικονικών κοινοτήτων που γίνονται ιδανικές αγορές-στόχοι.

Μια εικονική κοινότητα είναι μια συλλογή ανθρώπων που έχουν κοινό συμφέρον, αλλά αντί για αυτή τη συλλογή που συμβαίνει στον φυσικό κόσμο, γίνεται στο διαδίκτυο. Ακριβώς όπως το ηλεκτρονικό εμπόριο αυξάνει τις ευκαιρίες πώλησης για τον πωλητή, αυξάνει τις δυνατότητες αγοράς για τον αγοραστή. Οι επιχειρήσεις μπορούν να χρησιμοποιούν το ηλεκτρονικό εμπόριο στις διαδικασίες αγορών τους για τον εντοπισμό νέων προμηθευτών και επιχειρηματικών συνεργατών. Η διαπραγμάτευση των τιμών και

των όρων παράδοσης είναι ευκολότερη στο ηλεκτρονικό εμπόριο, επειδή ο ιστός μπορεί να προσφέρει ανταγωνιστικές προσφορές πολύ αποτελεσματικά. Το ηλεκτρονικό εμπόριο αυξάνει την ταχύτητα και την ακρίβεια με την οποία οι επιχειρήσεις μπορούν να ανταλλάσσουν πληροφορίες, γεγονός που μειώνει το κόστος και στις δύο πλευρές των συναλλαγών. Το ηλεκτρονικό εμπόριο παρέχει στους αγοραστές ευρύτερο φάσμα επιλογών από το παραδοσιακό εμπόριο, επειδή μπορούν να εξετάσουν πολλά διαφορετικά προϊόντα και υπηρεσίες από μια ευρύτερη ποικιλία πωλητών.

Τα οφέλη του ηλεκτρονικού εμπορίου επεκτείνονται επίσης στη γενική ευημερία της κοινωνίας. Οι ηλεκτρονικές πληρωμές επιστροφής φόρου, δημόσιας συνταξιοδότησης και κοινωνικής υποστήριξης κοστίζουν λιγότερο για την έκδοση και την άφιξη με ασφάλεια και γρήγορα όταν μεταδίδονται μέσω του Διαδικτύου. Επιπλέον, οι ηλεκτρονικές πληρωμές μπορούν να ελέγχονται και να ελέγχονται ευκολότερα από τις πληρωμές που πραγματοποιούνται με επιταγή, οι οποίες μπορούν να βοηθήσουν στην προστασία από τις απάτες και τις απώλειες κλοπής. Το ηλεκτρονικό εμπόριο μπορεί να προσφέρει προϊόντα και υπηρεσίες σε απομακρυσμένες περιοχές. Για παράδειγμα, η εξ αποστάσεως εκπαίδευση επιτρέπει στους ανθρώπους να μαθαίνουν δεξιότητες και να κερδίζουν βαθμούς ανεξάρτητα από τον τόπο κατοικίας τους ή τις ώρες της ημέρας που έχουν στη διάθεσή τους για σπουδές.

Τα μειονεκτήματα του ηλεκτρονικού εμπορίου

Είναι δύσκολο να διεξάγονται ηλεκτρονικά μερικές επιχειρήσεις. Για παράδειγμα, φθαρτά τρόφιμα και αντικείμενα υψηλού κόστους όπως κοσμήματα ή αντίκες μπορεί να είναι αδύνατο να επιθεωρούνται επαρκώς από μια απομακρυσμένη τοποθεσία, ανεξάρτητα από τις τεχνολογίες που σχεδιάζονται στο μέλλον. Ωστόσο, τα περισσότερα από τα μειονεκτήματα του ηλεκτρονικού εμπορίου σήμερα οφείλονται στο νέο χαρακτήρα και στον ταχύ ρυθμό ανάπτυξης των βασικών τεχνολογιών. Η απόδοση των αριθμών των επενδύσεων είναι δύσκολο να υπολογιστεί για επενδύσεις στο ηλεκτρονικό εμπόριο, επειδή το κόστος και τα οφέλη είναι δύσκολο να ποσοτικοποιηθούν. Το κόστος, το οποίο αποτελεί συνάρτηση της τεχνολογίας, μπορεί να αλλάξει δραματικά κατά τη διάρκεια ακόμη βραχύβιων έργων υλοποίησης ηλεκτρονικού εμπορίου, καθώς οι βασικές τεχνολογίες αλλάζουν ταχύτατα. Εκτός από τα τεχνολογικά ζητήματα, πολλές επιχειρήσεις αντιμετωπίζουν πολιτιστικά και νομικά εμπόδια στο ηλεκτρονικό εμπόριο.

Μερικοί καταναλωτές εξακολουθούν να ανησυχούν για την αποστολή των αριθμών πιστωτικών καρτών μέσω του Διαδικτύου. Οι συναλλαγές μεταξύ αγοραστών και πωλητών στο ηλεκτρονικό εμπόριο περιλαμβάνουν αιτήματα για πληροφορίες, αναφορές τιμών, τοποθέτηση παραγγελιών και πληρωμών και υπηρεσίες μετά την πώληση.

1.3. Τεχνολογίες ηλεκτρονικού εμπορίου

Αρκετές τεχνολογίες είναι απαραίτητες για το ηλεκτρονικό εμπόριο. Το πιο προφανές είναι το διαδίκτυο. Πέρα από αυτό το σύστημα διασυνδεδεμένων δικτύων, απαιτούνται πολλά άλλα εξελιγμένα στοιχεία λογισμικού και υλικού για την παροχή της απαιτούμενης δομής υποστήριξης: λογισμικό βάσης δεδομένων, διακόπτες και διανομείς δικτύου, υλικό και λογισμικό κρυπτογράφησης, υποστήριξη πολυμέσων και παγκόσμιος ιστός. Οι μέθοδοι σύνδεσης όλων των στοιχείων του λογισμικού και του υλικού με τον σωστό τρόπο υποστήριξης του ηλεκτρονικού εμπορίου αλλάζουν και εξελίσσονται καθημερινά.

Ο ρυθμός αλλαγής είναι γρήγορος για όλα τα στοιχεία που υποστηρίζουν το ηλεκτρονικό εμπόριο. Κάθε επιχείρηση που ασχολείται με το ηλεκτρονικό εμπόριο και ελπίζει να ανταγωνιστεί στο μέλλον πρέπει να προσαρμοστεί στις νέες τεχνολογίες Διαδικτύου μόλις αυτές γίνουν διαθέσιμες. Η αναμενόμενη υπερφόρτωση του ηλεκτρονικού εμπορίου απαιτεί από τις εταιρείες να βρουν γρηγορότερους και αποτελεσματικότερους τρόπους αντιμετώπισης της συνεχώς αυξανόμενης βιασύνης των online αγοραστών και της αυξανόμενης κίνησης μεταξύ των επιχειρήσεων.

1.4. Χαρακτηριστικά των τεχνολογιών του ηλεκτρονικού εμπορίου

Τα ακόλουθα είναι τα χαρακτηριστικά των τεχνολογιών ηλεκτρονικού εμπορίου:

Ευκολία αυτοματοποιημένης επεξεργασίας: Ο πληρωτής μπορεί τώρα να αυτοματοποιήσει εύκολα την παραγωγή και την επεξεργασία πολλαπλών πληρωμών με ελάχιστη προσπάθεια και κόστος. Στα προηγούμενα χρόνια η εξάρτηση από τις τράπεζες να χειρίζονται τις περισσότερες πληρωμές και η έλλειψη μιας φθηνής, πανταχού

παρουσίας τεχνολογίας επικοινωνιών που καθιστά την αυτοματοποίηση των διαδικασιών πληρωμής δαπανηρή και δύσκολη.

Αμέλεια του αποτελέσματος: Η άμεση πληρωμή προκύπτει εξαιτίας της αυτοματοποίησης και της ικανότητας των ενδιάμεσων συστημάτων και παρόχων να επεξεργάζονται τις πληρωμές σε πραγματικό χρόνο. Στα χειροκίνητα συστήματα με βάση το χαρτί υπάρχει μια χρονική καθυστέρηση λόγω της απαίτησης της ανθρώπινης παρέμβασης στη διαδικασία. 2.1c Διαφάνεια και προσβασιμότητα: Η διαθεσιμότητα φτηνών τεχνολογιών πληροφορικής και επικοινωνιών και το κατάλληλο λογισμικό επιτρέπουν σε μικρές επιχειρήσεις και άτομα να έχουν πρόσβαση ή να παρέχουν ένα φάσμα υπηρεσιών πληρωμών που προηγουμένως ήταν διαθέσιμες μόνο σε μεγάλους οργανισμούς μέσω ειδικών δικτύων ή μονάδων επεξεργασίας συναλλαγών των τραπεζών(Koponen, 2006).

• παρέχει χρήσιμες πληροφορίες για τα συμφραζόμενα για ένα ή περισσότερα από τα μέρη της συναλλαγής. Οι πληροφορίες για τις εξασφαλίσεις μπορούν να περιλαμβάνουν πολλά πράγματα που κυμαίνονται από τόνο φωνής σε τηλεφωνική κλήση στις επαγγελματικές κάρτες και επιστολόχαρτα και εμφανή εξουσία του ατόμου με τον οποίο ασχολείται η επιχείρηση. Δεδομένου ότι οι πληροφορίες λαμβάνονται μόνο μέσω ενός μόνο καναλιού (όπως ηλεκτρονικού μηνύματος) σε ηλεκτρονικά συστήματα, απαιτούνται νέες διαδικασίες για την υποστήριξη και ενίσχυση των πληρωμών με τον ίδιο τρόπο όπως τα χειροκίνητα συστήματα.

Παγκοσμιοποίηση: Η παγκοσμιοποίηση ή η ελαχιστοποίηση των γεωγραφικών παραγόντων κατά τη διενέργεια πληρωμών αποτελεί προφανή πτυχή των νέων συστημάτων πληρωμών. Οι επιπτώσεις της αφορούν τομείς όπως το μέγεθος της αγοράς πληρωμών, η αβεβαιότητα ως προς τη νομική δικαιοδοσία σε περίπτωση διαφορών, η θέση και η διαθεσιμότητα των διαδρομών συναλλαγών και η δυνατότητα ενός καθεστώτος πληρωμών να προσαρμόζεται ταχέως στα ρυθμιστικά καθεστώτα που επιβάλλει μια χώρα μετακινώντας σε άλλο.

*1.5. **Αντιληπτός κίνδυνος (καταναλωτής)***

Ο αντιληπτός κίνδυνος είναι μια έννοια που χρησιμοποιείται για την κατανόηση των στάσεων των καταναλωτών. Σε αυτό το τμήμα της εργασίας θα παρουσιαστούν οι διαστάσεις του αντιληπτού κινδύνου, τα αποτελέσματα του αντιληπτού κινδύνου και του λιανικού εμπορίου στο διαδίκτυο και ο αντιληπτός κίνδυνος (Davis, 1989).

Σύμφωνα με έρευνα της Bauer, "η καταναλωτική συμπεριφορά συνεπάγεται κίνδυνο, υπό την έννοια ότι οποιαδήποτε ενέργεια ενός καταναλωτή θα προκαλέσει συνέπειες τις οποίες δεν μπορεί να προβλέψει με κάτι που να προσεγγίζει την βεβαιότητα και μερικές από τις οποίες τουλάχιστον είναι πιθανό να είναι δυσάρεστες". Ο κίνδυνος θεωρείται ως προϊόν δύο διαστάσεων: οι αντιληπτές (αρνητικές) συνέπειες της συμπεριφοράς και η πιθανότητα εμφάνισής τους (Cox, 1967, Dowling, 1986).

Με βάση τις πληροφορίες που υποβλήθηκαν υποτίθεται ότι η αυξημένη πληροφόρηση θα μειώσει την αβεβαιότητα και επομένως θα μειώσει τον αντιληπτό κίνδυνο. Ένα από τα συμπεράσματα μιας μελέτης που διεξήχθη από τον Cunningham ήταν ότι «η σύνθεση του αντιληπτού κινδύνου που ποικίλλει ανά προϊόν τόσο ως προς το σχετικό βάρος των συνεπειών όσο και ως προς τις μεταβλητές αβεβαιότητας και ως προς τη διακύμανση για καθεμία από αυτές τις μεταβλητές» (Cox, 1967 : 91).

Οι Dowling και Staelin (1994) υποθέτουν ότι ο αντιληπτός κίνδυνος περιλαμβάνει το "μέγεθος των συνεπειών και τις πιθανότητες ότι αυτές οι συνέπειες μπορεί να προκύψουν αν αποκτηθεί το προϊόν". Υπάρχει έλλειψη συνεπούς προσδιορισμού των διαστάσεων του αντιληπτού κινδύνου μεταξύ των μελετών.

Σύμφωνα με τον Dowling (1986) ο αριθμός και οι τύποι ζημιών επηρεάζονται από τον τύπο προϊόντος, τον ερωτώμενο και την κατάσταση αγοράς. Έχουν εντοπιστεί πέντε κύριες διαστάσεις κινδύνου του αντιληπτού κινδύνου:

1. Απόδοση
2. Οικονομική
3. Κοινωνική

4. Ψυχολογική
5. Φυσικός Κίνδυνος

(Cox, 1967, Stone and Gronhaug, 1993, Tsiros and Heilman, 2005),

Ο Mitchell (2001) χρησιμοποίησε 4 διαστάσεις: φυσικό κίνδυνο, οικονομικό κίνδυνο, χρόνο και ο κίνδυνος ευκολίας και ο ψυχοκοινωνικός κίνδυνος στην έρευνά του που παρουσίασε ένα νέο εννοιολογικό πλαίσιο για την εικόνα του καταστήματος χρησιμοποιώντας τον αντιληπτό κίνδυνο.

Οι Sharma et al., (2009) χρησιμοποίησαν τρεις τύπους μεταβλητών κινδύνου για τον καταναλωτή - στάση ανάληψης κινδύνου από τους καταναλωτές, εκτίμηση της επικινδυνότητας χρησιμοποιώντας 5 από τις διαστάσεις κινδύνου και τη συνειδητοποίηση των τιμών στην έρευνα για να εκφράσουν τον αντιληπτό κίνδυνο ως υψηλότερη σειρά μεταβλητών κινδύνου για τον καταναλωτή).

Η έρευνα που διεξήχθη από τους Dowling και Staelin (1994) υποθέτει ότι η συμμετοχή του πελάτη στην απόφαση αγοράς θα επηρεάσει τον αντιληπτό κίνδυνο αυτού του προϊόντος. Αναγνωρίστηκαν τρεις κατηγορίες συμμετοχής:

1) η συμμετοχή του

2) η συμμετοχή στην αγορά και

3) η συμμετοχή του προϊόντος. Οι Stone και Gronhaug (1993) εξέτασαν τον αντιληπτό κίνδυνο ως μεσολαβητή του ατομικού ψυχολογικού κινδύνου για να επηρεάσουν τον συνολικό κίνδυνο.

Η έρευνα διεξήχθη με τη χρήση πληροφοριών αγοράς ενός προσωπικού υπολογιστή, επειδή θεωρήθηκε ότι ήταν μια "επικίνδυνη", πολύπλοκη και δαπανηρή αγορά. Τα ευρήματα της έρευνας κατέληξαν στο συμπέρασμα ότι και οι πέντε διαστάσεις κινδύνου αλληλεπικαλύπτονται θετικά με τη μεταβλητή κριτηρίων, αλλά η συνεισφορά στο συνολικό κίνδυνο ποικίλλει σε μεγάλο βαθμό. Τα στοιχεία έδειξαν ότι οι οικονομικοί και ψυχολογικοί κίνδυνοι ήταν οι κυριότεροι και ότι ο ψυχολογικός κίνδυνος είναι μια σημαντική διαμεσολαβητική λειτουργία για άλλους τύπους κινδύνου. (Shulmanetal. , 2011).

Οι Dowling και Staelin (1994) εξέτασαν την ψυχολογική δομή του αποδεκτού κινδύνου ως συντονιστή της σχέσης μεταξύ του ειδικού για το προϊόν αντιλαμβανόμενου κινδύνου και της χρήσης πρόσθετων δραστηριοτήτων μείωσης του κινδύνου, η έρευνα διεξήχθη χρησιμοποιώντας πληροφορίες αγοράς νέων φορεμάτων.

Ο Sweeney et al (1999) εξέτασε τον αντιληπτό κίνδυνο ως μεσολαβητή της σχέσης μεταξύ των διαφόρων ποιοτικών συνιστωσών και της εκτιμώμενης αξίας για το χρήμα, τα συμπεράσματα από τη μελέτη κατέληξαν στο συμπέρασμα ότι ο αντιληπτός κίνδυνος είναι ένας μεσολαβητής της σχέσης για την ποιότητα των προηγούμενων.

Οι μελλοντικές έρευνες δείχνουν ότι πρέπει να συμπεριληφθούν σε μελέτες πολλαπλά προϊόντα και κατηγορίες προϊόντων για να αυξηθεί η γενίκευση της έννοιας του κινδύνου. (Dowling, 1986 · Dowling and Staelin, 1994 · Stone and Gronhaug, 1993 · Sweeney et al., 1999)

Σύμφωνα με τον Dowling (1986), δεν υπάρχει αρκετή θεωρητική εξέλιξη του αντιληπτού κινδύνου "χωρίς κατάλληλο μοντέλο της διαδικασίας που δημιουργεί κίνδυνο η αντίληψη και η παρέμβαση μεταξύ αυτής της δομής και της συμπεριφοράς, αποδίδοντας σημασία στις εμπειρικές συσχετίσεις είναι δύσκολη».

Ο Tong (2010) προτείνει ότι είναι ζωτικής σημασίας για τους εμπόρους να ελαχιστοποιούν τους κινδύνους που οι καταναλωτές αισθάνονται όταν κάνουν αγορές μέσω διαδικτύου. Πολλά άρθρα υποδηλώνουν ότι οι αντιληπτοί κίνδυνοι συνδέονται με την αγορά διαδικτυακών εμπορευμάτων, αλλά δεν διερευνούν την άμεση σχέση μεταξύ του αντιληπτού κινδύνου και της αποτυχίας ολοκλήρωσης μιας συναλλαγής (εγκατάλειψη του καλαθιού αγορών). Είναι απαραίτητο οι έμποροι που δραστηριοποιούνται στο διαδίκτυο να κατανοήσουν τον κίνδυνο που νιώθει κάποιος, όταν αγοράζει εμπορεύματα στο διαδίκτυο, προκειμένου να μειωθεί η εγκατάλειψη του καλαθιού αγορών.

Ο Liljander et al., (2009) ερεύνησε την εικόνα του καταστήματος ως παράγοντα μείωσης του κινδύνου χρησιμοποιώντας την έννοια του αντιληπτού κινδύνου. Η έρευνά

τους κατέληξε στο συμπέρασμα ότι σε ορισμένες κατηγορίες προϊόντων, όπως είναι τα είδη ένδυσης, οι αγορές πιθανώς επηρεάζονται από τον αντιληπτό ψυχολογικό κίνδυνο, τον λειτουργικό κίνδυνο και τον οικονομικό κίνδυνο.

Οι Campbell και Goodstein (2001) διαπίστωσαν ότι ο υψηλότερος αντιληπτός κίνδυνος αναστέλλει τις εξερευνητικές τάσεις, οδηγώντας στην προτίμηση του κανόνα απέναντι στο μυθιστόρημα. μπορεί να θεωρηθεί ότι η διαδικτυακή λιανική πώληση μπορεί να είναι καινοφανής όταν ο πελάτης δεν διαθέτει τεχνογνωσία. Ο Tong (2010) ανέφερε ότι η πιθανότητα αγοράς στο Διαδίκτυο μειώνεται καθώς οι καταναλωτές αντιλαμβάνονται την αύξηση του κινδύνου σε σχέση με την τεχνολογία. Η έρευνα έχει δείξει ότι η έννοια του αντιληπτού κινδύνου είναι χρήσιμη για τον προσδιορισμό των μελλοντικών προθέσεων αγοράς, οι οποίες μπορούν να αποτελέσουν χρήσιμο στοιχείο για την κατανόηση της εγκατάλειψης του καλαθιού αγορών (Petersen and Kumar, 2009).

ΚΕΦΑΛΑΙΟ 2- ΑΣΦΑΛΕΙΑ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

2.1. Η σημασία της ασφάλειας στο Ηλεκτρονικό Εμπόριο

Η ασφάλεια στο ηλεκτρονικό εμπόριο είναι ένα κομμάτι του πλαισίου ασφάλειας πληροφοριών και εφαρμόζεται ειδικά στα συστατικά στοιχεία που επηρεάζουν το ηλεκτρονικό εμπόριο που περιλαμβάνει την ασφάλεια υπολογιστών, την ασφάλεια των δεδομένων. Το ηλεκτρονικό εμπόριο χρειάζεται εξαρτήματα υψηλής ασφάλειας που επηρεάζουν τον τελικό χρήστη μέσω της καθημερινής αλληλεπίδρασης πληρωμής με τις επιχειρήσεις. Το ηλεκτρονικό εμπόριο απαιτούσε μια αξιόπιστη υποδομή και ένα πλαίσιο που θα επέτρεπε ένα ασφαλές και επιτυχημένο ηλεκτρονικό εμπόριο. Σήμερα, η προστασία και η ασφάλεια είναι μια αξιοσημείωτη ανησυχία για τις ηλεκτρονικές τεχνολογίες, για παράδειγμα, το M-commerce (Mobile-Commerce) μοιράζεται τις ανησυχίες για την ασφάλεια με άλλες και ενώσεις που ασχολούνται με το ηλεκτρονικό εμπόριο (Closeetal, 2012).

Στις εφαρμογές ηλεκτρονικού εμπορίου του Διαδικτύου που χειρίζονται πληρωμές, όπως η ηλεκτρονική αποθήκευση χρημάτων, οι ηλεκτρονικές ανταλλαγές ή οι χρεωστικές κάρτες, οι πιστωτικές κάρτες, το PayPal, το ηλεκτρονικό χρήμα, οι προπληρωμένες κάρτες, οι κάρτες πλοήγησης, οι κάρτες βίζας ή άλλες μάρκες. Έχουν ανακαλυφθεί ανησυχίες σχετικά με την προστασία, αποκαλύπτοντας την απουσία εμπιστοσύνης σε ποικίλα πλαίσια, όπως το εμπόριο, τα ηλεκτρονικά αρχεία υγείας, την τεχνολογία ηλεκτρονικής προσέλκυσης και τη διαπροσωπική επικοινωνία μεγάλης εμβέλειας και αυτό επηρέασε άμεσα τους χρήστες. Η ασφάλεια είναι μια από τις πιο σημαντικές μεταβλητές που περιορίζουν τους πελάτες και τις ενώσεις που ασχολούνται με το ηλεκτρονικό εμπόριο και το ηλεκτρονικό εμπόριο που επί του παρόντος αντιμετωπίζουν σταδιακά τα ζητήματα ασφάλειας στα εσωτερικά τους δίκτυα. Υπάρχουν τέτοιου είδους οδηγίες για την εξασφάλιση συστημάτων και δικτύων που είναι διαθέσιμα στο προσωπικό του συστήματος ηλεκτρονικού εμπορίου για να το διαβάσουν και να το εφαρμόσουν. Δεδομένου ότι μεγάλο μέρος των πελατών χρησιμοποιούν τις ηλεκτρονικές αγορές, κάποιοι είναι εγγράφων και άλλοι είναι αναλφάβητοι, με αποτέλεσμα η

εκπαίδευση του καταναλωτή σε ζητήματα ασφάλειας να βρίσκεται ακόμη στα αρχικά στάδια.

Ωστόσο, θα αποδειχθεί το πιο βασικό στοιχείο της αρχιτεκτονικής ασφάλειας του ηλεκτρονικού εμπορίου. Οι ιοί, τα σκουλήκια, τα προγράμματα των δούλων του Δούρειου Ίππου που ξεκίνησαν ενάντια στα συστήματα των πελατών αποτελούν τη μεγαλύτερη απειλή για το ηλεκτρονικό εμπόριο, διότι μπορούν να παρεμποδίσουν ή να ανατρέψουν το μεγαλύτερο μέρος των μηχανισμών ελέγχου ταυτότητας και έγκρισης που χρησιμοποιούνται σε ένα ηλεκτρονικό εμπόριο. Αυτά τα έργα μπορούν να εγκατασταθούν σε απομακρυσμένο υπολογιστή με τα πιο απλά μέσα: συνημμένα ηλεκτρονικού ταχυδρομείου(Closeetal, 2012).

Επομένως, ορισμένα προσωπικά δεδομένα έχουν καταστεί αξιοσημείωτο μέλημα για τους καταναλωτές με την αύξηση της κλοπής ταυτότητας και της πλαστοπροσωπίας και κάθε ανησυχία για τους καταναλωτές πρέπει να αντιμετωπιστεί ως μια αξιοσημείωτη ανησυχία για τους παρόχους ηλεκτρονικού εμπορίου. Η γρήγορη εξέλιξη των διαδικτυακών και κινητών διαύλων έχει αποκαλύψει νέες αγορές και έφερε τεράστιες ευκαιρίες τόσο σε αναδυόμενους όσο και σε καθιερωμένους οργανισμούς. Την προηγούμενη δεκαετία παρατηρήθηκε επίσης αξιοσημείωτη διακοπή στις διαδικασίες και στα συστήματα πληρωμών ηλεκτρονικού εμπορίου. Η διασυνδεδεμένη, μυστηριώδης και στιγμιαία φύση αυτών των καναλιών έχει αναπόφευκτα οδηγήσει στην ανάπτυξη αδικημάτων εναντίον των επιχειρήσεων ηλεκτρονικού εμπορίου και λιανικών υπηρεσιών, των ανθρώπων και των πελατών τους.

Αυτές οι απειλές ηλεκτρονικού εγκλήματος και μηχανογραφημένες ψευδείς αντιπαραθέσεις συνεχίζουν να εξελίσσονται γρήγορα, με τους επιτιθέμενους να χρησιμοποιούν ολοένα και πιο εξελιγμένες τεχνικές για να στοχεύουν τις ευπάθειες στους ανθρώπους, τις διαδικασίες και τις τεχνολογίες. Οι απειλές κατά του ηλεκτρονικού εγκλήματος, εάν υλοποιηθούν με επιτυχία, μπορούν να υπονομεύσουν τις βασικές προηγμένες υπηρεσίες, να προκαλέσουν αξιοσημείωτες βλάβες στην αξιοπρέπεια και να οδηγήσουν σε σημαντικά κρατικά και λειτουργικά βάσανα για τις ενώσεις και τους πελάτες τους. Για να επιτευχθούν οι στόχοι ασφαλείας, είναι απαραίτητο να αναγνωριστεί ότι η ασφάλεια των υπηρεσιών και η προστασία των πληροφοριών των πελατών είναι ουσιώδεις. Για το σκοπό αυτό, και ειδικά για να βοηθήσουμε την

τρέχουσα εξίσωση ασφαλείας, είναι απαραίτητο να έχουμε ένα ευρύ μοντέλο ασφάλειας για τους πελάτες (Shazia,2012).

Αυτό θα έπρεπε να σχεδιαστεί για να προσφέρει βελτιώσεις στις δυνατότητες ασφαλείας των πελατών και των υπηρεσιών back office, και συγκεκριμένα να βελτιώσει τις υπάρχουσες αμυντικές υπηρεσίες ασφαλείας για απομακρυσμένα διαδικτυακά, τηλεφωνικά και κινητά κανάλια διανομής χρημάτων. Η ασφάλεια είναι ένα από τα κύρια και προχωρά με ανησυχίες που περιορίζουν τους πελάτες και τις ενώσεις που ασχολούνται με το ηλεκτρονικό εμπόριο.

Το σημείο αυτής της εργασίας είναι να διερευνήσει την αντίληψη της ασφάλειας στις ιστοσελίδες ηλεκτρονικού εμπορίου B2C και C2C τόσο από τις πελατειακές όσο και από τις έγκυρες προοπτικές. Με την ταχεία ανάπτυξη του ηλεκτρονικού εμπορίου, τα θέματα ασφάλειας εξέρχονται από την προσοχή των ανθρώπων. Η ασφάλεια της ανταλλαγής είναι ο πυρήνας και τα βασικά ζητήματα της ανάπτυξης του ηλεκτρονικού εμπορίου. Το παρόν έγγραφο σχετικά με τα θέματα ασφάλειας των δραστηριοτήτων ηλεκτρονικού εμπορίου θέτει στρατηγική ρύθμισης από δύο πτυχές που είναι η τεχνολογία και το σύστημα, η βελτίωση του περιβάλλοντος για την ανάπτυξη του ηλεκτρονικού εμπορίου και η προώθηση της περαιτέρω ανάπτυξης του ηλεκτρονικού εμπορίου.

Οι εφαρμογές Web ενσωματώνουν ολοένα και περισσότερο τις υπηρεσίες outsider. Η ολοκλήρωση εισάγει νέες προκλήσεις ασφάλειας λόγω της πολυπλοκότητας μιας εφαρμογής για τον συντονισμό των εσωτερικών κρατών με τις υπηρεσίες των συστατικών υπηρεσιών και του διαδικτυακού πελάτη μέσω του Διαδικτύου. Το ηλεκτρονικό εμπόριο προσφέρει μια μεγάλη ευκαιρία για τη διαχείριση μιας βιομηχανίας λογαριασμού, αλλά επιπλέον δημιουργεί μια σειρά νέων κινδύνων και ευπάθειας, για παράδειγμα, απειλές για την ασφάλεια. Ως εκ τούτου, η ασφάλεια των δεδομένων αποτελεί βασική διαχείριση chnical απαίτηση για οποιαδήποτε αποτελεσματική και αποτελεσματική δραστηριότητες ανταλλαγής πληρωμών μέσω του Διαδικτύου. Εν πάση περιπτώσει, ο ορισμός του είναι μια πολύπλοκη προσπάθεια λόγω των σταθερών τεχνολογικών και επιχειρηματικών αλλαγών και απαιτεί συντονισμένο συνδυασμό υπολογισμών και τεχνικών ρυθμίσεων(Shazia,2012).

2.2. Θέματα ασφάλειας ηλεκτρονικού εμπορίου

Η ασφάλεια ηλεκτρονικού εμπορίου είναι η προστασία των περιουσιακών στοιχείων του ηλεκτρονικού εμπορίου από μη εξουσιοδοτημένη πρόσβαση, χρήση, μετατροπή ή καταστροφή. Οι καταναλωτές φοβούνται την απώλεια των δημοσιονομικών τους πληροφοριών και οι ιστότοποι ηλεκτρονικού εμπορίου φοβούνται τις απώλειες που συνδέονται με τα χρήματα που συνδέονται με τυχόν φαινομενικά τρομερή έκθεση και θραύσματα. Υπάρχουν ορισμένα βασικά κοινωνικά και έγκυρα θέματα με ασφάλεια. Το πρώτο είναι η ανάπτυξη επαρκών έγκυρων διαδικασιών για τη διαχείριση τυχόν ευκαιριών, η ανάπτυξη πολιτικών ασφάλειας και ο διαχωρισμός των καθηκόντων, η διασφάλιση της ασφάλειας και ο έλεγχος πρόσβασης (Bascar, 2015).

Το δεύτερο είναι ότι η αδύναμη σύνδεση στην ασφάλεια είναι συχνά υπάλληλοι ή χρήστες, αντί της τεχνολογίας και η τρίτη είναι η διαχείριση λογισμικού ή η επίβλεψη του τρόπου με τον οποίο αναπτύσσεται η τεχνολογία ασφάλειας. Ένα επίμονο πρόβλημα είναι οι διαφορετικοί και λανθασμένοι τύποι ασφαλείας των χρηστών και η φαινομενική απροθυμία τους ή η μη τήρηση των βασικών πολιτικών και οδηγιών ασφαλείας. Για παράδειγμα, οι χρήστες μπορούν να αποθηκεύουν κωδικούς πρόσβασης σε μη κρυπτογραφημένα αρχεία σε ευάλωτες μηχανές ή οι υπάλληλοι μπορούν να αποκαλύψουν τους κωδικούς τους σε εξωτερικούς συνεργάτες.

 Μη εξουσιοδοτημένη πρόσβαση: Υπονοεί την παράνομη πρόσβαση σε πληροφορίες, συστήματα ή εφαρμογές για κάποιο κακόβουλο σκοπό. Στην παθητική μη εξουσιοδοτημένη πρόσβαση ο χάκερ ακούει κανάλια αλληλογραφίας για την ανακάλυψη μυστικών ή περιεχομένου που μπορεί να χρησιμοποιηθεί για βλάβη. Ωστόσο, στην ενεργή μη εξουσιοδοτημένη πρόσβαση, ο hacker τροποποιεί το σύστημα ή τις πληροφορίες με πρόθεση να χειριστεί ή να αλλάξει.

 Άρνηση παροχής υπηρεσιών: Μπορεί να συμβεί με spamming και ιούς. Το spam είναι ουσιαστικά εκπληκτικό το κτύπημα ηλεκτρονικού ταχυδρομείου που προκαλείται από έναν χάκερ που στοχεύει έναν υπολογιστή ή δίκτυο και στέλνει μεγάλο αριθμό μηνυμάτων ηλεκτρονικού ταχυδρομείου σε αυτόν. Οι επιθέσεις DDOS (Distributed Denial of Service Attacks) περιλαμβάνουν τους hackers που θέτουν πράκτορες λογισμικού σε μια σειρά από συστήματα outsider και τους απενεργοποιούν ώστε να στέλνουν αιτήματα ταυτόχρονα σε έναν επιδιωκόμενο στόχο. Ωστόσο, οι ιοί είναι αυτοκαταναλωτικά προγράμματα υπολογιστών σχεδιασμένα να εκτελούν ανεπιθύμητα συμβάντα.

Τα σκουλήκια είναι ειδικοί ιοί που εξαπλώνονται χρησιμοποιώντας απευθείας συνδέσεις στο Διαδίκτυο και οι Trojan Horses μεταμφιέζονται ως νόμιμο λογισμικό που παγιδεύει τους χρήστες για να εκτελέσει το πρόγραμμα.

 Κλοπή και απάτη: Οι ψευδείς δηλώσεις συμβαίνουν όταν χρησιμοποιούνται ή τροποποιούνται οι κλεμμένες πληροφορίες. Η κλοπή λογισμικού συνεπάγεται παράνομη αναπαραγωγή από διακομιστές του οργανισμού ή κλοπή υλικού, συγκεκριμένα υπολογιστών. Οι χάκερ σπάνε σε ανασφαλείς εμπορικούς διακομιστές ιστού για να συλλέγουν τα αρχεία των αριθμών πιστωτικών καρτών που αποθηκεύονται γενικά μαζί με τα προσωπικά δεδομένα όταν ένας καταναλωτής πραγματοποιεί online αγορά. Το back-end του εμπόρου και η βάση δεδομένων είναι επιπρόσθετα ευαίσθητα για κλοπή από κέντρα εξωραϊσμού και άλλους φορείς επεξεργασίας(Σερπάνος, 2011).

2.3. Το μοντέλο του ηλεκτρονικού εμπορίου και η ασφάλεια

Τα συστήματα ηλεκτρονικού εμπορίου χρησιμοποιούν τεχνολογίες του Διαδικτύου και καινοτόμες επιχειρησιακές διαδικασίες για την ανάπτυξη εφαρμογών που ξεπερνούν τα παραδοσιακά όρια του χρόνου, του διαστήματος, του οργανισμού και των εδαφικών συνόρων. Στην απλούστερη μορφή του, το αρχιτεκτονικό μοντέλο ενός συστήματος ηλεκτρονικού εμπορίου διαθέτει υποδομή πληροφορικής που υποστηρίζει διαφορετικές βάσεις δεδομένων, διεπαφές χρήστη και εφαρμογές. Μπορεί να περιγραφεί σε λίγο πιο λεπτομερή μορφή ως μοντέλο που αξιοποιεί τις τεχνολογίες Ιστού για την υλοποίηση κρίσιμων για το χρήστη εφαρμογών ηλεκτρονικού επιχειρείν. Αυτό το μοντέλο αρχιτεκτονικής χρησιμοποιεί διαφορετικούς τύπους λεπτών πελατών για την πρόσβαση σε υπηρεσίες που παρέχονται από διαχειριστές πόρων που μπορούν να προσεγγιστούν σε ένα ισχυρό και αξιόπιστο δίκτυο (Niranjanamurthy et al., 2013).

Αυτοί οι μικροί πελάτες μπορούν να χρησιμοποιούν προγράμματα περιήγησης σε προσωπικούς υπολογιστές, συσκευές δικτύου, προσωπικούς ψηφιακούς βοηθούς, κινητά τηλέφωνα και άλλες διάσπαρτες υπολογιστικές συσκευές. Πριν από την εφαρμογή ενός συστήματος ηλεκτρονικού εμπορίου, πρέπει να αντιμετωπιστούν οι διάφορες προκλήσεις ασφάλειας που αντιμετωπίζει ένα τέτοιο σύστημα και τα κύρια συστατικά στοιχεία του ώστε να διασφαλιστεί η διαθεσιμότητα, η επιβιωσιμότητά του και η ασφάλεια και το απόρρητο των δεδομένων που εμπλέκονται στους διάφορους τύπους συναλλαγών.

Η ασφάλεια ηλεκτρονικού εμπορίου είναι η προστασία των περιουσιακών στοιχείων ηλεκτρονικού εμπορίου από μη εξουσιοδοτημένη πρόσβαση, χρήση, μετατροπή ή καταστροφή. Ενώ τα χαρακτηριστικά ασφαλείας δεν εγγυώνται ένα ασφαλές σύστημα, είναι απαραίτητο να δημιουργηθεί ένα ασφαλές σύστημα. Επιπλέον, κανείς δεν θα ασχοληθεί με ένα σύστημα ηλεκτρονικού εμπορίου που ενδέχεται να διανέμει, ευθέως λόγω μιας επίθεσης ασφαλείας, ευαίσθητα δεδομένα καταναλωτών, όπως τον αριθμό της πιστωτικής κάρτας, τις προσωπικές πληροφορίες ή τα οικονομικά στοιχεία και τα στοιχεία του λογαριασμού. Σε ένα πολύ απλουστευμένο σενάριο όπου ο πελάτης χρησιμοποιεί έναν ιστότοπο για ένα σύστημα ηλεκτρονικού εμπορίου και δίνει τον αριθμό της πιστωτικής του κάρτας και πληροφορίες διεύθυνσης, αυτή η απλή on-line συναλλαγή έχει πολλές πιθανές ευπάθειες ασφαλείας που σχετίζονται με τα διάφορα στοιχεία του το οποίο περιλαμβάνει τα εξής(Niranjanamurthy et al., 2013).:

1) Προβλήματα ασφαλείας σε υπολογιστές-πελάτες / οικιακούς υπολογιστές, όπου τα δεδομένα που αποθηκεύονται στο web "cookie" μπορούν να κλαπούν και να ραγίζονται από εχθρικούς ιστότοπους ή από ιούς που μεταδίδονται μέσω ταχυδρομείου που μπορούν να κλέψουν τα οικονομικά δεδομένα του χρήστη από τον τοπικό δίσκο .

2) Υποκλοπές και κλοπή δεδομένων λόγω αναποτελεσματικής κρυπτογράφησης ή έλλειψης κρυπτογράφησης σε οικιακά ασύρματα δίκτυα. 3) Υποκλοπές και κλοπή δεδομένων από τις πληκτρολογήσεις του χρήστη στους τερματικούς σταθμούς PointofSale (POS) σε καταστήματα τούβλων και κονιαμάτων.

4) Υποκλοπές και κλοπή δεδομένων από κινητές και φορητές συσκευές του χρήστη.

5) Υποκλοπές και κλοπή δεδομένων από δίκτυα και διαφορετικές ενδιάμεσες επικοινωνίες. Παρόλο που ορισμένα από τα μέτρα ασφαλείας, όπως η κρυπτογράφηση δεδομένων, ο έλεγχος ταυτότητας και η εξουσιοδότηση, ενδέχεται να αντιμετωπίσουν ορισμένα από τα παραπάνω προβλήματα ασφάλειας. υπάρχουν περισσότερες προκλήσεις ευπάθειας και ασφάλειας που πρέπει να αντιμετωπιστούν σε άλλα μέρη ενός συστήματος ηλεκτρονικών συστημάτων, ειδικά στους πελάτες λογισμικού και στους διακομιστές που πρέπει να χρησιμοποιούν τα δεδομένα.

2.4. Κατηγορίες-Ταξινόμησητων ζητημάτων ασφάλειας του ηλεκτρονικού εμπορίου

Με βάση το μοντέλο αρχιτεκτονικής που παρουσιάζεται στο σχήμα 1, απαιτείται ασφάλεια στα ακόλουθα επίπεδα οποιουδήποτε συστήματος ηλεκτρονικού εμπορίου:

1) Οι διακομιστές front-end , κωδικός

2) Τα συστήματα back-end , θα πρέπει να προστατεύονται

3) Το εταιρικό δίκτυο πρέπει να προστατεύεται από την εισβολή. Για την εφαρμογή της ασφάλειας σε όλα αυτά τα επίπεδα, ένα τυπικό σύστημα ηλεκτρονικού εμπορίου μπορεί να χωριστεί στους ακόλουθους τομείς:

1) Δημόσιο δίκτυο, το οποίο αποτελείται από πελάτες που έχουν πρόσβαση στους διακομιστές front-end και στο Internet.

2) Αποστρατιωτικοποιημένη Ζώνη (DMZ), η οποία αποτελείται από συμπλέγματα διακομιστών front-end και back-end.

3) Εταιρικό δίκτυο. Οι τομείς προστατεύονται ο ένας από τον άλλο χρησιμοποιώντας firewalls.

Οι εξωτερικές επιθέσεις μπορούν να προληφθούν μέσω προστασίας δικτύου, πλατφόρμας, εφαρμογών και βάσεων δεδομένων. Στη συνέχεια, και με βάση την παραπάνω συζήτηση, θα ταξινομήσω τις προκλήσεις ασφάλειας ηλεκτρονικού εμπορίου σε τρία διαφορετικά επίπεδα: Προκλήσεις σε επίπεδο πελάτη, προκλήσεις σε επίπεδο εξυπηρετητών και εφαρμογών λογισμικού Επίπεδο και προκλήσεις στο δίκτυο και πίσω - επεξεργαστές επιπέδου Επίπεδο. Επιπλέον, θα ταξινομήσω και θα συζητήσω τους διάφορους τύπους απειλών ασφάλειας, επιθέσεων και προβλημάτων ευπάθειας που σχετίζονται με κάθε επίπεδο(Singh, 2014).

Α. Προβλήματα ασφάλειας επιπέδου πελάτη

Πολλοί πελάτες χρησιμοποιούν ασύρματες συνδέσεις Internet και κινητές συσκευές για πρόσβαση σε συστήματα ηλεκτρονικού επιχειρείν. Τα ασύρματα δίκτυα και οι κινητές συσκευές παρουσιάζουν κίνδυνο ασφάλειας, καθώς οι εξωτερικοί χρήστες μπορούν να παρακολουθήσουν τις ασύρματες επικοινωνίες. Η εξασφάλιση ασύρματου δικτύου με κωδικό πρόσβασης μπορεί να δυσκολέψει τους εξωτερικούς χρήστες να συνδεθούν στο δίκτυο και να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες, αλλά

μια ασύρματη σύνδεση δεν είναι τόσο ασφαλής όσο μια ενσύρματη σύνδεση, ακόμη και αν έχει προστασία με κωδικό πρόσβασης (Singh, 2014).

Συλλογές και αναμετάδοση μηνυμάτων. Ο επιτιθέμενος μπορεί να συλλάβει ένα πλήρες μήνυμα που έχει την πλήρη πιστοποίηση ενός νόμιμου χρήστη και να το αναπαράγει με κάποια δευτερεύουσα αλλά κρίσιμη τροποποίηση στον ίδιο προορισμό ή σε άλλη για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση και προνομιακή για σημαντικές πληροφορίες [9].

Υποκλοπή.

Αυτό είναι ένα πολύ γνωστό ζήτημα ασφάλειας σε ασύρματα δίκτυα. Εάν το δίκτυο δεν είναι αρκετά ασφαλές και οι μεταδιδόμενες πληροφορίες δεν είναι κρυπτογραφημένες, τότε ένας εισβολέας μπορεί να χάσει στο δίκτυο και να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα. Κινητά Συσκευές Ο εισβολέας ελέγχει την κινητή συσκευή ως πηγή δεδομένων ιδιοτυπίας και πληροφοριών ελέγχου. Τα δεδομένα μπορούν να ληφθούν από την ίδια τη συσκευή μέσω των διασυνδέσεων εξαγωγής δεδομένων, μιας συγχρονισμένης επιφάνειας εργασίας, των κινητών εφαρμογών που εκτελούνται στη συσκευή ή των εξυπηρετητών intranet.

Απώλεια συσκευής:

Η πιθανότητα απώλειας ή κλοπής της συσκευής και καταχρηστικής εκμετάλλευσης από μη εξουσιοδοτημένους χρήστες πρέπει να εξεταστεί με την εφαρμογή ορισμένων μέτρων ασφαλείας, όπως είναι το χαρακτηριστικό προστασίας κωδικού πρόσβασης σε κάθε κινητή συσκευή.

Β. Προσωπικοί διακομιστές και επίπεδο εφαρμογών λογισμικού Προκλήσεις ασφαλείας

Αυτά τα είδη προκλήσεων είναι τα αποτελέσματα της απόκτησης πλεονεκτημάτων από τα υπάρχοντα κενά που υπάρχουν στις περισσότερες εφαρμογές λογισμικού και λογισμικό διακομιστή. Ο επιτιθέμενος εντοπίζει τους τύπους λογισμικού που χρησιμοποιούνται για την ανάλυση του ιστότοπου, την ανίχνευση κενών και την εκμετάλλευση αυτών των κενών στο σύστημα [11]. Οι εκμεταλλεύσεις διακομιστών αναφέρονται σε τεχνικές που αποκτούν πρόσβαση διαχειριστή στον διακομιστή. Αυτό εκμεταλλεύεται τους περισσότερους κινδύνους επειδή ο επιτιθέμενος μπορεί να κάνει απεριόριστες ζημιές. Με την εκμετάλλευση ενός διακομιστή, έχετε πρόσβαση στον

έλεγχο των εμπόρων και όλων των πληροφοριών των αγοραστών σχετικά με τον ιστότοπο και μπορείτε να το χρησιμοποιήσετε προς όφελός σας.

Υπέρβαση του buffer. Οι επιθέσεις υπερχείλισης buffer και η εκτέλεση δέσμης ενεργειών σε ένα διακομιστή είναι δύο μεγάλες επιθέσεις διακομιστών. Σε μια επίθεση υπερχείλισης buffer, ο χάκερ εκμεταλλεύεται συγκεκριμένο τύπο σφάλματος προγράμματος υπολογιστή που περιλαμβάνει την κατανομή αποθήκευσης κατά την εκτέλεση του προγράμματος. Η τεχνική περιλαμβάνει την εξαπάτηση του διακομιστή να εκτελέσει τον κώδικα που γράφει ο εισβολέας.

Σφάλματα / σφάλματα λογισμικού.

Υπάρχουν τρύπες ασφαλείας στα περισσότερα νέα και υπάρχοντα συστήματα λογισμικού, κυρίως λόγω σφαλμάτων λογισμικού / σφαλμάτων που αφέθηκαν από απρόσεκτους ή μη εξειδικευμένους προγραμματιστές ή προγραμματιστές λογισμικού με επίκεντρο την ασφάλεια. Τα συστήματα λογισμικού ηλεκτρονικού εμπορίου πρέπει να είναι διαλειτουργικά και πρέπει να ανταλλάσσουν δεδομένα με συστήματα λογισμικού που ανήκουν και ελέγχονται από άλλους, όπως πελάτες, προμηθευτές, συνεργάτες και άλλοι πράκτορες ή διακομιστές λογισμικού επεξεργασίας.

Επομένως, οι μηχανισμοί ασφαλείας που χρησιμοποιούνται στα συστήματα ηλεκτρονικού εμπορίου πρέπει να είναι ευέλικτοι, να βασίζονται σε πρότυπα και να είναι διαλειτουργικοί με τα συστήματα άλλων. Πρέπει να υποστηρίζουν προγράμματα περιήγησης και να εργάζονται σε πολυεπίπεδες αρχιτεκτονικές με ένα ή περισσότερα μεσαία επίπεδα όπως διακομιστές web και διακομιστές εφαρμογών. Επιπλέον, τα πρότυπα και τα πρωτόκολλα δικτύων και επικοινωνιών βρίσκονται σε κατάσταση συνεχών αλλαγών που καθιστούν δύσκολη την ενημέρωση όλων των συμβουλών ασφαλείας και των ενημερωτικών εκδόσεων ασφαλείας. Οι χάκερ ανακαλύπτουν διαρκώς και κάνουν χρήση αυτών των τρωτών σημείων. Ιοί και άλλο κακόβουλο λογισμικό (Bascar, 2015).

Οι χάκερ μπορούν να χρησιμοποιήσουν ιούς και άλλο κακόβουλο λογισμικό για να μολύνουν τα συστήματα ηλεκτρονικού επιχειρείν και να είναι σε θέση να κλέψουν τις πληροφορίες των πελατών, να προκαλέσουν απώλεια δεδομένων ή να καταστήσουν τα ηλεκτρονικά συστήματα απρόσιτα. Σύμφωνα με τις αναφορές των καταναλωτών, το κακόβουλο λογισμικό κοστίζει στους καταναλωτές περίπου 2,3 δισεκατομμύρια δολάρια το 2010 και ως άλλο παράδειγμα το PlayStation Network της Sony ήταν το θύμα μιας

μεγάλης επιχείρησης πειρατείας το 2011 που είχε ως αποτέλεσμα την κλοπή εκατομμυρίων προσωπικών πληροφοριών των χρηστών10.

Γ. **Δίκτυα και διακομιστές-** Επίπεδα Προκλήσεις Ασφάλειας

Τα δίκτυα έχουν τα δικά τους θέματα ασφαλείας κυρίως λόγω του γεγονότος ότι τα περισσότερα δίκτυα εξαρτώνται από άλλα ιδιωτικά δίκτυα που ανήκουν και διαχειρίζονται άλλοι και από μια δημόσια κοινόχρηστη υποδομή όπου έχετε πολύ λιγότερο έλεγχο, και γνώση σχετικά με τα εφαρμοζόμενα μέτρα ασφαλείας. Παρόλο που κάποια βοήθεια κρυπτογράφησης επεκτείνεται στην εξασφάλιση πληροφοριών που μετακινούνται μέσω δικτύωνΈνα άλλο πιθανό σενάριο από έναν εισβολέα είναι να υποκλέψει τη σύνοδο εισάγοντας έναν κακόβουλο κεντρικό υπολογιστή μεταξύ του κεντρικού υπολογιστή-πελάτη και του κεντρικού εξυπηρετητή τελικού διακομιστή για να σχηματίσει αυτό που ονομάζεται man-in-the-middle.

Σε αυτή την περίπτωση όλες οι επικοινωνίες και οι μεταδόσεις δεδομένων θα περάσουν μέσω του ξενιστή του εισβολέα. Σεναριοποίηση μεταξύ ιστοτόπων. Οι επιτιθέμενοι εκμεταλλεύονται γνωστές ευπάθειες σε εφαρμογές που βασίζονται στον ιστό, στους διακομιστές τους ή στα συστήματα plug-in στα οποία βασίζονται. Χρησιμοποιώντας ένα από αυτά, διπλώνουν κακόβουλο περιεχόμενο στο περιεχόμενο που παραδίδεται από τον συμβιβασμένο ιστότοπο. Όταν το προκύπτον συνδυασμένο περιεχόμενο φτάνει στον περιηγητή ιστού πελάτη, όλα έχουν παραδοθεί από την αξιόπιστη πηγή και συνεπώς λειτουργούν υπό τις άδειες που έχουν χορηγηθεί σε αυτό το σύστημα. Τείχος προστασίας τείχους προστασίας: Ένα τείχος προστασίας είναι ένα λογισμικό ή μια συσκευή υλικού που χρησιμοποιείται σε συστήματα ηλεκτρονικού εμπορίου για τον διαχωρισμό των διακομιστών back-end από τα εταιρικά δίκτυα και επιτρέπει την επικοινωνία μεταξύ των διακομιστών back-end και μερικών διακομιστών εντός του εταιρικού δικτύου Firewalls είναι υποχρεωτικά για επιχειρηματικούς ιστότοπους.

Ωστόσο, συνήθως υλοποιούνται στο επίπεδο πρωτοκόλλου δικτύου και δεν προστατεύουν το σύστημα από επιθέσεις που αποσκοπούν σε υψηλότερα πρωτόκολλα, όπως το HTTP. Για παράδειγμα, οι διακομιστές Web δέχονται πακέτα δεδομένων μέσω θύρας 80, που προορίζονται για αιτήσεις HTTP. Εάν ένας χρήστης αποκτήσει πρόσβαση σε ένα στοιχείο μέσω μιας αίτησης HTTP που προκαλεί υπερχείλιση του buffer, η υπηρεσία μπορεί να καταρρεύσει και να παράσχει στον χρήστη πρόσβαση στο σύστημα

για περαιτέρω επιθέσεις. Οι χάκερ μπορούν να αποκτήσουν πρόσβαση στους εταιρικούς back-end εξυπηρετητές intranet χρησιμοποιώντας ορισμένα γνωστά αδιαφανή παραθυράκια τείχους προστασίας και να προσπαθήσουν να εισβάλουν σε τιμοκαταλόγους, καταλόγους και λίστες ηλεκτρονικών μηνυμάτων και να αλλάξουν ή να καταστρέψουν τα δεδομένα, γεγονός που μπορεί να διαταράξει ή και να απενεργοποιήσει τις επιχειρηματικές λειτουργίες .

ΚΕΦΑΛΑΙΟ 3- ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Η ασφάλεια είναι μία από τις βασικές και συνεχιζόμενες ανησυχίες που περιορίζουν τους πελάτες και τους οργανισμούς που ασχολούνται με το ηλεκτρονικό εμπόριο. Στόχος του παρόντος εγγράφου είναι να διερευνήσει την αντίληψη της ασφάλειας στο ηλεκτρονικό εμπόριο Οι ιστοσελίδες B2C και C2C τόσο από πλευράς πελατών όσο και από οργανωτικές προοπτικές (Νάστου , 2003).

Οι επιχειρήσεις ηλεκτρονικού εμπορίου αναπτύσσονται και αναπτύσσονται και βελτιώνονται καθημερινά πιο ασφαλείς τεχνολογίες. Οι τρέχουσες πολιτικές και τεχνολογίες ασφάλειας στο διαδίκτυο δεν ανταποκρίνονται στις ανάγκες των τελικών χρηστών. Η επιτυχία ή η αποτυχία μιας επιχείρησης ηλεκτρονικού εμπορίου εξαρτάται από χιλιάδες παράγοντες, μεταξύ των οποίων, μεταξύ άλλων, το επιχειρηματικό μοντέλο, την ομάδα, τους πελάτες, τους επενδυτές, το προϊόν και την ασφάλεια των μεταδόσεων δεδομένων και αποθήκευσης. Κάθε επιχείρηση που θέλει να έχει ανταγωνιστικό πλεονέκτημα στη σημερινή παγκόσμια αγορά θα πρέπει να υιοθετήσει μια ολοκληρωμένη πολιτική ασφάλειας σε συνεννόηση με τους εταίρους, τους προμηθευτές και τους διανομείς, οι οποίοι θα παράσχουν ασφαλές περιβάλλον για τον επόμενο πολλαπλασιασμό του ηλεκτρονικού εμπορίου(Δουκίδης και άλλοι, 2010).

3.1. PKI

Βασικές αρχές ασφάλειας πληροφοριών και συστήματα PKI

Γενικότερα, η πληροφορία που δημιουργείται ή διακινείται κατά τη διεξαγωγή μιας ηλεκτρονικής συναλλαγής σχετίζεται άμεσα με τους εμπλεκόμενους στην υπ' όψη συναλλαγή και θα πρέπει να διασφαλιστεί απέναντι σε όλους τους πιθανούς κινδύνους, όπως υποκλοπή, αλλοίωση, ανεπιθύμητη κοινοποίηση σε τρίτους κλπ. Για το σκοπό αυτό απαιτείται η δημιουργία ενός περιβάλλοντος ηλεκτρονικών συναλλαγών, το οποίο,

επιπλέον της ασφάλειας των συστημάτων, θα δίνει έμφαση στην ασφάλεια των ίδιων των πληροφοριών και θα διασφαλίζει τις εξής *βασικές αρχές*

I Επιβεβαίωση ταυτότητας (authentication), ώστε να αποδεικνύεται η ταυτότητα ενός ατόμου ή μιας εφαρμογής λογισμικού ή ενός μηχανήματος (π.χ. server),

2. Εμπιστευτικότητα (confidentiality), ώστε να εξασφαλίζεται ο ιδιωτικός χαρακτήρας της πληροφορίας,
3. Ακεραιότητα (integrity), ώστε να βεβαιώνεται ότι η πληροφορία δεν έχει αλλοιωθεί κατά τη μετάδοσή της,
4. Μη αποκήρυξη (non-repudiation), ώστε να αποκλειστεί το ενδεχόμενο κάποιος από τους συμμετέχοντες σε μια συναλλαγή να αρνηθεί εκ των υστέρων την εμπλοκή του σ' αυτήν ή τα αποτελέσματα της.

Με βάση τα σημερινά τεχνολογικά δεδομένα, η πλήρης διασφάλιση των πιο πάνω βασικών αρχών είναι δυνατόν να επιτευχθεί μόνο με τη χρήση της κρυπτογραφίας, η οποία επιπλέον θα πρέπει να συνδυάζεται με πολιτικές ασφάλειας, που να καθορίζουν τους κανόνες με τους οποίους λειτουργεί ένα σύστημα κρυπτογράφησης, προϊόντα (softwareκαι hardware), τα οποία να επιτρέπουν την δημιουργία, αποθήκευση και διαχείριση των κλειδιών ασφαλείας, που θα χρησιμοποιούνται κατά την κρυπτογράφηση / αποκρυπτογράφηση και, τέλος, διαδικασίες, που να περιγράφουν τους τρόπους δημιουργίας, διανομής και χρήσης των κλειδιών ασφαλείας(Κουργιαντάκης, 2013).

Η σύγχρονη προσέγγιση στις παραπάνω απαιτήσεις είναι γνωστή με τον όρο Συστήματα Υποδομής Δημοσίου Κλειδιού (PublicKeyInfrastructureSystems - Συστήματα PKI),
τα οποία ενσωματώνουν ως αναπόσπαστο τμήμα τους και διάφορες τεχνικές κρυπτογραφίας και επιτρέπουν την ασφαλή διεξαγωγή των εμπορικών συναλλαγών μέσω του Internet, επιτυγχάνοντας την τήρηση των τεσσάρων βασικών αρχών που προαναφέρθηκαν (Κουκουβίνος, 2007).

Πιο συγκεκριμένα και σε σχέση με τις τέσσερις βασικές αρχές, ένα σύστημα PKI λειτουργεί ως εξής:

Επιβεβαίωση (authentication)

Η επιβεβαίωση ταυτότητας σε ένα ηλεκτρονικό σύστημα είναι απαραίτητη, προκειμένου η πρόσβαση σ' αυτό να επιτρέπεται μόνο σε όσους μπορούν να παράσχουν

τα σχετικά διαπιστευτήρια, Στα περισσότερα συστήματα η επιβεβαίωση ταυτότητας διεκπεραιώνεται με τη χρήση ενός κωδικού χρήστη και ενός συνθηματικού (password), τεχνική η οποία παρουσιάζει πλήθος αδυναμιών από πλευράς ασφάλειας. Σε ένα περιβάλλον PKI, για την επιβεβαίωση ταυτότητας χρησιμοποιούνται τα "ψηφιακά πιστοποιητικά'' (ή ψηφιακές ταυτότητες). Τα συνηθέστερα σημεία αποθήκευσης ενός ψηφιακού πιστοποιητικού είναι είτε ο μαθητικός δίσκος του υπολογιστή του χρήστη είτε μια ειδική κάρτα (έξυπνη κάρτα) μικρού μεγέθους, που ο χρήστης έχει πάντα μαζί του. Με ψηφιακά πιστοποιητικά εξάλλου εφοδιάζονται όχι μόνο τα φυσικά πρόσωπα, αλλά και ορισμένα μηχανήματα, π.χ, ο Webservermιας επιχείρησης, ώστε να μπορεί να "αποδείξει" στον εν δυνάμει χρήστη που τον έχει επισκεφθεί μέσω του Internetότι πράγματι εκπροσωπεί μια συγκεκριμένη εταιρία και έχει κατά συνέπεια το δικαίωμα να προβαίνει σε νόμιμες ηλεκτρονικές συναλλαγές (πωλήσεις κλπ). (Κουργιαντάκης, 2013).

Εμπιστευτικότητα (confidentiality)

Βασικό χαρακτηριστικό μιας ασφαλούς συναλλαγής μεταξύ δύο μερών είναι το περιεχόμενό της να παραμείνει μυστικό και απροσπέλαστο για οποιονδήποτε τρίτο. Τα προς προστασία δεδομένα μπορεί να αφορούν επιχειρηματικά σχέδια, οικονομικές συναλλαγές, πνευματική ιδιοκτησία, εμπιστευτικές πληροφορίες σχετικές με το προσωπικό κλπ. Ένα σύστημα PKI χρησιμοποιεί διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης, στηριζόμενες σε κατάλληλα κλειδιά", προκειμένου να κρατήσει τα ευαίσθητα δεδομένα προστατευμένα από κάθε ανεπιθύμητη πρόσβαση. Έτσι ακόμη και αν τα δεδομένα υποκλαπούν, θα είναι εξαιρετικά δύσκολο έως αδύνατο να αξιοποιηθούν, διότι θα πρέπει προηγουμένως να αποκρυπτογραφηθούν.

Ακεραιότητα δεδομένων (dataintegrity)

Η αρχή αυτή διασφαλίζει ότι τα δεδομένα που έφθασαν στον παραλήπτη ενός μηνύματος είναι τα ίδια με αυτά που απέστειλε ο αποστολέας και δεν έχουν αλλοιωθεί καθοδόν. Η σημασία της ακεραιότητας των δεδομένων μιας ηλεκτρονικής συναλλαγής γίνεται εύκολα αντιληπτή αν σκεφθεί κανείς το παράδειγμα μιας ηλεκτρονικά μεταδιδόμενης οικονομικής προσφοράς για 1000 μονάδες ενός συγκεκριμένου είδους, προς 5 ευρώ ανά μονάδα. Αν η τιμή μονάδας αλλοιωθεί σε 50 ευρώ, τότε αμφισβητείται η ίδια η υπόσταση της προσφοράς. Ένα σύστημα PKI χρησιμοποιεί τους λεγάμενους

αλγόριθμους κατατεμαχισμού και την έννοια του ‘‘αποτυπώματος' ενός μηνύματος, σε συνδυασμό με ψηφιακές υπογραφές, προκειμένου να επιτρέψει στον' παραλήπτη να βεβαιωθεί ότι το μήνυμα δεν έχει αλλοιωθεί ούτε κατ' ελάχιστον σε σχέση με αυτό που πράγματι απέστειλε ο αποστολέας. Ακόμη και στην περίπτωση που δεν υφίσταται κίνδυνος κακόβουλης ενέργειας εκ μέρους τρίτων, η βεβαιότητα για την ακρίβεια και την πληρότητα ενός ηλεκτρονικού μηνύματος είναι σημαντική. (Κουργιαντάκης, 2013).

Μη αποκήρυξη (non-repudiation)

Η αρχή της μη αποκήρυξης σημαίνει ότι εάν προκύψει διαφωνία ή αμφισβήτηση σχετικά με τη διεξαγωγή μιας ηλεκτρονικής συναλλαγής, υπάρχουν {στα πλαίσια του συγκεκριμένου ηλεκτρονικού περιβάλλοντος) διαθέσιμα αδιάψευστα αποδεικτικά στοιχεία, τα οποία μπορούν' να χρησιμοποιηθούν από ένα τρίτο ουδέτερο μέρος, προκειμένου να διαπιστωθεί τι ακριβώς έχει συμβεί.

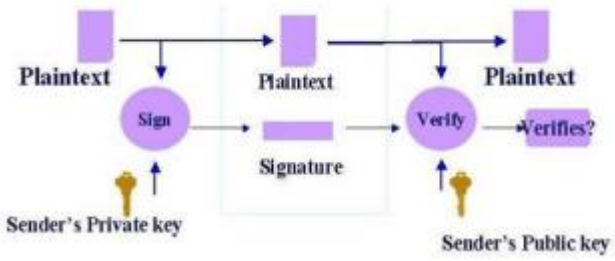
Πρόκειται ουσιαστικά για το συνδυασμό "επιβεβαίωση ταυτότητας - ακεραιότητα δεδομένων’, ο οποίος παρέχει στον παραλήπτη την βεβαιότητα ότι ο αποστολέας δεν θα μπορέσει να αρνηθεί (ψευδώς) ότι έχει δημιουργήσει, υπογράψει και αποστείλει ένα ηλεκτρονικό έγγραφο ή έχει συμμετάσχει σε μια συναλλαγή. Αυτό είναι ιδιαίτερα σημαντικό σε οικονομικές ιδίως συναλλαγές, όπου το ένα από τα δύο μέρη θα μπορούσε πιθανόν να αρνηθεί την πληρωμή πχ, ενός λογαριασμού για παροχή υπηρεσιών, με τον ισχυρισμό ότι οι σχετικές υπηρεσίες δεν είχαν ποτέ ζητηθεί. σε ένα περιβάλλον PKI, η μη αποκήρυξη χρησιμοποιεί μεν την έννοια των ψηφιακών υπογραφών, προϋποθέτει όμως και ένα γενικότερο πλαίσιο λειτουργίας που καθορίζεται από συγκεκριμένες πολιτικές και διαδικασίες. Με τα δεδομένα αυτά, ένα τέτοιο ηλεκτρονικό περιβάλλον θα μπορούσε να χρησιμοποιηθεί ακόμη και για την ψηφιακή υπογραφή συμβάσεων. Φυσικά, σημαντικό ρόλο παίζει στην περίπτωση αυτή και το ισχύον κάθε φορά νομικό πλαίσιο, το οποίο θα πρέπει να ληφθεί σοβαρά υπ’ όψη(Hamdan etal, 2010).

Συστήματα PKI

Γενικότερα, τα συστήματα PKI στηρίζονται σε μια σειρά από κοινά αποδεκτά πρότυπα (standards) και παρέχουν μια κοινή υποδομή ασφάλειας, η οποία μπορεί να αξιοποιηθεί από οποιοδήποτε επιμέρους πληροφοριακό υποσύστημα που υλοποιεί μια

συγκεκριμένη επιχειρηματική διαδικασία (π.χ. υποσύστημα παραγγελιών, υποσύστημα αποθεμάτων κλπ). Έτσι η **ασφάλεια** των πληροφοριών αποτελεί τελικά μέρος της υποδομής της επιχείρησης (όπως η τηλεφωνική υποδομή ή η υποδομή παροχής ηλεκτρικής ενέργειας), με αποτέλεσμα κάθε επιμέρους υποσύστημα να μην "κτίζει'' το δικό του περιβάλλον ασφάλειας, αλλά απλώς να χρησιμοποιεί με κατάλληλο τρόπο τις ήδη διαθέσιμες υπηρεσίες ασφάλειας (Δουκίδης, 2010)

Η υποδομή δημόσιου κλειδιού (PKI) αναφέρεται στην ιδέα ότι ο καλύτερος τρόπος δημιουργίας ενός συστήματος ασφαλούς επικοινωνίας μέσω δικτύων είναι η δημιουργία υποδομής που θα υποστηρίζει κρυπτογράφηση δημόσιου κλειδιού. Το PKI θα δημιουργήσει ένα περιβάλλον όπου οποιοσδήποτε χρήστης του Διαδικτύου θα μπορούσε να "μεταφέρει" πιστοποιητικά γύρω από αυτόν που τα αναγνωρίζουν με διάφορους τρόπους. Η εξακρίβωση της ταυτότητας των μερών μπορεί να γίνει πολύ φτηνή και εύκολη. Ορισμένοι υποστηρικτές του ηλεκτρονικού εμπορίου υποδεικνύουν ότι η δημιουργία ενός αδιάλειπτου και ισχυρού PKI θα έχει τεράστιες επιπτώσεις για την επιτάχυνση της ανάπτυξης του ηλεκτρονικού εμπορίου(Κουκουβίνος, 2007).



Εικόνα 4- Δομή Δημοσίου κλειδιού (PKI)

Τα πακέτα λογισμικού ηλεκτρονικού εμπορίου θα πρέπει επίσης να λειτουργούν με τεχνολογίες ασφαλούς ηλεκτρονικής μεταφοράς (SET) ή ασφαλούς στρώσης υποδοχής (SSL) για την κρυπτογράφηση των μεταδόσεων δεδομένων. (SSL), τα οποία επιτρέπουν τη μετάδοση κρυπτογραφημένων δεδομένων μέσω του Διαδικτύου εκτελώντας τα παραπάνω από τα παραδοσιακά πρωτόκολλα TCP / IP. Στον κυβερνοχώρο, τόσο ο πελάτης όσο και ο πωλητής δυσκολεύονται να αποδείξουν την ταυτότητά τους μεταξύ τους με βεβαιότητα, ιδιαίτερα κατά τη διάρκεια μιας πρώτης συναλλαγής. Πώς ο αγοραστής μεταδίδει με ασφαλή τρόπο ευαίσθητες πληροφορίες στον πωλητή; Πώς γνωρίζει ο πωλητής ότι πρόκειται για νόμιμη εντολή αγοράς; Πώς

γνωρίζουν και τα δύο μέρη ότι ένας άδικος τρίτος δεν έχει αντιγράψει ή / και δεν έχει τροποποιήσει τις πληροφορίες συναλλαγής; (Hamdan etal, 2010).

Αυτές οι ερωτήσεις και άλλοι, περιγράφουν το πρόβλημα που επηρεάζει τις εμπορικές συναλλαγές μέσω του διαδικτύου ή οποιουδήποτε δημόσιου δικτύου. Οι πελάτες (πελάτες) πρέπει να είναι βέβαιοι ότι:

1- επικοινωνούν με το σωστό διακομιστή.

2- Αυτό που στέλνουν παραδίδεται χωρίς τροποποίηση

3- Μπορούν να αποδείξουν ότι έστειλαν το μήνυμα.

4- Μόνο ο προορισμένος δέκτης μπορεί να διαβάσει το μήνυμα.

5 - Η παράδοση είναι εγγυημένη. Από την άλλη πλευρά, οι πωλητές (σοβαρότεροι) πρέπει να είναι σίγουροι ότι:

1- Επικοινωνούν με τον κατάλληλο πελάτη

2- Το περιεχόμενο του ληφθέντος μηνύματος είναι σωστό.

3- Η ταυτότητα του συγγραφέα είναι αδιαμφισβήτητη.

4- Μόνο ο συντάκτης θα μπορούσε να έχει γράψει το μήνυμα.

5- Αποδέχονται τη λήψη του μηνύματος. Όλες οι ανησυχίες που αναφέρονται παραπάνω μπορούν να επιλυθούν χρησιμοποιώντας κάποιο συνδυασμό κρυπτογραφικής μεθόδου και μεθόδων πιστοποιητικών .

Ο τύπος του κινδύνου που προκύπτει από την ανεπάρκεια της ασφάλειας είναι:

1- Προβλήματα ή σφάλματα διαμόρφωσης στο websever που μπορούν να προκαλέσουν κλοπή εμπιστευτικών εγγράφων.

2- Κίνδυνοι από την πλευρά των περιηγητών, δηλ. Παραβίαση του απορρήτου του χρήστη, βλάβη του συστήματος του χρήστη, διακοπή λειτουργίας του προγράμματος περιήγησης κ.λπ. 3

3- Παρακράτηση δεδομένων που αποστέλλονται από το πρόγραμμα περιήγησης στο sever ή αντίστροφα. Αυτό είναι δυνατό σε οποιοδήποτε σημείο της διαδρομής μεταξύ του προγράμματος περιήγησης και του διακομιστή, δηλαδή του δικτύου από την πλευρά του προγράμματος περιήγησης, του δικτύου στο διακομιστή, του ISP του τελικού χρήστη (InternetServiceProvider), του ISP του διακομιστή ή της περιφερειακής πρόσβασης του ISP.

Αρχές Πιστοποίησης και ο ρόλος τους σε ένα σύστημα PKI

Με δεδομένο το ρόλο του δημόσιου κλειδιού στα πλαίσια της ασύμμετρης κρυπτογραφίας, το κύριο ζητούμενο είναι ένας αξιόπιστος μηχανισμός για τη διανομή των κλειδιών αυτών.Ο μηχανισμός αυτός δεν μπορεί παρά να στηρίζεται στη σύνδεση ενός δημόσιου κλειδιού με ορισμένες πληροφορίες που προσδιορίζουν την ταυτότητα του κατόχου του. Ο συνδυασμός αυτός δημιουργεί τη λεγόμενη ^ψηφιακή ταυτότητα" (digitalidentity) ή όπως είναι πιο γνωστό, το “ψηφιακό πιστοποιητικό” (digitalcertificate).

Τα ψηφιακά πιστοποιητικά αποτελούν το ψηφιακό ανάλογο των κλασσικών ταυτοτήτων και αποτελούν τη βάση για τη δημιουργία ενός ασφαλούς ηλεκτρονικού περιβάλλοντος, διότι επιτρέπουν την διασφάλιση ενός επιπέδου εμπιστοσύνης, σχετικά με τοποιός είναι ο πραγματικός κάτοχος ενός δεδομένου δημόσιου κλειδιού(Κουκουβίνος, 2007).

\

Οι φορείς που είναι υπεύθυνοι για την έκδοση ψηφιακών πιστοποιητικών (ψηφιακών ταυτοτήτων) στα πλαίσια ενός συστήματος PKI ονομάζονται Αρχές Πιστοποίησης * ΑΠ (CertificationAuthorities- CA). Μια ΑΠ εφαρμόζει συγκεκριμένες διαδικασίες, οι οποίες επαληθεύουν την ταυτότητα του υποψηφίου και στη συνέχεια εκδίδει ένα ψηφιακό πιστοποιητικό, που μπορεί να χρησιμοποιηθεί σαν απόδειξη αυτής της ταυτότητας. Τα ψηφιακά πιστοποιητικά εκδίδονται με προκαθορισμένη διάρκεια ισχύος και είναι δυνατόν να ανακληθούν, αν αυτό χρειαστεί,

Οι Αρχές Πιστοποίησης παίζουν το ρόλο του έμπιστου τρίτου μέρους, όπως αυτός περιγράφηκε παραπάνω, καθιστώντας δυνατή και διευκολύνοντας την επικοινωνία ανάμεσα σε δύο άλλα μέρη και για το λόγο αυτό είναι γνωστές και ως "Εμπιστες Τρίτες Οντότητες - ΕΤΟ (TrustedThirdParties- TTP)".

Οι κλασσικές ταυτότητες της καθημερινής ζωής έχουν μακρόχρονη προϊστορία σχετικά με το ποιούς φορείς εμπιστευόμαστε για την έκδοσή τους και το τι διαδικασίες ακολουθούν οι φορείς αυτοί Εντούτοις, ανακύπτουν ορισμένα ζητήματα σχετικά μα αυτά. Τα ζητήματα αυτά είναι:

- Σε ποιούς θα πρέπει να ανατεθεί η λειτουργία μιας ΑΠ
- Πόσο ευρέως θα χρησιμοποιούνται οι ψηφιακές ταυτότητες
- Τι διαδικασίες και αποδεικτικές μέθοδοι θα ακολουθούνται κατά την έκδοση των ταυτοτήτων
- Ποιούς μηχανισμούς μπορεί να προσφέρει ένα ψηφιακό δίκτυο για να διασφαλίσει, σε λογικά πλαίσια, ότι μια ταυτότητα δεν μπορεί να πλαστογραφηθεί

Σε πρώτη προσέγγιση, θα ήταν λογικό να λειτουργήσουν ως ΑΠ οι φορείς που ήδη ασχολούνται με έκδοση ταυτοτήτων', όπως κάποιες κρατικές αρχές, τράπεζες, επαγγελματικές ενώσεις κλπ. Αυτό θα ήταν πιθανόν' αποδεκτό, αλλά με κάποιες επιφυλάξεις ως προς το σκοπό χρήσης αυτών των ψηφιακών πιστοποιητικών (Σουρής . και Γρηγοριάδης,2014).

Αυτό πάντως που παρατηρείται σήμερα στην πράξη είναι ότι, παράλληλα με τις παραδοσιακές έμπιστες οντότητες, έχουν αναδειχθεί νέες μορφές φορέων, εμπορικού χαρακτήρα, που λειτουργούν ως ΑΠ, Οι φορείς αυτοί παρέχουν, έναντι αμοιβής, τις λεγάμενες “υπηρεσίες πιστοποίησης" και έχουν επιτύχει να καθιερωθούν στο χώρο αυτό χωρίς να διαθέτουν προηγούμενη φήμη, στην οποία να στηριχθούν. Η ανάδειξή τους οφείλεται κυρίως σε λόγους, όπως τεχνογνωσία, κατασκευή και χρήση εγκαταστάσεων υψηλής ασφαλείας, ιδιαίτερα προσεκτική επιλογή προσωπικού και υιοθέτηση και εφαρμογή εξαιρετικά αυστηρών διαδικασιών και ελέγχων.

Είναι σαφές ότι στο σημείο αυτό υπάρχει ένα ζήτημα γενικότερου κοινωνικού και πολιτικού ενδιαφέροντος, το οποίο θα πρέπει να αντιμετωπιστεί πολύ προσεκτικά σε όλες του τις διαστάσεις. Η ανάπτυξη ενός ασφαλούς ηλεκτρονικού περιβάλλοντος με τα πλεονεκτήματα που μπορεί να προσφέρει είναι μια εξέλιξη, η οποία θα πρέπει να διευκολυνθεί. Απαιτεί βέβαια, μεταξύ άλλων, υψηλή εξειδίκευση και τεχνολογική γνώση σε ταχύτατα εξελισσόμενους τομείς, γεγονός που τοποθετεί σε πλεονεκτική θέση ορισμένους ιδιωτικούς φορείς, οι οποίοι ήδη λειτουργούν de facto ως ευρύτερα αποδεκτές ΑΠ. Με δεδομένο τον κρίσιμο ρόλο των ΑΠ. θα πρέπει να τεθεί ένα πλαίσιο λειτουργίας τους, το οποίο να διασφαλίζει τη συμμόρφωσή τους με κάποιους κανόνες, προς όφελος του κοινωνικού συνόλου γενικότερα. Προς την κατεύθυνση αυτή έχουν γίνει ήδη ορισμένα βήματα, σε επίπεδο νομοθεσίας, ενώ σχετικές αναφορές υπάρχουν παρακάτω,

3.2. Συστήματα Κρυπτογραφίας

Τα συστήματα κρυπτογραφίας χρησιμοποιούνται συχνά για να ικανοποιήσουν τις βασικές απαιτήσεις ασφαλείας της εμπιστευτικότητας και της ακεραιότητας στα δίκτυα. Όμως, καθώς οι κόμβοι των αισθητήρων είναι περιορισμένοι στις δυνατότητες υπολογιστικής και μνήμης, οι γνωστές παραδοσιακές κρυπτογραφικές τεχνικές δεν μπορούν απλά να μεταφερθούν σε WSN χωρίς να τις προσαρμόσουν(Σουρής . και Γρηγοριάδης,2014).

Η ασφαλής ανταλλαγή μηνυμάτων θα μπορούσε πιθανόν να στηριχτεί στη διακίνησή τους μέσα από διαύλους, οι οποίοι να είναι ελεγχόμενοι αφενός και δεδομένης ασφάλειας αφετέρου. Στην περίπτωση όμως του Internetκάτι τέτοιο δεν είναι δυνατόν, κατά συνέπεια Οα πρέπει η έμφαση να δοθεί όχι στο δίαυλο, αλλά στο ίδιο το μήνυμα.
Την ανάγκη αυτή έρχονται να καλύψουν τα συστήματα κρυπτογραφίας, τα οποία επιτρέπουν την επικοινωνία ανάμεσα σε δύο μέρη. παρέχοντας ταυτόχρονα τη δυνατότητα του αποκλεισμού της πρόσβασης τρίτων μερών στο περιεχόμενο του μεταφερομένου μηνύματος. Αυτό συνήθως επιτυγχάνεται με τη μετατροπή (κωδικοποίηση κρυπτογράφηση) του μηνύματος σε μη κατανοητή μορφή, τη μεταφορά του και τελικώς την εκ νέου μετατροπή του (αποκωδικοποίηση / αποκρυπτογράφηση) σε κατανοητή μορφή, ώστε να γίνει αντιληπτό από τον παραλήπτη.

Η μετατροπή του περιεχομένου ενός μηνύματος σε μη αναγνώσιμη μορφή (κρυπτογράφηση), καθώς και η αντίστροφη μετατροπή (αποκρυπτογράφηση) επιτυγχάνεται με τη χρήση πολύπλοκων μαθηματικών διαδικασιών, που είναι γνωστές ως κρυπτογραφικοί αλγόριθμοι. Οι αλγόριθμοι αυτοί χωρίζονται σε δύο μεγάλες κατηγορίες, τους συμμετρικούς και τους ασύμμετρους. Κατ' επέκταση, τα συστήματα κρυπτογραφίας, ανάλογα με το είδος των αλγορίθμων που χρησιμοποιούν, ανήκουν είτε στη Συμμετρική είτε στην Ασύμμετρη Κρυπτογραφία, χωρίς vc- αποκλείεται και η συνδυασμένη χρήση και των δύο κατηγοριών.

3.3. Συμμετρική Κρυπτογραφία

Το σύστημα αυτό (γνωστό και ως σύστημα συμμετρικού κλειδιού ή σύστημα μυστικού κλειδιού - secreikeycryptography) είναι το πλέον γνωστό και έχει χρησιμοποιηθεί κατά κόρον, από την αρχαιότητα μέχρι και σήμερα.

Ενδεικτικά αναφέρεται εδώ το σύστημα κρυπτογράφησης που είχε επινοήσει και χρησιμοποιούσε ο Ιούλιος Καίσαρ, Σύμφωνα με το σύστημα αυτό, κάθε γράμμα του μηνύματος αντικαθίσταται από το αντίστοιχο που βρίσκεται Ν θέσεις παρακάτω στο αλφάβητο, όπου Ν είναι το κλειδί που χρησιμοποιείται κάθε φορά. Έτσι για παράδειγμα, η φράση “pleaseignore” θα κρυπτογραφηθεί ως "rngcugkipqtg" για N=2 και ως "sohdvhIjqruh[1]’ για N=3.

Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης δέχονται σαν είσοδο κανονικό αναγνώσιμο κείμενο (cleartext- plaintext) και με τη χρήση του συμμετρικού κλειδιού παράγουν σαν αποτέλεσμα (εξαγόμενο) μια κρυπτογραφημένη μορφή του αρχικού κειμένου. Το συμμετρικό κλειδί δεν είναι παρά ένας τυχαίος αριθμός με το σωστό μέγεθος. Έτσι, αν ο αλγόριθμος είναι συμμετρική κρυπτογράφηση των 40 bits, το συμμετρικό κλειδί θα είναι μήκους 40 bits, ενώ αν πρόκειται για αλγόριθμο συμμετρικής κρυπτογράφησης των 128 bits, τότε το συμμετρικό κλειδί θα είναι μήκους 128 bits. (Σουρής . και Γρηγοριάδης,2014).

Είναι ζωτικής σημασίας το συμμετρικό κλειδί να δημιουργείται με τη χρήση μιας καλής **γεννήτριας** τυχαίων αριθμών. Αυτό σημαίνει ότι η γεννήτρια θα πρέπει να επιλέγει αριθμούς ομοιόμορφα κατανεμημένους σε όλο το πεδίο τιμών που επιτρέπει το μήκος του κλειδιού και να μην "προτιμά” (ή “αποφεύγει”) κάποιες τιμές, οπότε εξασθενεί η ισχύς της κρυπτογράφησης.

Η κρυπτογραφία ασχολείται με την επινόηση νέων και διαρκώς ισχυρότερων κρυπτογραφικών αλγορίθμων, ενώ η κρυπτανάλυση έχει σαν αντικείμενο την εξέταση των κρυπτογραφικών αλγορίθμων με χρήση ειδικών εργαλείων και τεχνικών, με σκοπό να εντοπίσει πιθανά αδύνατα σημεία τους, που θα τους καθιστούσαν ευάλωτους σε επιθέσεις. Κατά συνέπεια, κάθε κρυπτογραφικός αλγόριθμος που επινοείται από τους ειδικούς της κρυπτολογίας, θα πρέπει να τίθεται στη διάθεση των κρυπταναλυτών, προκειμένου να διασφαλιστεί ότι δεν έχει (λόγω σχεδιασμού ή εφόσον χρησιμοποιηθεί με κάποιο ειδικό τρόπο) κενά ή τρόπους παραβίασης. Αν ο πιο πάνω διεξοδικός έλεγχος

δεν πραγματοποιηθεί (πιθανόν για λόγους μη δημοσιοποίησης της χρησιμοποιούμενης τεχνικής), υπάρχει πάντα το ενδεχόμενο τα πιθανά αδύνατα σημεία του να εντοπισθούν από τρίτους, αφού έχει τεθεί σε χρήση, οπότε τα αποτελέσματα για όσους στηρίζονται σ'αυτόν να είναι μέχρι και καταστροφικά.

Επομένως ένας κρυπτογραφικός αλγόριθμος χαρακτηρίζεται ως ασφαλής, εφ'όσον έχει προηγηθεί ο εξαντλητικός έλεγχός του από τους κρυπταναλυτές, χωρίς να εντοπισθούν αδυναμίες. Απόαυτές τις προϋποθέσεις, ο μόνος τρόπος να παραβιαστεί ένα κρυπτογραφημένο μήνυμα, είναι να δοκιμαστούν όλες οι πιθανές τιμές, κλειδιών που αντιστοιχούν στο συγκεκριμένο μέγεθος. Αυτό αποκαλείται επίθεση ωμής βίας (bruteforceattack). Στατιστικά θα χρειαστεί να δοκιμαστούν μόνο οι μισές από τις πιθανές τιμές του κλειδιού, προκειμένου να εντοπισθεί το σωστό κλειδί. Τα μεγέθη των κλειδιών επιλέγονται έτσι ώστε να είναι πρακτικά αδύνατο να δοκιμαστούν έστω και οι μισές πιθανές τιμές του κλειδιού, ακόμη και με χρήση τεράστιου αριθμού υπολογιστών, μέσα στο χρονικό διάστημα κατά το οποίο τα υπό προστασία δεδομένα πρέπει να παραμείνουν ασφαλή. Είναι φυσικά αδύνατο να προβλεφθεί με ακρίβεια η εξέλιξη της τεχνολογίας των υπολογιστών οπότε είναι απαραίτητο να γίνουν κάποιες υποθέσεις σχετικά με την πιθανή αύξηση της επεξεργαστικής τους ισχύος. (Σουρής . και Γρηγοριάδης,2014).

Υπάρχουν δύο κατηγορίες συμμετρικών αλγορίθμων κρυπτογράφησης:

Α. Οι αλγόριθμοι, οι οποίοι χωρίζουν τα προς κρυπτογράφηση δεδομένα σε πακέτα των 64 bitsκαι είναι γνωστοί ως '"blockciphers '. Οι πιο γνωστός από αυτούς είναι ο DES (DataEncryptionStandard), ο οποίος έχει σταθερό μέγεθος κλειδιού 56 bitsκαι αναπτύχθηκε αρχικά από την IBMστη δεκαετία του 1970, ενώ στη συνέχεια υιοθετήθηκε και από την κυβέρνηση των ΗΠΑ ως το επίσημο πρότυπο κρυπτογράφησης απορρήτων πληροφοριών. Ο DESυπήρξε εν χρήσει για μεγάλο διάστημα και χρησιμοποιήθηκε σε πολλά κρυπτογραφικά συστήματα, όπως το σύστημα Kerberos, το οποίο αναπτύχθηκε στο M1T. Λόγω όμως της αυξανόμενης ισχύος των υπολογιστών, το μήκους 56 bitsκλειδί του αρχίζει να γίνεται ευάλωτο σε επιθέσεις τύπου "ωμής βίας". Οι προσπάθειες για βελτίωση του DESοδήγησαν στη δημιουργία του 3-DES (tripleDES). όπου τα δεδομένα κρυπτογραφούνται τρεις φορές. Πολύ γνωστός επίσης είναι ο αλγόριθμος RC2 (αναπτύχθηκε από τον RonRivest), ο οποίος μπορεί **να** αντικαταστήσει

τον DES. ενώ είναι δύο έως τρεις φορές πιο γρήγορος.

Ο RC5 είναι ένας ακόμη συμμετρικός αλγόριθμος με δημιουργό τον RonRivestκαι ο οποίος χωρίζει τα δεδομένα σε πακέτα των 64 ή των 128 bits, ενώ υποστηρίζει κλειδιά μεταβλητού μήκους μέχρι και 2048 bits. Το πλεονέκτημα στην περίπτωση αυτή είναι ότι όσο μεγαλύτερο μήκος κλειδιού επιλεγεί, τόσο πιο ισχυρή είναι η κρυπτογράφηση, αν και απαιτείται προφανώς μεγαλύτερη υπολογιστική ισχύς για να εκτελεστεί η κρυπτογράφηση. Εστί παρέχεται η δυνατότητα επιλογής, ανάλογα με τις εκάστοτε απαιτήσεις,

Β. Οι αλγόριθμοι που δεν εφαρμόζονται σε πακέτα δεδομένων συγκεκριμένου μεγέθους (64 ή 128 bits), αλλά σε ακολουθίες bits (streamciphers).

Ο πιο γνωστός από αυτούς είναι ο RC4, με κυριότερα χαρακτηριστικά του την ταχύτητα (είναι ταχύτερος από όλους της προηγούμενης κατηγορίας) και την υποστήριξη κλειδιών μεταβλητού μήκους.

Τέλος, κοινές σε όλους τους συμμετρικούς αλγόριθμους είναι οι εξής δύο ιδιότητες:

* Είναι γενικά γρήγοροι στην εκτέλεσή τους
* Είναι συμπαγείς (compact), με την έννοια ότι το παραγόμενο κρυπτογραφημένο μήνυμα έχει γενικά το ίδιο μέγεθος με το αρχικό μήνυμα(Σερπάνος, 2011).

Με βάση τα παραπάνω, εάν δύο πρόσωπα Α και Β θέλουν να επικοινωνήσουν (έστω όχι ο Αεπιθυμεί να στείλει ένα μυστικό μήνυμα στον Β). θα πρέπει να κινηθούν ως εξής:

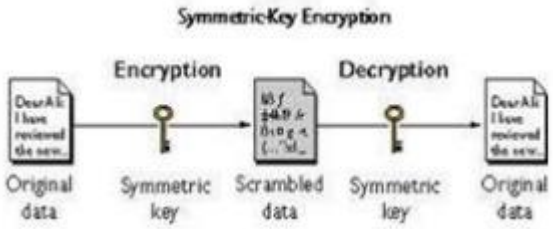
> Επιλέγεται ένας συμμετρικός αλγόριθμος
> Επιλέγεται το συμμετρικό κλειδί
> Το κλειδί πρέπει να γίνει γνωστό και στους δύο: εάν το έχει επιλέξει ο Α, θα πρέπει να το αποστείλει εκ των προτέρων στον Β.
> Ο Α κρυπτογραφεί το μήνυμα με τη χρήση του κλειδιού
> Ο Α αποστέλλει το κρυπτογραφημένο μήνυμα στον Β

Ο Β αποκρυπτογραφεί το μήνυμα

Τα κρυπτογραφικά κλειδιά παρουσιάζουν πολλές ομοιότητες με τα φυσικά κλειδιά της καθημερινής ζωής, που χρησιμοποιούνται π.χ. για να κλειδώσουν ή να ξεκλειδώσουν μια πόρτα. Για κάθε τύπο κλειδαριάς, υπάρχει ένα κλειδί ειδικού σχήματος που ταιριάζει σ'αυτήν και το οποίο πρέπει να έχει το σωστό μήκος και τη σωστή μορφολογία

Η συμμετρική κρυπτογράφηση (που ονομάζεται επίσης κρυπτογράφηση μυστικού κλειδιού) τόσο κρυπτογράφηση όσο και αποκρυπτογράφηση όπως φαίνεται στην εικόνα 4. Αυτό το κλειδί πρέπει να κρατηθεί μυστικό στο δίκτυο, το οποίο μπορεί να είναι αρκετά δύσκολο στο εκτεθειμένο περιβάλλον όπου χρησιμοποιούνται WSNs για την επίτευξη των απαιτήσεων ασφάλειας, αρκετοί ερευνητές έχουν επικεντρωθεί στην αξιολόγηση κρυπτογραφικών αλγορίθμων σε WSNs και να προτείνει ενεργειακά αποδοτικούς κρυπτογράφους.

Οι αλγόριθμοι συμμετρικού κλειδιού είναι πολύ πιο γρήγορα υπολογιστικοί από τους ασύμμετρους αλγορίθμους, καθώς η διαδικασία κρυπτογράφησης είναι λιγότερο περίπλοκη. Παραδείγματα είναι τα AES, 3DES κλπ. Εστιάζουμε πρώτα στην Συμμετρική Κρυπτογραφία λόγω της παραδοχής ότι η συμμετρική κρυπτογραφία έχει μεγαλύτερη αποτελεσματικότητα και απαιτεί λιγότερη κατανάλωση ενέργειας, σε αντίθεση με την κρυπτογραφία δημόσιου κλειδιού(Χονδροκούκης, 2005).



Εικόνα 5- Συμμετρική κρυπτογράφηση κλειδιού

Το δημόσιο κλειδί χρησιμοποιείται σε ορισμένες εφαρμογές για ασφαλείς επικοινωνίες π.χ. SSL (Secure Socket Layer) και IPSec πρότυπα τόσο το χρησιμοποιούν για τα βασικά πρωτόκολλα συμφωνίας τους. Αλλά καταναλώνει περισσότερη ενέργεια και είναι πιο ακριβό σε σύγκριση με το συμμετρικό κλειδί έχει δώσει ένα λόγο ότι το δημόσιο κλειδί καταναλώνει περισσότερη ενέργεια λόγω του μεγάλου αριθμού υπολογισμών και επεξεργασίας, γεγονός που το καθιστά πιο καταναλώσιμο από την

κατανάλωση ενέργειας σε σύγκριση με την τεχνική του συμμετρικού κλειδιού, π.χ. μια ενιαία λειτουργία δημόσιου κλειδιού μπορεί να καταναλώνει το ίδιο χρονικό διάστημα και ενέργεια με την κρυπτογράφηση δεκάδων μεγαβάτ με κρυπτογράφηση μυστικού κλειδιού(Χονδροκούκης, 2005).

Η περισσότερη κατανάλωση υπολογιστικών πόρων των τεχνικών δημόσιου κλειδιού οφείλεται στο γεγονός ότι χρησιμοποιεί δύο κλειδιά. Ένας από τους οποίους είναι δημόσιος και χρησιμοποιείται για κρυπτογράφηση και ο καθένας μπορεί να κρυπτογραφήσει ένα μήνυμα μαζί του και ο άλλος είναι ιδιωτικός στον οποίο πραγματοποιείται μόνο αποκρυπτογράφηση και τα δύο κλειδιά έχουν έναν μαθηματικό σύνδεσμο. Το ιδιωτικό κλειδί μπορεί να προέρχεται από ένα δημόσιο κλειδί. προκειμένου να την προστατεύσουμε από τον εισβολέα, η απόκτηση του ιδιωτικού κλειδιού από το κοινό γίνεται δυσκολότερη όσο το δυνατόν, λαμβάνοντας υπόψη έναν μεγάλο αριθμό που καθιστά αδύνατη την υπολογιστική. είναι προτιμότερο να επιλέξετε το WSN.

Το κόστος του δημόσιου κλειδιού είναι πολύ πιο ακριβό σε σύγκριση με το συμμετρικό κλειδί για παράδειγμα, μια κρυπτογράφηση RC5 64 bit σε ATmega 128 8 MHZ διαρκεί 5,6 χιλιοστά του δευτερολέπτου και μια αξιολόγηση συνάρτησης SHA1 των 160 bit διαρκεί μόνο 7,2 χιλιοστά του δευτερολέπτου. οι αλγόριθμοι κλειδιών είναι περισσότερο από 200 φορές ταχύτεροι από τους αλγόριθμους δημόσιου κλειδιού. Η κρυπτογράφηση του δημόσιου κλειδιού δεν είναι μόνο δαπανηρή στον υπολογισμό, αλλά και είναι ακριβότερη στην επικοινωνία σε σύγκριση με την συμμετρική κρυπτογράφηση κλειδιών.

Για την αποστολή ενός δημόσιου κλειδιού από έναν κόμβο σε άλλο, πρέπει να αποστέλλονται τουλάχιστον 1024 bits εάν το ιδιωτικό κλειδί είναι 1024 bits. Δύο τύποι συμμετρικών ψηφιακών ψηφιακών κρυπτογραφητών χρησιμοποιούνται: κρυπτογραφητές μπλοκ που δουλεύουν σε μπλοκ συγκεκριμένου μήκους και κρυπτογράφηση ροής που επεξεργάζονται δεδομένα bit. Ένας κρυπτογραφητής ρεύματος μπορεί να θεωρηθεί ως κρυπτογραφημένος κώδικας με μήκος μπλοκ 1 bit.. Οι συγγραφείς δεν εξετάζουν μόνο τις ιδιότητες ασφαλείας των αλγορίθμων, αλλά επιπροσθέτως προσπαθούν να βρουν τις πιο αποδοτικές από πλευράς αποθήκευσης και ενεργειακά αποδοτικές(Κουργιαντάκης, 2013).

3.4. Ασύμμετρη Κρυπτογράφηση

Σε ένα ασύμμετρο κρυπτοσύστημα (ή κρυπτοσύστημα δημόσιου κλειδιού), υπάρχουν δύο διαφορετικά κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων.(Abood, 2017).

ΚΕΦΑΛΑΙΟ 4- ΤΡΟΠΟΣ ΛΕΙΤΟΥΡΓΙΑΣ ΠΡΩΤΟΚΟΛΛΩΝ ΣΤΟ E-COMMERCE

4.1. Το πρωτόκολλο SSL

Το πρωτόκολλο SSL έχει γίνει ο defacto τρόπος προστασίας με κρυπτογράφηση της HTTP κίνησης του Διαδικτύου όταν αυτό απαιτείται. Η έκρηξη τα τελευταία χρόνια του ηλεκτρονικού εμπορίου, των ηλεκτρονικών τραπεζικών συναλλαγών και άλλων παρόμοιων εφαρμογών με αυξημένες απαιτήσεις ασφάλειας κατά τη μεταφορά των ευαίσθητων δεδομένων του χρήστη, φροντίζουν ώστε το πρωτόκολλο SSL να βρίσκεται σε συχνή χρήση.

Το SSL είναι το πανταχού παρόν πρωτόκολλο ασφαλείας που χρησιμοποιείται σχεδόν στο 100% των ασφαλών συναλλαγών στο Διαδίκτυο. Ουσιαστικά, το SSL μετατρέπει ένα τυπικό αξιόπιστο πρωτόκολλο μεταφοράς (όπως το TCP) σε ένα ασφαλές κανάλι επικοινωνιών κατάλληλο για τη διεξαγωγή ευαίσθητων συναλλαγών. Το πρωτόκολλο SSL ορίζει τις μεθόδους με τις οποίες μπορεί να δημιουργηθεί ένας ασφαλής δίαυλος επικοινωνίας - δεν δείχνει ποιοι κρυπτογραφικοί αλγόριθμοι χρειάζονται για να χρησιμοποιηθεί. Το SSL υποστηρίζει πολλούς διαφορετικούς αλγόριθμους και χρησιμεύει ως πλαίσιο όπου η κρυπτογραφία μπορεί να χρησιμοποιηθεί με βολικό και κατανεμημένο τρόπο. Χρήσεις για SSL

Οι χρήσεις για SSL είναι ατελείωτες. Κάθε εφαρμογή που χρειάζεται να μεταδίδει δεδομένα μέσω ενός μη ασφαλούς δικτύου, όπως το διαδίκτυο ή ένα intranet της εταιρείας, είναι πιθανός υποψήφιος για SSL. Το SSL παρέχει ασφάλεια και, το σημαντικότερο, ηρεμία. Όταν χρησιμοποιείτε το SSL, μπορείτε να είστε αρκετά σίγουροι ότι τα δεδομένα σας είναι ασφαλή από τα ηλεκτρονικά μηνύματα και την παραβίαση. Το SSL είναι σχετικά νέο για τον ενσωματωμένο κόσμο, επειδή ήταν πολύ περίπλοκο για να χειριστεί τους παραδοσιακούς μικροεπεξεργαστές embeddedsystems. Ωστόσο, ξεκινώντας με τον Rev. A του μικροεπεξεργαστή Rabbit 3000, προστέθηκε βοήθεια υλικού για να επιταχυνθούν κάποιες από τις πιο σύνθετες λειτουργίες κρυπτογράφησης SSL, καθιστώντας την SSL μια βιώσιμη λύση σε μια αγορά στην οποία τα τυπικά

(συνήθως πολύπλοκα) πρωτόκολλα ασφαλείας δεν έχουν παραδοσιακά υποστηρίζεται. Οι εφαρμογές για ενσωματωμένες εφαρμογές είναι εξίσου πολυάριθμες με εκείνες του κόσμου των Η / Υ. Τα παρακάτω είναι μόνο μερικές πιθανές εφαρμογές για ενσωματωμένο SSL.

• Η αυτόματη αυτόματη μηχανή πώλησης μπορεί τώρα να γίνει πραγματικότητα - το SSL κάνει σχεδόν αδύνατη την παραποίηση των επικοινωνιών.

• Τα συστήματα αυτοματισμού στο σπίτι μπορούν να ενεργοποιηθούν από το Διαδίκτυο-ξεχάσατε να απενεργοποιήσετε το φούρνο; Απλώς συνδεθείτε στο σπίτι σας από τον υπολογιστή σας στη δουλειά και απενεργοποιήστε το. Το SSL παρέχει ένα ασφαλές μέσο προστασίας του σπιτιού σας από τους χάκερ.

• Οι αναγνώσεις από ιατρικές συσκευές μπορούν να σταλούν μέσω ενός τυπικού δικτύου - το SSL προστατεύει το απόρρητό σας.

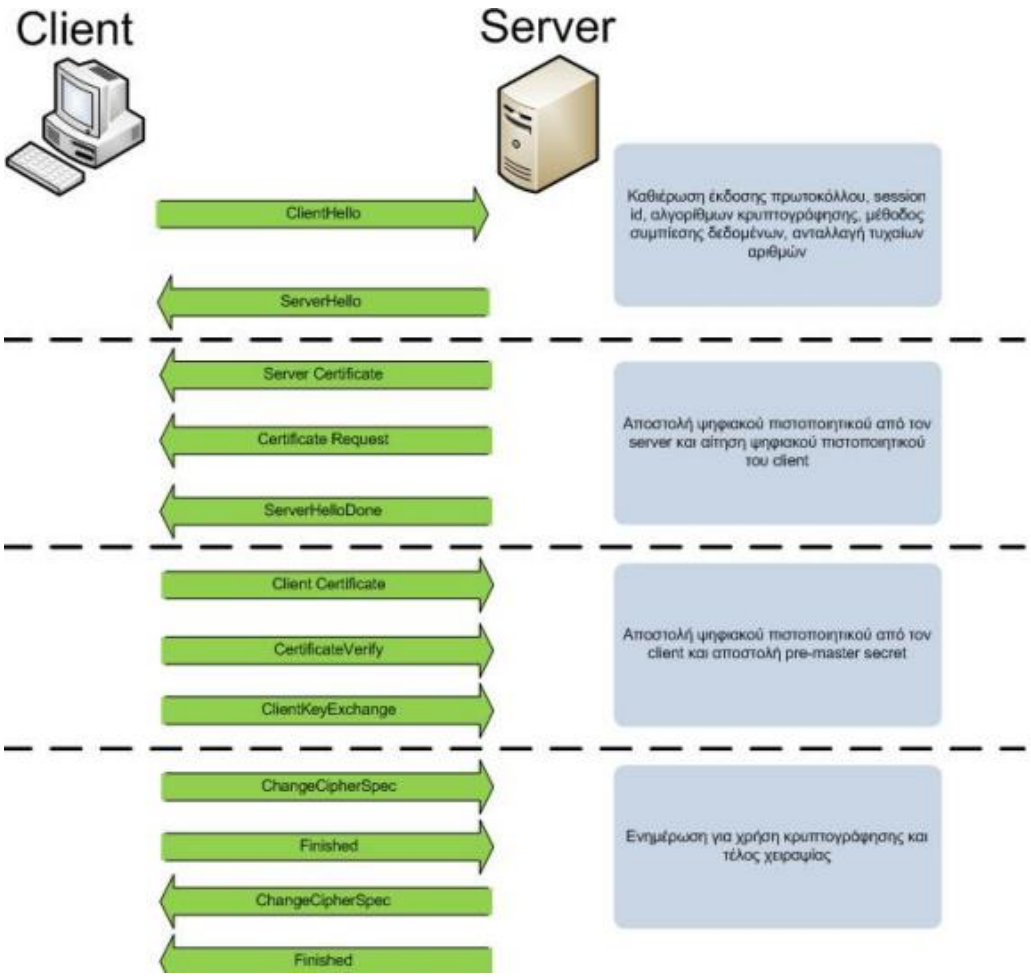
• Τηλεφωνικό διακόπτη Web-configurable-SSL κρυπτογραφεί όλα τα δεδομένα, ώστε κανείς που παρακολουθεί το δίκτυο να διαβάσει τις πληροφορίες σας. Δεδομένου ότι η πρόσβαση στο Διαδίκτυο σημαίνει ότι τα δεδομένα σας πιθανότατα θα ταξιδεύουν μέσω ενός δικτύου ανταγωνιστή, το SSL έχει πολύ νόημα.

• Διαμόρφωση απομακρυσμένης εισόδου - αλλάξτε ταυτόχρονα τον κωδικό πρόσβασης σε όλες τις πόρτες ενός κτιρίου. Το SSL προστατεύει τον κωδικό πρόσβασης, επιτρέποντας στις πόρτες να συνδεθούν σε ένα τυπικό εταιρικό δίκτυο, χωρίς να χρειάζονται ακριβό ιδιόκτητο υλικό! Παρακολούθηση / τιμολόγηση τηλεοπτικού καλωδιακού κουτιού - συνδέστε ένα κουτί καλωδίων στο Διαδίκτυο για να παρακολουθήσετε τη χρήση και να κάνετε online χρέωση.

• Παρακολούθηση / τιμολόγηση βοηθητικών προγραμμάτων (αέριο, ηλεκτρικό, νερό) - σύνδεση με αέριο και ηλεκτρικούς μετρητές στο Διαδίκτυο χωρίς να ανησυχούν οι χρήστες να παραβιάζουν τις πληροφορίες που αποστέλλονται.

Το SSL εφαρμόζεται στα περισσότερα μεγάλα προγράμματα περιήγησης Web που χρησιμοποιούνται από τους καταναλωτές, καθώς και στο λογισμικό εμπορικών διακομιστών, το οποίο υποστηρίζει την εικονική βιτρίνα του πωλητή στον κυβερνοχώρο. Εκατοντάδες εκατομμύρια δολάρια αλλάζουν ήδη τα χέρια όταν οι cybershoppers εισάγουν τους αριθμούς πιστωτικών καρτών τους σε ιστοσελίδες που είναι ασφαλισμένες

με τεχνολογία SSL. Με αυτή την έννοια, το SSL παρέχει ένα ασφαλές κανάλι μεταξύ του καταναλωτή και του εμπόρου για την ανταλλαγή πληροφοριών πληρωμής. Αυτό σημαίνει ότι όλα τα δεδομένα που αποστέλλονται μέσω αυτού του καναλιού είναι κρυπτογραφημένα, ώστε κανένας άλλος από αυτά τα δύο μέρη να μην μπορεί να το διαβάσει.



Εικόνα 7- Τρόπος λειτουργίας

Το SSL προστατεύει το κανάλι επικοινωνιών. Παρέχει επίσης έλεγχο ταυτότητας (στην πλευρά του πελάτη, προαιρετικά στην πλευρά του διακομιστή) των επικοινωνούντων μερών. Το SSL μπορεί να εξασφαλίσει οποιαδήποτε σύνδεση μεταξύ δύο σημείων και κανείς που παρακολουθεί τη σύνδεση δεν μπορεί να καταστρέψει τίποτα ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε οποιαδήποτε ευαίσθητη πληροφορία. Το SSL παρέχει ένα ασφαλές κανάλι χωρίς την ανάγκη να πληρούν τα δύο σύνολα για την ανταλλαγή κλειδιών. Το SSL είναι η εξασφάλιση επικοινωνιών, καθώς το TCP είναι σε κανονικές επικοινωνίες - παρέχει μια τυπική υποδομή επικοινωνιών, την οποία μπορούν να χρησιμοποιήσουν εύκολα και σχεδόν αόρατα οι συμβατές εφαρμογές. Το SSL παρέχει ένα ζωτικής σημασίας στοιχείο σε οποιοδήποτε ασφαλές σύστημα. Οι βασικοί μηχανισμοί ελέγχου ταυτότητας, όπως ο κωδικός Telnet και ο βασικός έλεγχος ταυτότητας HTTP, γίνονται πολύ ισχυρές επιλογές ασφαλείας όταν εκτελούνται με

χρήση SSL αντί απλών TCP-passwords δεν αποστέλλονται πλέον απλού κειμένου, καθιστώντας αυτές τις μεθόδους πολύ πιο χρήσιμες. Το SSL κρυπτογραφεί τη σύνδεση και όχι τα δεδομένα σε κανένα από τα δύο άκρα και δεν περιέχει κανένα μηχανισμό για έλεγχο ταυτότητας χρήστη ή κωδικό πρόσβασης (μόνο η σύνδεση έχει πιστοποιηθεί - η ασφάλεια αποτυγχάνει όταν το μηχάνημα βρίσκεται σε αμφότερα τα άκρα).

Το E Commerce εξυπηρετεί την εμπορία αγαθών και υπηρεσιών μέσω του ηλεκτρονικού μέσου όπως το internet, το κινητό ή οποιοδήποτε άλλο δίκτυο υπολογιστών. Με την αυξανόμενη χρήση του Διαδικτύου σε όλο τον κόσμο, η ηλεκτρονική ανταλλαγή δεδομένων (EDI) έχει επίσης αυξηθεί σε διογκωτικά ποσά και έτσι έχει ευημερήσει το ηλεκτρονικό εμπόριο με το παραγωγικό παζάρι εικονικού διαδικτύου μέσα στον ψηφιακό κόσμο που δικαίως ονομάζεται e-malls το ηλεκτρονικό εμπόριο τότε μπορείτε να αγοράσετε σχεδόν οτιδήποτε επιθυμείτε χωρίς πραγματικά να αγγίζετε το προϊόν σωματικά και να ζητάτε από τον πωλητή n αριθμό φορές πριν από την τοποθέτηση της τελικής παραγγελίας. Εδώ είναι μια όμορφη εικόνα που απεικονίζει τον τρόπο με τον οποίο η ανθρώπινη ζωή εξελίχθηκε για να προσαρμοστεί στον ψηφιακό κόσμο και ως εκ τούτου να εμπορεύεται μέσω του Διαδικτύου.

Οι περισσότερες online αγορές πληρώνονται με πιστωτική κάρτα. Οι έμποροι, όπως οι πληρωμές μέσω πιστωτικών καρτών, επειδή μια άμεση εξουσιοδότηση εγγυάται ότι η κάρτα είναι έγκυρη (σε αντίθεση με μια επιταγή που μπορεί να αναπηδήσει). Οι πελάτες αρέσκονται στην πληρωμή με πιστωτικές κάρτες επειδή μπορούν εύκολα να ακυρώσουν μια συναλλαγή σε περίπτωση που δεν λαμβάνουν προϊόντα ή υπηρεσίες σύμφωνα με τη συμφωνία στη συναλλαγή. Ενώ μερικές από τις πληρωμές με πιστωτικές κάρτες για υπηρεσίες online εκτελούνται μέσω τηλεφώνου, οι περισσότερες από αυτές τις πληρωμές γίνονται συμπληρώνοντας ένα ηλεκτρονικό έντυπο. Τα στοιχεία της πιστωτικής κάρτας που υποβάλλονται από τον πελάτη αποστέλλονται στην τράπεζα που έχει εκδώσει την πιστωτική κάρτα για επαλήθευση. Εάν η συναλλαγή εγκριθεί, ο έμπορος ειδοποιεί τον πελάτη ότι έχει τοποθετηθεί η παραγγελία.

Η πραγματική μεταφορά χρημάτων από την τράπεζα πιστωτικών καρτών στον έμπορο μπορεί να συμβεί σε λίγες ώρες ή ακόμα και σε λίγες μέρες. Οι έμποροι που δέχονται πληρωμές με πιστωτικές κάρτες καταβάλλουν τέλη (μεταξύ 1 και 7% της

χρέωσης της κάρτας) για κάθε χρέωση της κάρτας. Επιπλέον, σε ορισμένες περιπτώσεις οι έμποροι πληρώνουν τέλη εξουσιοδότησης για κάθε απόπειρα εξουσιοδότησης πιστωτικής κάρτας, καθώς και άλλα τέλη που σχετίζονται με την επεξεργασία πιστωτικών καρτών. Αυτή η τεράστια αύξηση στην αφομοίωση του ηλεκτρονικού εμπορίου έχει οδηγήσει σε μια νέα γενιά συναφών απειλών για την ασφάλεια, αλλά κάθε σύστημα ηλεκτρονικού εμπορίου πρέπει να πληροί τέσσερις αναπόσπαστες απαιτήσεις, δηλ. Προστασία της ιδιωτικής ζωής, ακεραιότητα, εξακρίβωση της γνησιότητας και μη επανάληψη.

Ένα πρωτόκολλο που έχει σχεδιαστεί για να διασφαλίζει την ασφάλεια και την ακεραιότητα των ηλεκτρονικών επικοινωνιών και αγορών, η Secure Electronic Transaction (SET) χρησιμοποιεί ψηφιακά πιστοποιητικά, που εκδίδονται σε εμπόρους και άλλες επιχειρήσεις και πελάτες, για να πραγματοποιήσει μια σειρά ελέγχων ασφαλείας, επιβεβαιώνοντας ότι η ταυτότητα ενός πελάτη ή ενός αποστολέα των πληροφοριών είναι έγκυρη. Το SET παρέχει το βασικό πλαίσιο εντός του οποίου λειτουργούν πολλά από τα διάφορα συστατικά της διασφάλισης των ψηφιακών συναλλαγών. Τα ψηφιακά πιστοποιητικά, οι ψηφιακές υπογραφές και τα ψηφιακά πορτοφόλια λειτουργούν σύμφωνα με το πρωτόκολλο SET.

4.1.2.Πλεονεκτήματα και Μειονεκτήματατου SSL

 Διαφάνεια - δεδομένου ότι το SSL παρέχει ασφάλεια στη στρώση περιόδου σύνδεσης, η παρουσία του είναι εντελώς αόρατη είτε στο λογισμικό ηλεκτρονικών καταστημάτων των εμπόρων είτε στον πελάτη. Αυτό είναι ιδιαίτερα σημαντικό για τους εμπόρους επειδή δεν υπάρχει κόστος για την ενσωμάτωση του SSL με τα υπάρχοντα συστήματα τους, εκτός από το κόστος εγκατάστασης του πιστοποιητικού.

 Ευκολία χρήσης για τους πελάτες - το SSL είναι ήδη ενσωματωμένο σε προγράμματα περιήγησης Web που χρησιμοποιούνται συνήθως και δεν υπάρχει ανάγκη εγκατάστασης πρόσθετου λογισμικού.

 Χαμηλή πολυπλοκότητα - το σύστημα δεν είναι περίπλοκο, με αποτέλεσμα την ελάχιστη επίδραση στην ταχύτητα συναλλαγής.

Μειονέκτημα του SSL

Το πρωτόκολλο SSL έχει κάποια σοβαρά προβλήματα όταν πρόκειται να αντιμετωπίσει τις προκλήσεις ασφάλειας του σημερινού χρηματοπιστωτικού τομέα. Παρακάτω αναφέρονται τα σημαντικότερα μειονεκτήματα:

 Ο έμπορος δεν μπορεί να αναγνωρίσει με αξιοπιστία τον κάτοχο της κάρτας.

 Χωρίς διακομιστή τρίτου μέρους, το SSL δεν μπορεί να παρέχει διαβεβαίωση μη αντιποίνων.

 Το SSL κρυπτογραφεί αδιακρίτως όλα τα δεδομένα επικοινωνίας χρησιμοποιώντας την ίδια δύναμη κλειδιού, η οποία είναι περιττή επειδή δεν χρειάζονται όλα τα δεδομένα για το ίδιο επίπεδο προστασίας. Για παράδειγμα, ένας αριθμός πιστωτικής κάρτας χρειάζεται ισχυρότερη κρυπτογράφηση από μια λίστα στοιχείων παραγγελιών. Χρησιμοποιώντας την ίδια δύναμη κλειδιού και για τις δύο δημιουργεί περιττές υπολογιστικές επιβαρύνσεις.

Με άλλα λόγια, το SSL μπορεί να μας δώσει εμπιστευτικές επικοινωνίες, εισάγει επίσης τεράστιους κινδύνους:

 Ο κάτοχος της κάρτας προστατεύεται από τους υποκλοπών, αλλά όχι από τον έμπορο.

 Ο έμπορος δεν έχει προστατευθεί από τους ανέντιμους πελάτες που παρέχουν άκυρο αριθμό πιστωτικής κάρτας ή που ζητούν επιστροφή από την τράπεζά τους χωρίς αιτία. Σε αντίθεση με την κοινή πεποίθηση, δεν είναι ο κάτοχος της κάρτας, αλλά ο έμπορος που έχει τα περισσότερα να χάσει από την απάτη. Η νομοθεσία στις περισσότερες χώρες προστατεύει τον καταναλωτή

4.2. Τοπρωτόκολλο SET Secure Electronic Transaction (SET)

Το ηλεκτρονικό εμπόριο, όπως εξηγείται από τη δημοτικότητα του Διαδικτύου, θα έχει τεράστιο αντίκτυπο στον κλάδο των χρηματοπιστωτικών υπηρεσιών. Κανένα

χρηματοπιστωτικό ίδρυμα δεν θα παραμείνει ανεπηρέαστο από την έκρηξη του ηλεκτρονικού εμπορίου. Παρόλο που το SSL είναι εξαιρετικά αποτελεσματικό και ευρέως αποδεκτό ως πρότυπο ηλεκτρονικής πληρωμής, απαιτεί από τον πελάτη και τον έμπορο να εμπιστεύονται ο ένας τον άλλον. Μια ανεπιθύμητη απαίτηση, ακόμη και σε συναλλαγές πρόσωπο με πρόσωπο, και σε όλο το Διαδίκτυο αναγνωρίζει απαράδεκτους κινδύνους. Η MasterCard και η VISA ανέπτυξαν το SET σε συνεργασία με κορυφαίες εταιρείες τεχνολογίας, συμπεριλαμβανομένων των Microsoft, IBM, Netscape, SAIC, GTE, RSA, Terisa Systems και VeriSign. Την 1η Φεβρουαρίου 1996, αυτές οι εταιρείες ανακοίνωσαν το ενιαίο τεχνικό πρότυπο για τη διασφάλιση των αγορών πληρωμών που πραγματοποιούνται μέσω ανοικτών δικτύων. Αυτό το πρότυπο καλείται ως προδιαγραφή SET Secure Electronic Transaction. Η προδιαγραφή SET περιλαμβάνει ψηφιακά πιστοποιητικά, τα οποία επαληθεύουν την πραγματική ταυτότητα των μερών που συμμετέχουν στη συναλλαγή. Χρησιμοποιώντας αυτές τις εξελιγμένες κρυπτογραφικές τεχνικές, το πρωτόκολλο SET, στοχεύει να καταστήσει τον κυβερνοχώρο έναν ασφαλέστερο χώρο για τη διεξαγωγή επιχειρήσεων και με τον τρόπο αυτό να αυξήσει την εμπιστοσύνη των καταναλωτών στο ECommerce. Το SET αναπτύχθηκε για να αντιμετωπίσει αυτές τις σημαντικές απαιτήσεις στη βιομηχανία ηλεκτρονικών αγορών: [

 Παροχή εμπιστευτικότητας των πληροφοριών - επιτυγχάνεται με τη χρήση κρυπτογράφησης μηνυμάτων.

 Εξασφάλιση της ακεραιότητας όλων των μεταδιδόμενων δεδομένων - επιτυγχάνεται με τη χρήση ψηφιακών υπογραφών. κάτοχος κάρτας που σημαίνει ότι είναι ο νόμιμος χρήστης της κάρτας πληρωμής με επωνυμία - που επιτυγχάνεται με τη χρήση ψηφιακών υπογραφών και πιστοποιητικών κατόχων καρτών

 Πιστοποίηση ενός εμπόρου να δέχεται συναλλαγές με κάρτες πληρωμών και να εξασφαλίζει τη σχέση του με ένα αποκτών χρηματοπιστωτικό ίδρυμα - επιτυγχάνεται με τη χρήση ψηφιακών υπογραφών και εμπορικά πιστοποιητικά

 Προστασία όλων των νόμιμων μέρη που συμμετέχουν στη συναλλαγή χρησιμοποιώντας τις βέλτιστες πρακτικές ασφαλείας

 Διευκολύνετε τη διαλειτουργικότητα μεταξύ παρόχων λογισμικού και δικτύων - επιτυγχάνεται με τη χρήση συγκεκριμένων πρωτοκόλλων και μορφών μηνυμάτων.

Το SET είναι μια ανοικτή προδιαγραφή κρυπτογράφησης και ασφάλειας που έχει σχεδιαστεί για την προστασία των συναλλαγών με πιστωτικές κάρτες στο Διαδίκτυο. Η τρέχουσα έκδοση, SETv1, προέκυψε από την πρόσκληση για πρότυπα ασφαλείας από τη MasterCard και τη Visa τον Φεβρουάριο του 1996.

Ένα ευρύ φάσμα εταιρειών συμμετείχε στην ανάπτυξη των αρχικών προδιαγραφών, συμπεριλαμβανομένων των IBM, Microsoft, Netscape, RSA, Terisa και Verisign. Ξεκινώντας από το 1996. Το SET δεν είναι το ίδιο σύστημα πληρωμών (Lietal, 2014).

Πρόκειται μάλλον για ένα σύνολο πρωτοκόλλων και μορφών ασφαλείας που επιτρέπουν στους χρήστες να χρησιμοποιούν την υπάρχουσα υποδομή πληρωμής με πιστωτικές κάρτες σε ένα ανοικτό δίκτυο, όπως το Διαδίκτυο, με ασφαλή τρόπο (Abood, 2017).

Στην ουσία, το SET παρέχει τρεις υπηρεσίες:

• Παρέχει ένα ασφαλές κανάλι επικοινωνίας μεταξύ όλων των εμπλεκομένων σε μια συναλλαγή

• Παρέχει εμπιστοσύνη από τη χρήση ψηφιακών πιστοποιητικών X.509v3

• Εξασφαλίζει την προστασία της ιδιωτικής ζωής, επειδή οι πληροφορίες είναι διαθέσιμες μόνο σε μέρη μιας συναλλαγής όταν και όπου

Απαιτήσεις. SET: Ένας καλός τρόπος για να ξεκινήσουμε τη συζήτησή μας για το SET είναι να εξετάσουμε τις επιχειρηματικές απαιτήσεις για το SET, τα βασικά χαρακτηριστικά του και τους συμμετέχοντες στις συναλλαγές SET. Απαιτήσεις: Η προδιαγραφή SET απαριθμεί τις ακόλουθες επιχειρηματικές απαιτήσεις για ασφαλή επεξεργασία πληρωμών με πιστωτικές κάρτες μέσω Διαδικτύου και άλλων δικτύων:

• Παροχή εμπιστευτικότητας των πληροφοριών πληρωμής και παραγγελίας: Είναι απαραίτητο να διασφαλιστεί ότι οι πληροφορίες αυτές είναι ασφαλείς και προσπελάσιμες μόνο παραλήπτης. Η εμπιστευτικότητα μειώνει επίσης τον κίνδυνο απάτης από οποιοδήποτε μέρος της συναλλαγής ή από κακόβουλα τρίτα μέρη. Το SET χρησιμοποιεί κρυπτογράφηση για την παροχή εμπιστευτικότητας.

• Εξασφάλιση ακεραιότητας όλων των μεταδιδόμενων δεδομένων: Δηλαδή, βεβαιωθείτε ότι δεν εμφανίζονται αλλαγές στο περιεχόμενο κατά τη μετάδοση των μηνυμάτων SET. Οι ψηφιακές υπογραφές χρησιμοποιούνται για την παροχή ακεραιότητας.

• Καθορισμός ότι ένας κάτοχος κάρτας είναι νόμιμος χρήστης ενός λογαριασμού πιστωτικής κάρτας: Ένας μηχανισμός που συνδέει έναν κάτοχο κάρτας με έναν συγκεκριμένο αριθμό λογαριασμού μειώνει τη συχνότητα απάτης και το συνολικό κόστος της επεξεργασίας πληρωμών. Οι ψηφιακές υπογραφές και πιστοποιητικά χρησιμοποιούνται για να επαληθεύσουν ότι ένας κάτοχος κάρτας είναι νόμιμος χρήστης ενός έγκυρου λογαριασμού.

• Καθορισμός ότι ένας έμπορος μπορεί να δεχτεί συναλλαγές με πιστωτικές κάρτες μέσω της σχέσης του με ένα χρηματοπιστωτικό ίδρυμα: Αυτό είναι το συμπλήρωμα της προηγούμενης απαίτησης. Οι κάτοχοι καρτών πρέπει να είναι σε θέση να εντοπίζουν εμπόρους με τους οποίους μπορούν να διεξάγουν ασφαλείς συναλλαγές. Και πάλι, χρησιμοποιούνται ψηφιακές υπογραφές και πιστοποιητικά(Lietal, 2014).

• Εξασφάλιση της χρήσης των βέλτιστων πρακτικών ασφαλείας και των τεχνικών σχεδιασμού του συστήματος για την προστασία όλων των νόμιμων μερών σε μια συναλλαγή ηλεκτρονικού εμπορίου: Το SET είναι μια καλά δοκιμασμένη προδιαγραφή που βασίζεται σε εξαιρετικά ασφαλείς κρυπτογραφικούς αλγόριθμους και πρωτόκολλα.

• Δημιουργίαενός πρωτόκολλου που δεν εξαρτάται ούτε από τους μηχανισμούς ασφαλείας μεταφοράς ούτε εμποδίζει τη χρήση τους: Το SET μπορεί να λειτουργήσει με ασφάλεια σε μια "ακατέργαστη" στοίβα TCP / IP. Ωστόσο, το SET δεν παρεμβαίνει στη χρήση άλλων μηχανισμών ασφαλείας, όπως το IPSec και το SSL / TLS.

• Διευκόλυνση και ενθάρρυνση της διαλειτουργικότητας μεταξύ παρόχων λογισμικού και δικτύων: Τα πρωτόκολλα και οι μορφές SET είναι ανεξάρτητα από την πλατφόρμα υλικού, το λειτουργικό σύστημα και το λογισμικό Ιστού.

Παράδειγμα λειτουργίας του πρωτοκόλλου SET

Σε μια εφαρμογή SET, ο έμπορος προσαρμόζει τις φόρμες παραγγελίας ώστε να επιτρέψει στους αγοραστές να ζητήσουν από το διακομιστή εμπόρων το μήνυμα έναρξης πληρωμής, επίσης γνωστό ως μήνυμα αφύπνισης. Όταν ο περιηγητής ιστού του αγοραστή λάβει αυτό το μήνυμα έναρξης πληρωμής, οι αγοραστές προσδιορίζουν τις πληροφορίες της κάρτας πληρωμής. Μετά την εισαγωγή του αρχείου πληροφοριών πληρωμής, ο περιηγητής εκκινεί μηχανισμό ελέγχου ταυτότητας για τον κάτοχο κάρτας. Ένας κωδικός επαλήθευσης αποστέλλεται στο κινητό τηλέφωνο του κατόχου κάρτας. Εκτός και μέχρι να εισαχθεί αυτός ο κωδικός, η σειρά δεν είναι τοποθετημένη. Εισάγοντας τον κωδικό επαλήθευσης, ο κάτοχος της κάρτας επικυρώνεται και η παραγγελία γίνεται μετά την υποβολή του κώδικα.

Όταν υποβληθεί το έντυπο, οι πληροφορίες πιστωτικής κάρτας κρυπτογραφούνται χρησιμοποιώντας SSL. Στη συνέχεια μεταβιβάζεται στον αποκτώντα, χρησιμοποιώντας τα κανονικά μηνύματα SET, μέσω της πλατφόρμας πληρωμής. Δεδομένου ότι το πρωτόκολλο SET αρχίζει από τον εμπορικό διακομιστή, πρέπει να αλλάξετε τον τρόπο επεξεργασίας των συναλλαγών και των API σε σύγκριση με τη διαδικασία με ένα πορτοφόλι. Η διαδικασία εξηγείται στη λίστα που ακολουθεί.

 Ο κάτοχος της κάρτας αποφασίζει να πραγματοποιήσει μια αγορά. Όταν ο κάτοχος κάρτας κάνει κλικ στο κουμπί Αγορά, αποστέλλεται μια εντολή στο διακομιστή εμπόρου.

 Ο εμπορικός διακομιστής καλεί το API etAcceptPayment () του διακομιστή πληρωμών.

 Ο διακομιστής πληρωμών ελέγχει για να διαπιστώσει εάν πρέπει να γίνει η εξουσιοδότηση σε αυτό το σημείο. Για παράδειγμα, εάν ο αγοραστής του εμπόρου είναι διαθέσιμος. Όταν μπορεί να γίνει η εξουσιοδότηση, ο διακομιστής δημιουργεί ένα αίτημα εξουσιοδότησης (AuthReq) το αποστέλλει στον αποκτώντα, και περιμένει ένα μήνυμα απάντησης εξουσιοδότησης (AuthRes).

 Το λογισμικό αγοραστή ή η πύλη πληρωμών λαμβάνει το αίτημα. Χρησιμοποιώντας ένα κανονικό δίκτυο back-end ή άλλα κανάλια επικοινωνίας, το απορροφούμενο ίδρυμα επικοινωνεί με το ίδρυμα έκδοσης του κατόχου της κάρτας.

Ελέγχει ότι η κάρτα πληρωμής είναι έγκυρη και ότι ο κάτοχος της κάρτας διαθέτει επαρκή κεφάλαια ή πίστωση για την πραγματοποίηση της αγοράς.

 Το μήνυμα AuthRes λαμβάνεται από το διακομιστή πληρωμών και υποβάλλεται σε επεξεργασία. Οι πληροφορίες αποθηκεύονται στη βάση δεδομένων για καταγραφή και περαιτέρω επεξεργασία παραγγελιών.

 Ο έμπορος μπορεί τώρα να εκπληρώσει τη σειρά. Όταν τα αγαθά αποστέλλονται, ο έμπορος ζητά την πληρωμή καλώντας το etDeposit () API.

 Ο διακομιστής πληρωμών ξεκινά τώρα τη διαδικασία λήψης στέλνοντας ένα αίτημα καταγραφής στη Gateway πληρωμής. Η σύλληψη είναι η μεταφορά κεφαλαίων από τον αγοραστή του εμπόρου στον έμπορο και στη συνέχεια στον αποκτώντα του εμπόρου από το ίδρυμα έκδοσης του κατόχου της κάρτας.

 Η πύλη πληρωμής λαμβάνει το αίτημα λήψης και στέλνει ένα μήνυμα απόκρισης λήψης.

 Η πύλη πληρωμής χρησιμοποιεί το κλειστό (back-end) δίκτυο για να επικοινωνήσει με τον αγοραστή του εμπόρου και ζητά τη μεταφορά της πληρωμής. Ο αγοραστής καταθέτει την πληρωμή στο λογαριασμό του εμπόρου.

 Ο έμπορος εξυπηρετητής στέλνει την επιβεβαίωση στον κάτοχο της κάρτας.

 Η τράπεζα έκδοσης του κατόχου της κάρτας καταθέτει την πληρωμή στον τραπεζικό λογαριασμό του εμπόρου και ενημερώνει το λογαριασμό του κατόχου της κάρτας στην τράπεζα έκδοσης του κατόχου της κάρτας.

5 Ο – ΚΕΦΑΛΑΙΟ- ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΕΦΑΡΜΟΓΗ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ SSL

Για την καλύτερη και βαθύτερη κατανόηση του τρόπου λειτουργίας του πιστοποιητικού SSL, παρατίθενται ορισμένες τεχνικές λεπτομέρειες καθώς και μια μελέτη περίπτωσης ενός πιστοποιητικού στην ηλεκτρονική τραπεζική της τράπεζας «Πειραιώς»/

5.1. Τομείς Εφαρμογής των πιστοποιητικών SSL / TLS

Οι εφαρμογές SSL / TLS μπορούν να χρησιμοποιηθούν με πολλούς τρόπους και για διάφορους σκοπούς, όπως: Επικοινωνίες μεταξύ περιηγητών-διακομιστών Συχνά, το SSL / TLS χρησιμοποιείται για την εξασφάλιση επικοινωνιών μεταξύ ενός διακομιστή ιστού και ενός προγράμματος περιήγησης ιστού, μεταδίδεται. Αυτές οι πληροφορίες μπορεί να αφορούν μια ηλεκτρονική αγορά, ιατρικά δεδομένα ασθενούς ή τραπεζικά στοιχεία. Το SSL / TLS διασφαλίζει ότι ο χρήστης του προγράμματος περιήγησης ιστού γνωρίζει σε ποιόν διαβιβάζονται οι πληροφορίες του και ότι μόνο ο προοριζόμενος παραλήπτης μπορεί να έχει πρόσβαση στις πληροφορίες.

Οι επικοινωνίες μεταξύ διακομιστών SSL / TLS μπορούν επίσης να χρησιμοποιηθούν για την εξασφάλιση επικοινωνιών μεταξύ δύο διακομιστών, όπως δύο επιχειρήσεις που συνεργάζονται μεταξύ τους. Σε αυτό το σενάριο, και οι δύο διακομιστές έχουν συνήθως ένα πιστοποιητικό, αλληλοεξουδετερώνοντάς τα μεταξύ τους καθώς και εξασφαλίζοντας τις επικοινωνίες μεταξύ τους.

Παράδειγμα SSL / TLS

Όταν οι χρήστες επισκέπτονται έναν ιστότοπο ο οποίος έχει ασφαλιστεί με πιστοποιητικό SSL / TLS, το πρόγραμμα περιήγησης ιστού τους παρέχει οπτικές ενδείξεις για να τους ενημερώσει ότι λειτουργεί το SSL / TLS. Ένα σημαντικό παράδειγμα είναι η διεύθυνση που εμφανίζεται στο πεδίο διεύθυνσης του προγράμματος περιήγησης, το οποίο θα αρχίσει με "https: //" για μια ασφαλή σύνδεση SSL / TLS και "http: //" για μη ασφαλείς συνδέσεις. Τα περισσότερα προγράμματα περιήγησης εμφανίζουν επίσης κάποιο είδος εικονιδίου κλειδώματος (βλ. Εικόνα 8), αν και η

τοποθεσία και η εμφάνιση θα διαφέρουν από το πρόγραμμα περιήγησης στο πρόγραμμα περιήγησης

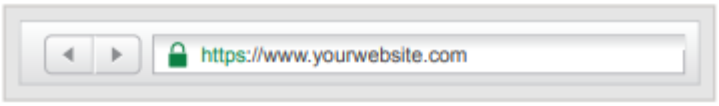


Figure 1: What visitors might see if they access an encrypted website.

Εικόνα 8-

Τα προγράμματα περιήγησης ενδέχεται επίσης να επιτρέπουν στο χρήστη να κάνει κλικ στο εικονίδιο κλειδώματος για να προβάλετε περισσότερες πληροφορίες σχετικά με το πιστοποιητικό.

• Την ημερομηνία έναρξης και λήξης της εγκυρότητας του πιστοποιητικού. Όπως και οι περισσότερες άλλες μορφές αναγνώρισης, τα ψηφιακά πιστοποιητικά λήγουν και πρέπει να ανανεωθούν, επιτρέποντας στην ΑΠ να επαληθεύσει την ταυτότητα του κατόχου του πιστοποιητικού. Ισχυρή επικύρωση πιστοποιητικού Υπάρχουν διαθέσιμοι τρεις διαθέσιμοι τύποι πιστοποιητικών SSL / TLS, καθένας με διαφορετικά επίπεδα επικύρωσης: επικύρωση τομέα (DV), επαλήθευση οργανισμού (OV) και, πιο πρόσφατα, εκτεταμένη επικύρωση (EV). Τα πιστοποιητικά DV εκδίδονται πολύ γρήγορα, αλλά δεν υπάρχουν στοιχεία εταιρείας που να ελέγχονται ή να εμφανίζονται στο πιστοποιητικό. Με την OV, εμφανίζονται στους επισκέπτες ορατά οι τελευταίες πληροφορίες για την εταιρεία, οι οποίες μπορεί να περιλαμβάνουν τη διεύθυνση της εταιρείας ή το όνομα μιας συγκεκριμένης επαφής με την εταιρεία.

Αυτές οι δύο επιλογές λειτουργούν καλά για καταστάσεις όπου η εμπιστοσύνη και η αξιοπιστία ενός ιστότοπου είναι λιγότερο σημαντικές, είτε επειδή ο ιστότοπος δεν αντιμετωπίζει τον καταναλωτή, είτε ο ιστότοπος δεν περιλαμβάνει κωδικούς πρόσβασης, πληρωμές ή άλλα ευαίσθητα δεδομένα. Έτσι, ως τρόπος να βοηθήσουμε τους ιστότοπους και τους καταναλωτές να διαφοροποιήσουν μεταξύ των τριών και να εξασφαλίσουν μια ασφαλή συνολική υποδομή διαδικτύου για ιστότοπους που μεταφέρουν ευαίσθητες

πληροφορίες, το CA / BrowserForum, μια ανεξάρτητη βιομηχανική ομάδα, δημιούργησε οδηγίες για ένα πιστοποιητικό EV.

Ένα πιστοποιητικό EV είναι ένα πιστοποιητικό SSL / TLS που απαιτεί από την ΑΠ εκδότρια να λάβει αυστηρά μέτρα για την επικύρωση της ταυτότητας του αιτούντος πιστοποιητικού. Οι αρχές πιστοποίησης πρέπει επίσης να διενεργήσουν ανεξάρτητο έλεγχο των διαδικασιών επικύρωσής τους προκειμένου να συνεχίσουν να προσφέρουν πιστοποιητικά EV, πράγμα που σημαίνει ότι τα πιστοποιητικά EV τείνουν να είναι διαθέσιμα μόνο από κορυφαίες, αξιόπιστες ΑΠ, όπως η Symantec. Αυτά τα βελτιωμένα οπτικά στοιχεία από τα πιστοποιητικά EV καθιστούν ευκολότερο για τους χρήστες να επιβεβαιώνουν θετικά την ταυτότητα του ιστοτόπου με τον οποίο επικοινωνούν. Οι χρήστες που βλέπουν την ετικέτα "NotSecure" δίπλα από τη διεύθυνση ιστού σας ενδέχεται να σταματήσουν στη μέση της διαδικασίας εγγραφής, να εγκαταλείψουν το καλάθι αγορών τους ή απλά να σταματήσουν να διαβάζουν και να κλείνουν την καρτέλα

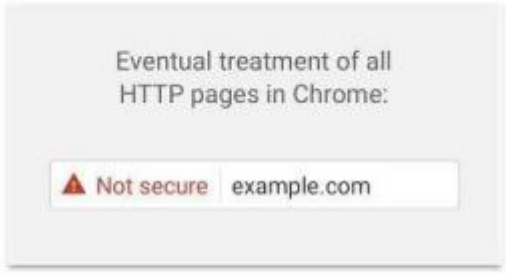


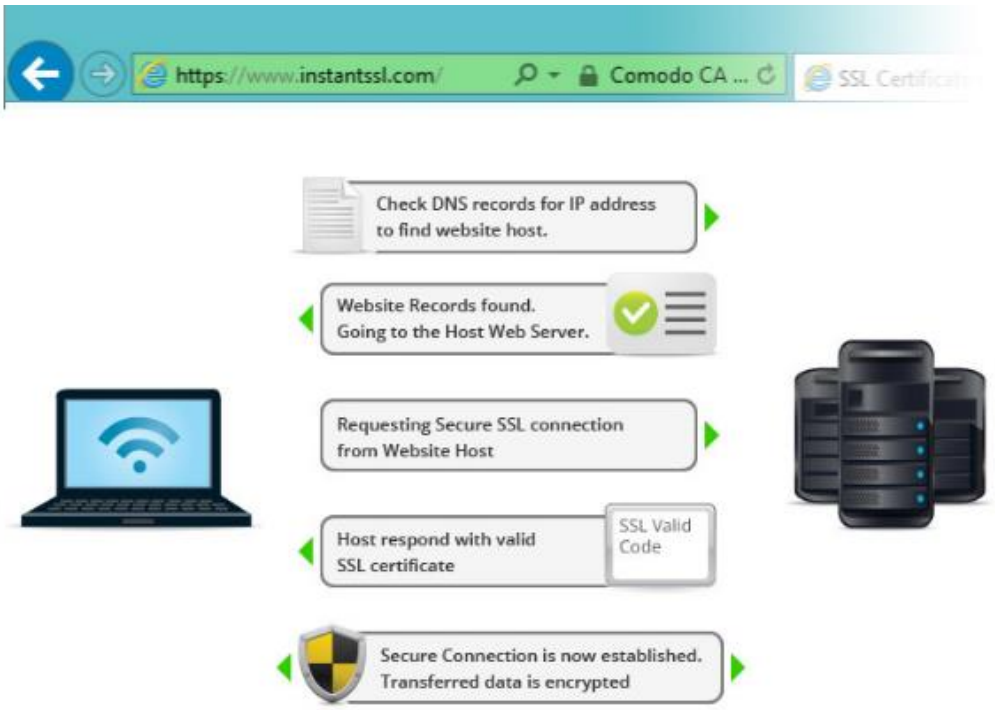
Figure 3: Many web browsers will begin showing "Not Secure" warnings on many websites that are unencrypted.

5.2. Βήματα λειτουργίας του πρωτοκόλλου

Ένας τελικός χρήστης ζητάει από το πρόγραμμα περιήγησής του να κάνει ασφαλή σύνδεση με έναν ιστότοπο (π.χ.https: //www.example.com). Το πρόγραμμα περιήγησης αποκτά τη διεύθυνση IP του ιστότοπου από έναν διακομιστή DNS και στη συνέχεια ζητά μια ασφαλή σύνδεση στον ιστότοπο. Για να ξεκινήσει αυτή η ασφαλής σύνδεση, το πρόγραμμα περιήγησης ζητά από τον ίδιο τον διακομιστή να στείλει ένα αντίγραφο του πιστοποιητικού SSL στο πρόγραμμα περιήγησης. Το πρόγραμμα περιήγησης ελέγχει το πιστοποιητικό για να βεβαιωθεί: ότι είναι υπογεγραμμένο από αξιόπιστη ΑΠ. Είναι

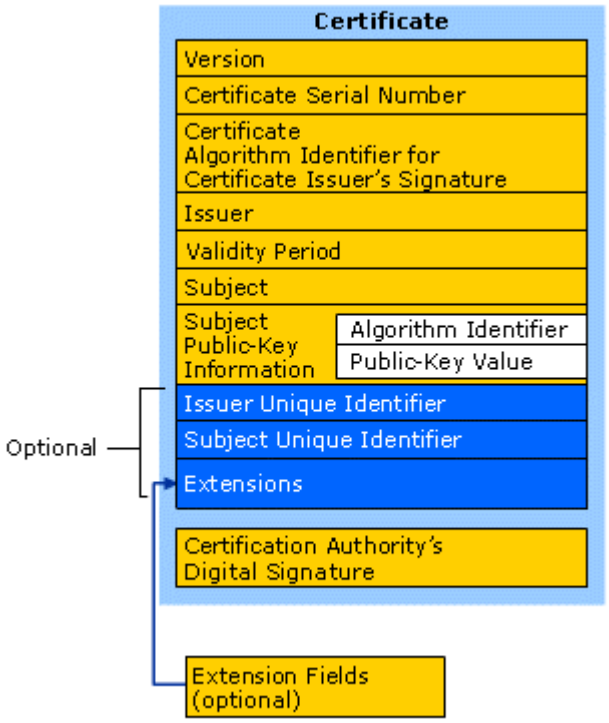
έγκυρο - ότι δεν έχει λήξει ή έχει ανακληθεί. Αυτό επιβεβαιώνει τα απαιτούμενα πρότυπα ασφαλείας για τα βασικά μήκη και άλλα στοιχεία.

Ότι ο τομέας που αναφέρεται στο πιστοποιητικό αντιστοιχεί στον τομέα που ζητήθηκε από τον χρήστη. Όταν το πρόγραμμα περιήγησης επιβεβαιώσει ότι ο ιστότοπος μπορεί να σκουριάζει, δημιουργεί ένα συμμετρικό κλειδί συνεδρίας το οποίο κρυπτογραφεί με το δημόσιο κλειδί στο πιστοποιητικό του ιστότοπου. Στη συνέχεια, το κλειδί περιόδου σύνδεσης αποστέλλεται στον διακομιστή ιστού. Ο διακομιστής ιστού χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το κλειδί συμμετρικής συνόδου. Ο διακομιστής στέλνει μια επιβεβαίωση που είναι κρυπτογραφημένη με το κλειδί της περιόδου σύνδεσης. Από εδώ και πέρα, όλα τα δεδομένα που μεταδίδονται μεταξύ του διακομιστή και του προγράμματος περιήγησης είναι κρυπτογραφημένα και ασφαλή.



5.3. «Ανατομία» του Ψηφιακού Πιστοποιητικού

Στην εικόνα τα περιεχόμενα των πιστοποιητικών X.509 έκδοσης 3



Εικόνα 9- Περιεχόμενα πιστοποιητικού X.509 έκδοση 3

Τα πιστοποιητικά X.509 έκδοσης 3 υποστηρίζουν τα ακόλουθα πεδία που υποστηρίζονται από την έκδοση X.509: Θέμα: Παρέχει το όνομα του υπολογιστή, του χρήστη, της συσκευής δικτύου ή της υπηρεσίας στην οποία η ΑΠ εκδίδει το πιστοποιητικό. Το όνομα του αντικειμένου αντιπροσωπεύεται συνήθως χρησιμοποιώντας μια μορφή X.500 ή LightweightDirectoryAccessProtocol (LDAP).

Σειριακός αριθμός: Παρέχει ένα μοναδικό αναγνωριστικό για κάθε πιστοποιητικό που εκδίδει μια ΑΠ. Εκδότης: Παρέχει ένα διακριτικό όνομα για την ΑΠ που εξέδωσε το πιστοποιητικό. Το όνομα του εκδότη αντιπροσωπεύεται συνήθως χρησιμοποιώντας μια μορφή X.500 ή LDAP. Ισχύει από: Παρέχει την ημερομηνία και την ώρα έναρξης ισχύος του πιστοποιητικού.

ValidTo: Παρέχει την ημερομηνία και την ώρα που το πιστοποιητικό δεν θεωρείται πλέον έγκυρο. Η ημερομηνία κατά την οποία μια εφαρμογή ή μια υπηρεσία αξιολογεί το πιστοποιητικό πρέπει να εμπίπτει μεταξύ των πεδίων ValidFrom και ValidTo του πιστοποιητικού ώστε το πιστοποιητικό να θεωρηθεί έγκυρο.

Δημόσιο κλειδί: Περιέχει το δημόσιο κλειδί του ζεύγους κλειδιών που σχετίζεται με το πιστοποιητικό.

Αλγόριθμος υπογραφής: Ο αλγόριθμος που χρησιμοποιείται για την υπογραφή του πιστοποιητικού. Τιμή υπογραφής: Μορφή bit που περιέχει την ψηφιακή υπογραφή.

Εκτός από τα πεδία της έκδοσης 1, τα πιστοποιητικά X.509 έκδοσης 3 περιλαμβάνουν επεκτάσεις που προσφέρουν πρόσθετες λειτουργίες και δυνατότητες στο πιστοποιητικό. Αυτές οι επεκτάσεις είναι προαιρετικές και δεν περιλαμβάνονται υποχρεωτικά σε κάθε πιστοποιητικό που εκδίδει η ΑΠ: Αντικείμενο εναλλακτικό όνομα: Ένα θέμα μπορεί να παρουσιαστεί σε πολλές διαφορετικές μορφές.

Για παράδειγμα, εάν το πιστοποιητικό πρέπει να περιλαμβάνει όνομα λογαριασμού χρήστη με τη μορφή διακριτικού ονόματος LDAP, όνομα ηλεκτρονικού ταχυδρομείου και όνομα κύριου χρήστη (UPN), μπορείτε να συμπεριλάβετε το όνομα ηλεκτρονικού ταχυδρομείου ή το UPN σε ένα πιστοποιητικό προσθέτοντας μια υποκείμενη εναλλακτική επέκταση ονόματος που περιλαμβάνει αυτές τις πρόσθετες μορφές ονόματος.

Σημεία διανομής CRL (CDP): Όταν ένας χρήστης, υπηρεσία ή υπολογιστής παρουσιάζει ένα πιστοποιητικό, μια εφαρμογή ή μια υπηρεσία πρέπει να καθορίσει εάν το πιστοποιητικό έχει ανακληθεί πριν από τη λήξη της περιόδου ισχύος του. Η επέκταση CDP παρέχει μία ή περισσότερες διευθύνσεις URL όπου η εφαρμογή ή η υπηρεσία μπορεί να ανακτήσει τη λίστα ανάκλησης πιστοποιητικών (CRL) από.

Αρχή πρόσβασης πληροφοριών (AIA): Αφού μια εφαρμογή ή μια υπηρεσία επικυρώσει ένα πιστοποιητικό, το πιστοποιητικό της ΑΠ που εξέδωσε το πιστοποιητικό - επίσης γνωστό ως μητρική CA - πρέπει επίσης να αξιολογηθεί για ανάκληση και εγκυρότητα. Η επέκταση AIA παρέχει μία ή περισσότερες διευθύνσεις URL από τις οποίες μια εφαρμογή ή υπηρεσία μπορεί να ανακτήσει το πιστοποιητικό της ΑΠ εκδότη.

Ενισχυμένη χρήση κλειδιών (EKU): Αυτό το χαρακτηριστικό περιλαμβάνει ένα αναγνωριστικό αντικειμένου (OID) για κάθε εφαρμογή ή υπηρεσία για την οποία μπορεί να χρησιμοποιηθεί ένα πιστοποιητικό. Κάθε OID είναι μια μοναδική ακολουθία αριθμών από ένα παγκόσμιο μητρώο.

Πολιτικές πιστοποιητικών: Περιγράφει τα μέτρα που λαμβάνει ένας οργανισμός για την επικύρωση της ταυτότητας ενός αιτούντος πιστοποιητικού πριν εκδώσει ένα πιστοποιητικό. Ένα OID χρησιμοποιείται για να αντιπροσωπεύει τη διαδικασία επικύρωσης και μπορεί να περιλαμβάνει μια διεύθυνση URL κατάλληλη για την πολιτική, η οποία περιγράφει πλήρως τα μέτρα που ελήφθησαν για την επικύρωση της ταυτότητας. Ταξινόμηση Οι εμπορικές ΑΠ χρησιμοποιούν την έννοια των τάξεων για διαφορετικούς τύπους ψηφιακών πιστοποιητικών. Για παράδειγμα, η VeriSign έχει την ακόλουθη ταξινόμηση

Κατηγορία 1 για άτομα, προοριζόμενα για ηλεκτρονικό ταχυδρομείο.

Κλάση 2 για οργανισμούς, για τους οποίους απαιτείται απόδειξη ταυτότητας.

Κλάση 3 για την υπογραφή διακομιστών και λογισμικού, για την οποία η ανεξάρτητη επαλήθευση και έλεγχος ταυτότητας και εξουσιοδότησης γίνεται από την αρχή έκδοσης πιστοποιητικών.

Κλάση 4 για ηλεκτρονικές συναλλαγές μεταξύ επιχειρήσεων.

Κλάση 5 για ιδιωτικούς οργανισμούς ή κυβερνητική ασφάλεια. Άλλοι προμηθευτές μπορούν να επιλέξουν να χρησιμοποιήσουν διαφορετικές κλάσεις ή καθόλου κλάσεις, καθώς αυτό δεν ορίζεται στις προδιαγραφές, αν και οι περισσότεροι προτιμούν να χρησιμοποιούν τάξεις σε κάποια μορφή.

Μορφή και κωδικοποίηση πιστοποιητικών

Οι μορφές ψηφιακών πιστοποιητικών X.509 ορίζονται με τη χρήση του ASN.1 ή της σύνταξης Η συμβολική σύνταξη 1 είναι μια μορφή εκπροσώπησης δεδομένων του Διεθνούς Οργανισμού Τυποποίησης (ISO) που χρησιμοποιείται για την επίτευξη διαλειτουργικότητας μεταξύ των πλατφορμών.

Η τρέχουσα δομή ενός ψηφιακού πιστοποιητικού X.509 v3 φαίνεται στην εικόνα 10.

```
Certificate  ::=  SEQUENCE  {
        tbsCertificate       TBSCertificate,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
        version         [0]  EXPLICIT Version DEFAULT v1,
        serialNumber         CertificateSerialNumber,
        signature            AlgorithmIdentifier,
        issuer               Name,
        validity             Validity,
        subject              Name,
        subjectPublicKeyInfo SubjectPublicKeyInfo,
        issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version MUST be v2 or v3
        subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version MUST be v2 or v3
        extensions      [3]  EXPLICIT Extensions OPTIONAL
                             -- If present, version MUST be v3
        }
AlgorithmIdentifier  ::=  SEQUENCE  {
        algorithm               OBJECT IDENTIFIER,
        parameters              ANY DEFINED BY algorithm OPTIONAL  }

.... More definitions will follow for CertificateSerialNumber, Name, Validity etc ...
```

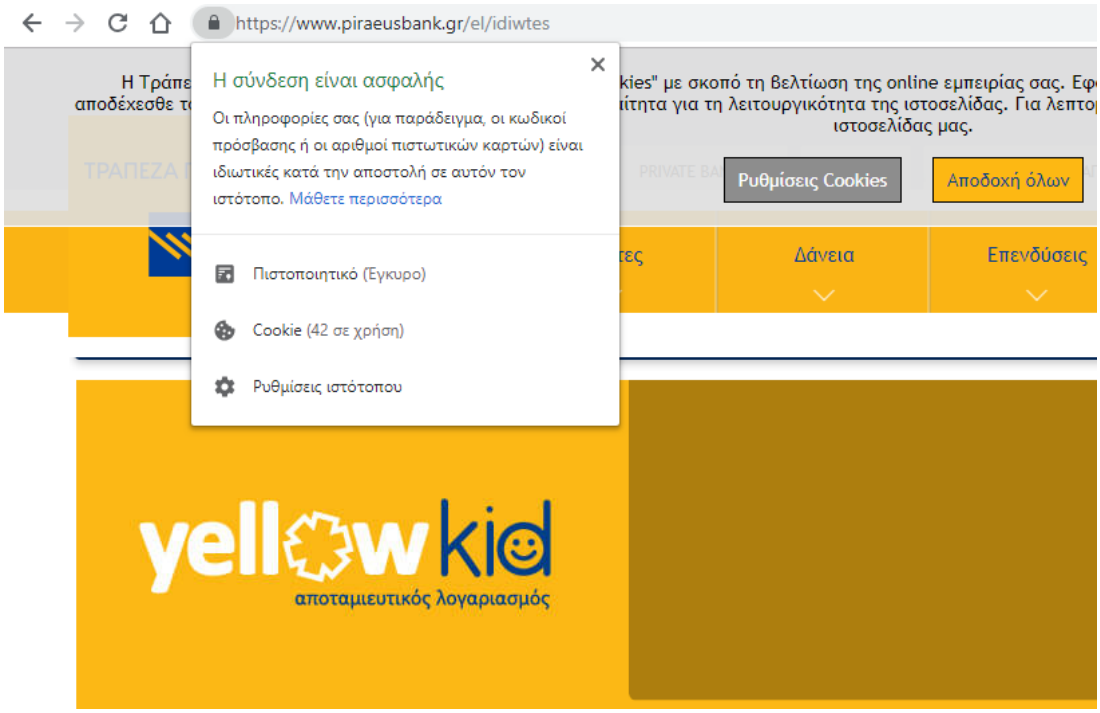
Εικόνα 10- Δομή ενός πιστοποιητικού X.509 v3

5.4. Τράπεζα Πειραιώς- πιστοποιητικό

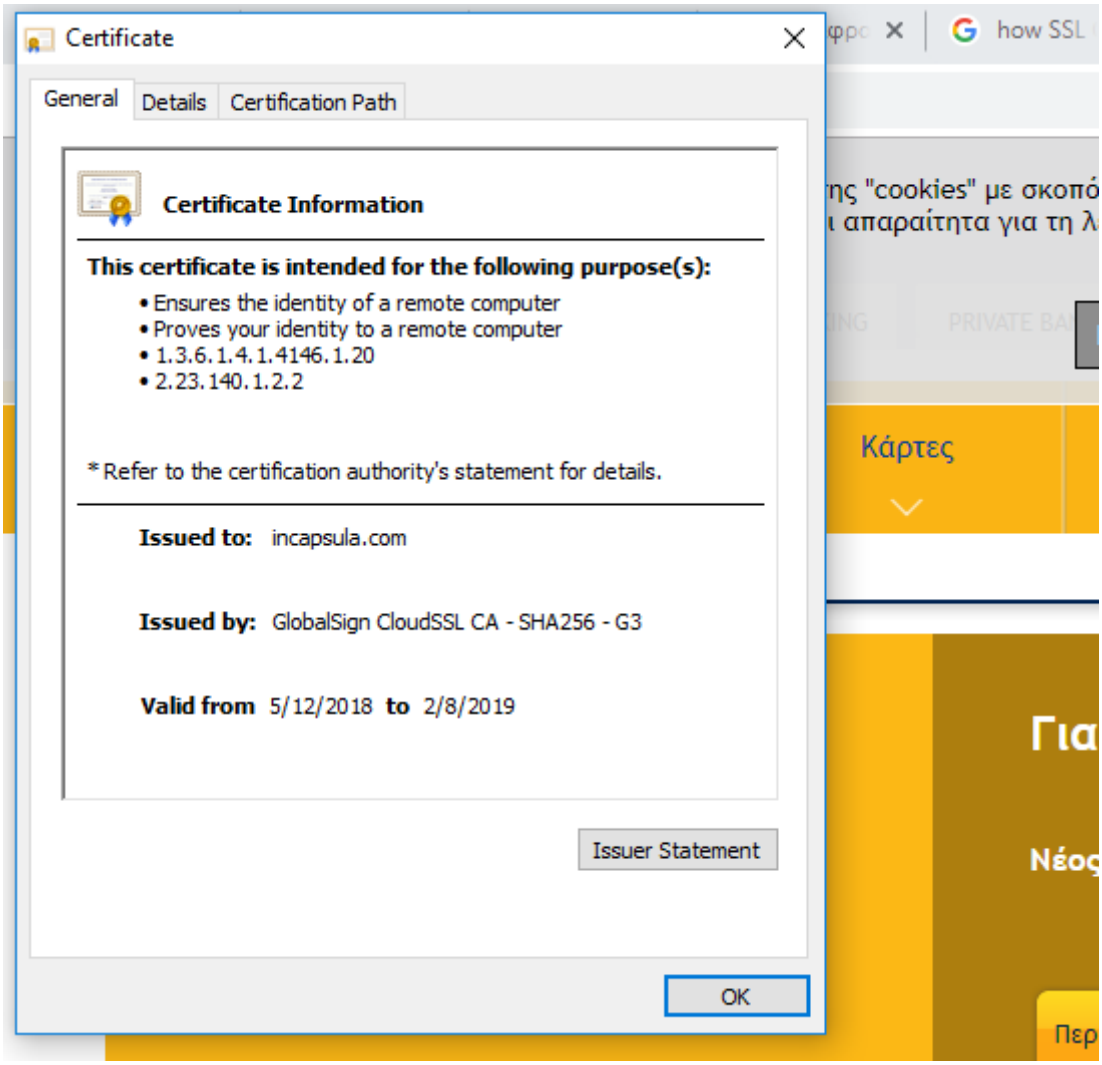
Ας ελέγξουμε ένα πραγματικό πιστοποιητικό, τα στοιχεία του και τις λεπτομέρειες έκδουσας αρχής του. Υπάρχουν εργαλεία προβολής πιστοποιητικών που διαβάζουν αυτές τις μορφές κωδικοποίησης και εμφανίζουν τα πιστοποιητικά.

Παράδειγμα πιστοποιητικού στο e-banking της τράπεζας Πειραιώς

Μετάβαση στη διεύθυνση https://www.piraeusbank.gr/ και στη συνέχεια κάνουμε κλικ στον σύνδεσμο προβολής πιστοποιητικού, όπως φαίνεται στην εικόνα.



Εικόνα 11- Προβολή πιστοποιητικού στην τράπεζα Πειραιώς

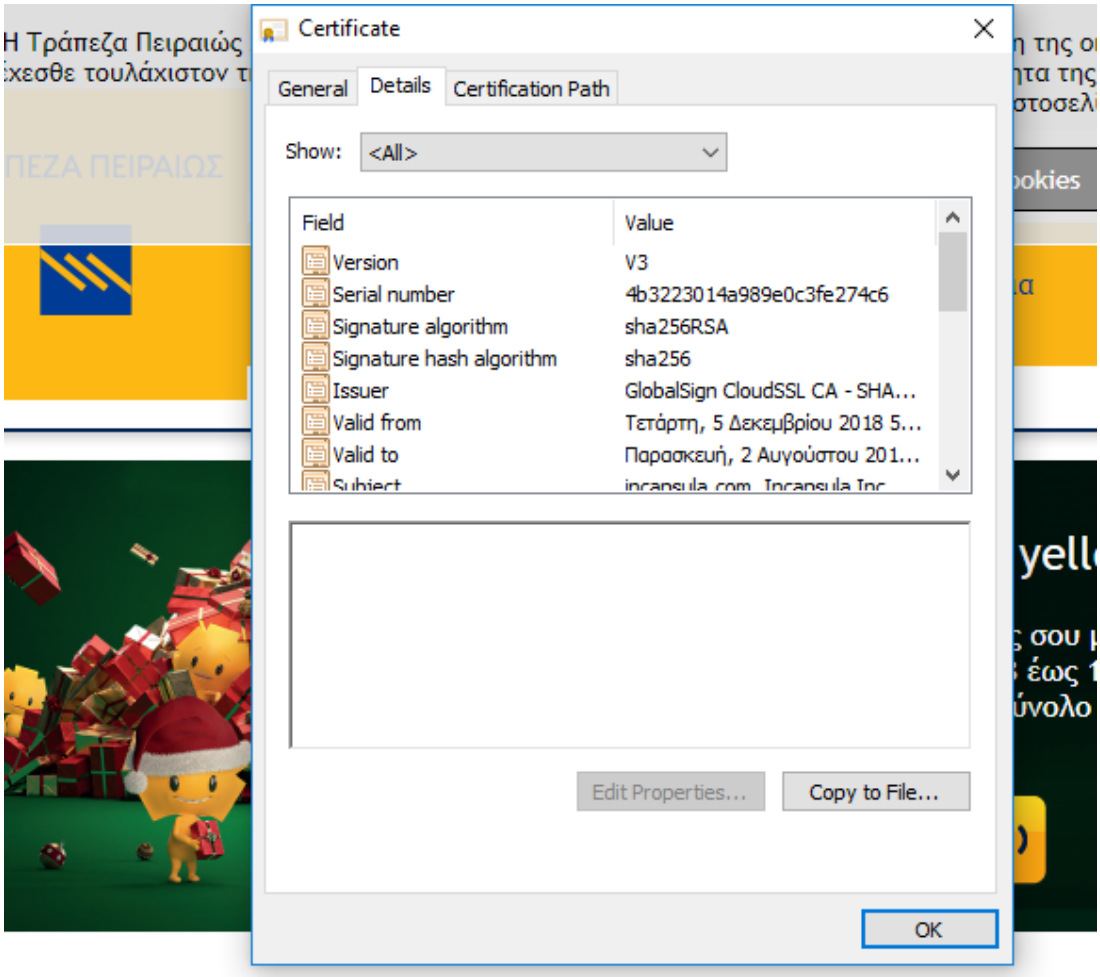


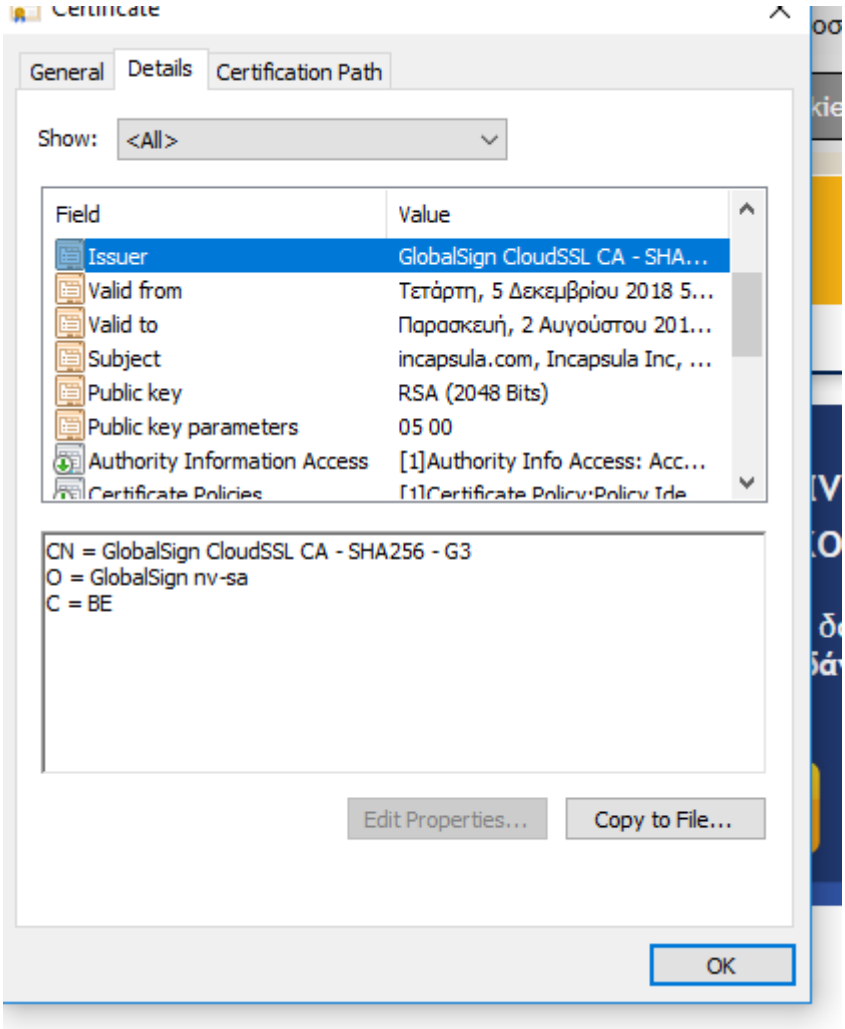
Εικόνα 12- Προβολή γενικών πληροφοριών του πιστοποιητικού

Μόλις κάνουμε κλικ στη σύνδεση πιστοποιητικού προβολής, θα ανοίξει το εργαλείο προβολής πιστοποιητικών των Windows και θα εμφανιστεί το πιστοποιητικό που ανήκει στην τράπεζα Πειραιώς. Αυτό το πιστοποιητικό, όπως μπορούμε να δούμε στην εικόνα στο πεδίο "Εκδοση", εκδίδεται από την GlobalSign .

Στη συνέχεια, επιλέγοντας από την καρτέλα «Λεπτομέρειες» (Details) το πρόγραμμα προβολής πιστοποιητικών εμφανίζει επίσης τις λεπτομέρειες ενός πιστοποιητικού. Υπάρχουν πολλά πεδία και το αναπτυσσόμενο μενού "Εμφάνιση" τα φιλτράρει για καλύτερη προβολή. Η εικόνα εμφανίζει μερικά από τα βασικά πεδία που

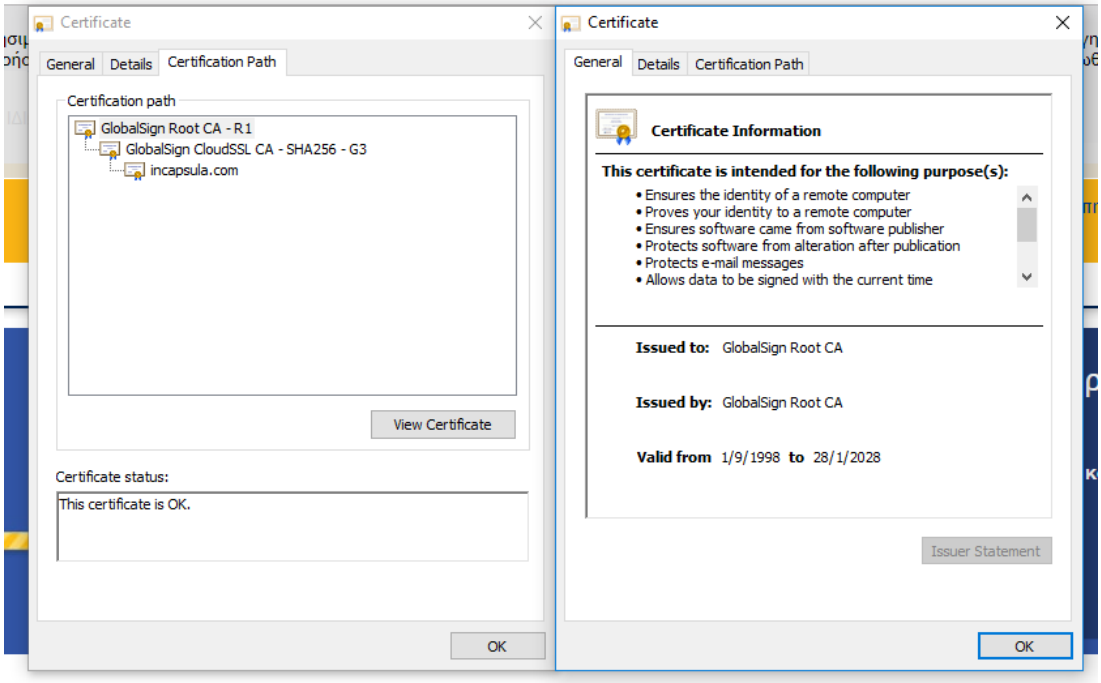
ονομάζονται πεδία έκδοσης 1. Εδώ στα αριστερά βλέπετε το θέμα, το SBI, και τη λεπτομέρεια του Distinguished Name (DN). Στη δεξιά πλευρά του εκδότη.





Εικόνα 13- Λεπτομέρειες πιστοποιητικού της Τράπεζας

Κάντε κλικ στην καρτέλα "CertificationPath " για να δούμε την διαδρομή των πιστοποιητικών και πατώντας στο κουμπί "Προβολή πιστοποιητικού" όπως φαίνεται παρακάτω φαίνεται ότι δείχνει επίσης ότι το Globalsign είναι μια CA δύο επιπέδων, όπου η VeriSign είναι η Root και η "Επέκταση επικύρωσης GlobalSign CLoudSSlCA" είναι μια εκδοτική ΑΠ.



Εικόνα 14- Προβολή επιπέδων (διαδρομής) πιστοποιητικού

5.5. Διαδικασία επικύρωσης πιστοποιητικού

Πριν αποδεχτούν τα πιστοποιητικά, οι φυλλομετρητές / εφαρμογές πραγματοποιούν έλεγχο επαλήθευσης για να βεβαιωθούν ότι τα πιστοποιητικά είναι έγκυρα και ότι διαθέτουν έγκυρη διαδρομή πιστοποίησης. Η κατάσταση ενός πιστοποιητικού δημόσιου κλειδιού καθορίζεται μέσω τριών διακριτών, αλλά αλληλένδετων διαδικασιών. Αλλά αυτό μπορεί να διαφέρει ελαφρώς με βάση τις υλοποιήσεις.

Ανακάλυψη πιστοποιητικού ή οικοδόμηση αλυσίδας

Η διαδικασία δημιουργίας αλυσίδας θα επικυρώσει τη διαδρομή πιστοποίησης, ελέγχοντας κάθε πιστοποιητικό στη διαδρομή πιστοποίησης από το πιστοποιητικό τερματισμού στο πιστοποιητικό της αρχικής πιστοποίησης. Τα πιστοποιητικά ανακτώνται από το κατάστημα των ενδιάμεσων αρχών πιστοποίησης, από το κατάστημα αρχών αξιόπιστων αρχών πιστοποίησης ή από μια διεύθυνση URL που καθορίζεται στο χαρακτηριστικό AIA του πιστοποιητικού. Αν διαπιστώσει κάποιο πρόβλημα με ένα από τα πιστοποιητικά στη διαδρομή ή εάν δεν μπορεί να βρει ένα πιστοποιητικό, η διαδρομή πιστοποίησης απορρίπτεται ως μη πιστοποιημένη διαδρομή πιστοποίησης.

Για να βελτιώσουν τις επιδόσεις, τα προγράμματα περιήγησης / λειτουργικά συστήματα ενδέχεται να αποθηκεύουν δευτερεύοντα πιστοποιητικά ΑΠ στο κατάστημα των ενδιάμεσων αρχών πιστοποίησης, έτσι ώστε τα μελλοντικά αιτήματα για το πιστοποιητικό να μπορούν να ικανοποιηθούν από το κατάστημα αντί να έχουν πρόσβαση στο πιστοποιητικό μέσω μιας διεύθυνσης URL.

Αποθήκευση πιστοποιητικού

Ένα κατάστημα πιστοποιητικών θα περιέχει συχνά πολλά πιστοποιητικά, ενδεχομένως εκδοθέντα από διάφορες ΑΠ. Στα συστήματα των Windows υπάρχουν ξεχωριστά καταστήματα που είναι γνωστά ως το κατάστημα μηχανών που χρησιμοποιείται από τον υπολογιστή και το κατάστημα χρηστών ή το κατάστημά μου χρησιμοποιείται από τον χρήστη που είναι συνδεδεμένος αυτήν τη στιγμή.

Στην Java, τα πιστοποιητικά περιβάλλοντος αποθηκεύονται σε αρχεία JKS και υποδεικνύονται από Ιδιότητες συστήματος

-Djavax.net.ssl.keyStore = $ {somepath} /keystore.jks -Djavax.net.ssl.trustStore = $ {somepath} /cacerts.jks -Djavax.net.ssl.keyStorePassword = κλειδί-κατάστημα-κλειδί

Σκοπός

Ο αλυσιδωτός κινητήρας πιστοποιητικών κατασκευάζει όλες τις πιθανές αλυσίδες πιστοποιητικών.

Το όλο γράφημα των αλυσίδων πιστοποιητικών κατασκευάζεται και στη συνέχεια παραγγέλλεται από την "ποιότητα" της αλυσίδας. Η αλυσίδα καλύτερης ποιότητας για ένα δεδομένο πιστοποιητικό τέλους επιστρέφεται στην εφαρμογή κλήσης ως προεπιλεγμένη αλυσίδα.

Κάθε αλυσίδα κατασκευάζεται χρησιμοποιώντας έναν συνδυασμό των πιστοποιητικών που υπάρχουν στα καταστήματα πιστοποιητικών και των πιστοποιητικών που είναι διαθέσιμα από τις δημοσιευμένες τοποθεσίες URL. Κάθε πιστοποιητικό στην αλυσίδα έχει εκχωρηθεί ένας κωδικός κατάστασης. Ο κωδικός κατάστασης δηλώνει εάν το συγκεκριμένο πιστοποιητικό είναι:

Υπογραφή έγκυρη

Θα πρέπει να γίνει έλεγχος αν είναι έγκυρη η υπογραφή, την ημερομηνία και ώρα έναρξης και λήξης της υπογραφής και του πιστοποιητικού, αν έχουν ρυθμιστεί σωστά, η ημερομηνία έναρξης η ακόμα ή έχει λήξει το πιστοποιητικό, ή αν έχει ανακληθεί το πιστοποιητικό.

Κάθε κωδικός κατάστασης έχει προτεραιότητα σε αυτόν. Για παράδειγμα, ένα πιστοποιητικό που έχει λήξει έχει υψηλότερη προτεραιότητα από ένα πιστοποιητικό που έχει ανακληθεί. Αυτό οφείλεται στο γεγονός ότι ένα πιστοποιητικό που έχει λήξει δεν πρέπει να ελέγχεται για την κατάσταση ανάκλησης.

Εάν οι κωδικοί κατάστασης έχουν εκχωρηθεί στα πιστοποιητικά μιας αλυσίδας πιστοποιητικών, ο κώδικας κατάστασης με το υψηλότερο προτέρημα εφαρμόζεται στην αλυσίδα πιστοποιητικών και μεταδίδεται στην κατάσταση της αλυσίδας πιστοποιητικών.

Επικύρωση διαδρομής

Για κάθε πιστοποιητικό στην αλυσίδα, ο αλυσιδωτός κινητήρας πιστοποιητικού πρέπει να επιλέξει πιστοποιητικό της ΑΠ έκδοσης. Αυτή η διαδικασία, γνωστή ως

επικύρωση διαδρομής, επαναλαμβάνεται μέχρις ότου επιτευχθεί πιστοποιητικό που έχει υπογράψει αυτόματα (συνήθως αυτό είναι ένα πιστοποιητικό ριζικής CA).

Υπάρχουν διάφορες διαδικασίες που μπορούν να χρησιμοποιηθούν για την επιλογή του πιστοποιητικού για μια CA που εκδίδει. Η πραγματική διαδικασία που χρησιμοποιείται βασίζεται στο εάν το πιστοποιητικό που βρίσκεται υπό διερεύνηση έχει οριστεί για την επέκταση του αναγνωριστικού κλειδιού Authority (AKI). Η επιθεώρηση της επέκτασης του AKI θα οδηγήσει σε μία από τις τρεις διαδικασίες αντιστοίχισης που εφαρμόζονται:

Ακριβής αντιστοίχιση

Εάν η επέκταση AKI περιέχει το όνομα χρήστη του εκδότη και τον σειριακό αριθμό του εκδότη, επιλέγονται μόνο τα πιστοποιητικά που αντιστοιχούν στο όνομα χρήστη και τον σειριακό αριθμό κατά τη διαδικασία δημιουργίας αλυσίδας. Ως περαιτέρω δοκιμή, το όνομα του εκδότη στο εκδοθέν πιστοποιητικό πρέπει να ταιριάζει με το όνομα του θέματος στο πιστοποιητικό του εκδότη.

Αντιστοίχιση κλειδιού

Εάν η επέκταση AKI περιέχει μόνο πληροφορίες δημόσιου κλειδιού, επιλέγονται ως έγκυροι εκδότες μόνο τα πιστοποιητικά που περιέχουν το δηλωμένο δημόσιο κλειδί στην επέκταση κλειδιού SubjectKey (SKI).

Όνομα αντιστοιχία.

Εάν δεν υπάρχει καμία πληροφορία στο AKI ή εάν το AKI δεν υπάρχει στο πιστοποιητικό, το πιστοποιητικό θα επισημαίνεται ως "αντιστοιχία ονόματος". Στην αντιστοίχιση ονόματος, το όνομα του αντικειμένου ενός πιστοποιητικού πρέπει να ταιριάζει με το όνομα του εκδότη στο τρέχον πιστοποιητικό στο προκειμένου να επιλεγεί το πιστοποιητικό ως έγκυρος εκδότης. Επειδή τα δεδομένα αποθηκεύονται σε δυαδική μορφή, η διαδικασία αντιστοίχισης ονομάτων χαρακτηρίζεται από πεζά γράμματα. Σε όλες τις περιπτώσεις, ακόμα και αν δεν υπάρχει πιστοποιητικό αντιστοίχισης στο

κατάστημα, το τρέχον πιστοποιητικό θα εξακολουθεί να χαρακτηρίζεται ως "ακριβής αντιστοίχιση", "αντιστοιχία κλειδιού" ή "αντιστοίχιση ονόματος", επειδή περιγράφεται η δοκιμασμένη αντιστοίχιση

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η παρούσα εργασία μελέτησε τις ηλεκτρονικές πληρωμές στο ηλεκτρονικό εμπόριο, πρωτόκολλα που χρησιμοποιούνται καθώς και τον τρόπο λειτουργίας αυτών. Σήμερα είναι η εποχή της τεχνολογίας των πληροφοριών. Το ηλεκτρονικό εμπόριο είναι το σημαντικό επίτευγμα αυτής της εποχής. Στο ηλεκτρονικό εμπόριο, η συναλλαγή πραγματοποιείται μέσω του δικτύου.

Το διαδίκτυο στις μέρες μας παίζει κυρίαρχο ρολό στην καθημερινότητα των ανθρώπων. Παράλληλα με την ανάπτυξη του διαδικτύου υπάρχει ανάπτυξη και στο ηλεκτρονικό εμπόριο. Τα οφέλη του ηλεκτρονικού εμπορίου είναι πολλά και για τους πελάτες αλλά και για την ηλεκτρονική εταιρεία. Συγκεκριμένα για τους αγοραστές πλεονέκτημα είναι η παγκόσμια αγορά που προσφέρει το ηλεκτρονικό εμπόριο, οι χαμηλότερες τιμές, η εξοικονόμηση χρόνου κ.α. Για την εταιρεία από την άλλη τα πλεονεκτήματα πηγάζουν στην εξοικονόμηση χρημάτων αλλά και στην εύκολη συλλογή χαρακτηριστικών των πελατών της. Φυσικά, υπάρχουν και μειονεκτήματα στο ηλεκτρονικό εμπόριο. Η ασφάλεια είναι αυτό που απασχολεί τους περισσότερους, ενώ για τους ιδιοκτήτες εταιρειών σημαντικό πρόβλημα προκαλούν οι ιοί και τα προγράμματα που μπαίνουν στα συστήματα των εταιρειών. Επίσης οι hackers αποτελούν κίνδυνο για τις ηλεκτρονικές εταιρείες. Ο τρόπος πληρωμής των ηλεκτρονικών αγορών απασχολεί ιδιαίτερα τους αγοραστές γιατί υπάρχουν πολλοί τρόποι πληρωμής πλέον (αντικαταβολή, ηλεκτρονικές επιταγές, πιστωτική κάρτα κ.α.) Η ανάπτυξη του

ηλεκτρονικού εμπορίου αλλά και η ανάπτυξη του διαδικτύου γενικότερα έκανε τους ιδιοκτήτες εταιρειών (όχι μονό ηλεκτρονικών εταιρειών) να ασχοληθούν με την ηλεκτρονική διαφήμιση.

Κατά τη διάρκεια διαφόρων φάσεων μιας ηλεκτρονικής συναλλαγής, οι πληροφορίες όπως οι προδιαγραφές του προϊόντος, τα στοιχεία της παραγγελίας, η πληρωμή και οι πληροφορίες παράδοσης μεταφέρονται μέσω του Διαδικτύου. Οι πληροφορίες συναλλαγών που μεταδίδονται μέσω του δημόσιου διαδικτύου μπορούν να αξιοποιηθούν, να παραληφθούν, να εκτραπούν, να τροποποιηθούν και να κατασκευαστούν από εισβολέα που προσπαθεί να κερδίσει κάποιο όφελος ή να προκαλέσει ζημιές σε ανταγωνιστικές επιχειρήσεις.

Η ασφάλεια ηλεκτρονικού εμπορίου είναι το σημαντικό ζήτημα που διατηρεί πολλές οργανώσεις εμπορίου φοβούνται να χρησιμοποιούν το Διαδίκτυο για την επιχείρησή τους. Τα Secured Socket Layer (SSL) και οι Secured Electronic Transactions (SET) είναι τα σημαντικότερα δημοφιλή πρωτόκολλα ασφάλειας ηλεκτρονικού εμπορίου. Κάθε μία από αυτές έχει τον τομέα της χρήσης, τα προϊόντα της, τη στρατηγική της και τη δική της διαδικασία κρυπτογράφησης. Η διεξαγωγή μελέτης σύγκρισης μεταξύ SSL και SET δεν είναι εύκολο πράγμα. Η χρήση του SSL ή του SET εξαρτάται από την εκτίμηση του χρήστη.

Μια μελέτη σύγκρισης παρουσιάζει το ζήτημα του σχεδιασμού του καθενός, τον τρόπο εξασφάλισης του ηλεκτρονικού εμπορίου, την εξακρίβωση της ταυτότητας των μερών, τη χρήση ανταλλαγής κλειδιών και τις μεθοδολογίες κρυπτογράφησης. Παρόλο που εξακολουθούν να υπάρχουν πολλές προσπάθειες που εστιάζονται στην ασφάλεια του ηλεκτρονικού εμπορίου, δεν είναι εύκολη η χρήση του Διαδικτύου για την ανταλλαγή κρίσιμων δεδομένων, όπως είναι ο αριθμός πιστωτικής κάρτας, οι κωδικοί πρόσβασης ή οποιαδήποτε ευαίσθητη προσωπική πληροφορία.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΕΛΛΗΝΙΚΗ

Γεωργιάδης Χ.Κ. (2003), «Προβλήματα Ασφάλειας στο Ηλεκτρονικό Εμπόριο», (Διδακτικές Σημειώσεις), Παν. Θεσσαλίας

Δουκίδης, Ι.Γ., κ.ά. (1998), «Ηλεκτρονικό Εμπόριο», Εκδόσεις Νέων Τεχνολογιών, Αθήνα.

Δουκίδης Γ., Θεμιστοκλέους Μ., Δράκος Β., Παπαζαφειροπούλου Ν., (1998), «Ηλεκτρονικό Εμπόριο», Οικονομικό Πανεπιστήμιο, Εκδόσεις Νέων Τεχνολογιών, Αθήνα.

Πομπότσης Άνδρέας, Γ. Π. (2003). Ασφάλεια Δικτύων Υπολογιστών. Τζιόλας, Α

Πασχόπουλος , Α. & Σκαλτσάς , Π., 2001. Ηλεκτρονικό Εμπόριο, Ανάπτυξη & Εφαρμογή Επιχειρηματικής Στρατηγικής και Marketing στο διαδίκτυο. Β' Έκδοση. Αθήνα : Εκδόσεις Κλειδάριθμος

Σιώμκος Γ και Τσιάμης Ι(2004), Στρατηγικό ηλεκτρονικό μάρκετινγκ, Εκδόσεις Σταμούλης, Αθήνα

Καλλονιάτης, Χ. (2015, 6 6). Βασικά θέματα κρυπτογραφίας. Ανάκτηση από Τμήμα Πολιτισμικής Τεχνολογίας & Επικοινωνίας Πανεπιστημίου Αιγαίου: http://www.ct.aegean.gr/index.php

Χονδροκούκης Γ. (2005). Εισαγωγή στο ηλεκτρονικό εμπόριο. Πανεπιστήμιο Πειραιώς. Πειραιάς.

Δ.Μαρτάκος, Ν.Κυρλόγλου, Α.Μητράκας, Μ.Γιαννακάκη, Χ.Σιούλης,« Ηλεκτρονικές υπογραφές και ηλεκτρονικά πιστοποιητικά ταυτοποίησης», Ebusiness forum, ομάδα εργασίας Έ2', Μάρτιος 2004

Διδακτορική Διατριβή: "Θεωρία και εφαρμογές κρυπτογραφικών συστημάτων δημοσίου κλειδιού βασισμένων σε ελλειπτικές καμπύλες", Ελισάβετ Κωνσταντίνου, Ιούνιος 2005

Γ. Πάγκαλος & Ι. Μαυρίδης, «Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων», Εκδόσεις Ανικούλα Θεσσαλονίκη 2002

Πολλάλης Γ., Γιαννακόπουλος Δ., (2007) ΗΛΕΚΤΡΟΝΙΚΟ Επιχεφείν (Θεωρία & Μελέτες Περίπτωσης): Τεχνολογίες & Στρατηγικές Ψηφιακής Οικονομίας, Εκδόσεις Αθ. Σταμούλης, Αθήνα

Δουκίδης , Γ. & Φραιδάκη, Κ, 2010. Καταγραφή του Ηλεκτρονικού Εμπορίου Β-C στην Ελλάδα: Αντιλήψεις και συμπεριφορά των online καταναλωτών. Εργαστήριο :Ηλεκτρονικού Εμπορίου (ELTRUN).
Σαμαράς Γιάννης Β. (2002), «Ηλεκτρονικό Εμπόριο –Αρχές – Εξελίξεις – Στρατηγική Από τη Σκοπιά του Manager», Εκδόσεις Μ. Γκιούρδας, Αθήνα.
Κουργιαντάκης Μ. (2013). Οδηγός Ηλεκτρονικού Επιχεφείν. Επιμελητήριο Χανίων. Χανιά. www.chania-cci.gr/website/images/stories/.../E-business Guide 2013.pdf
Μάρκελλος, Κ. και Τσακαλίδης, Α. (2005) e-Επιχειρηματικότητα από την ιδέα στην υλοποίηση. Εκδόσεις Ελληνικά Γράμματα.
Παναγιώτης Ε. Νάστου, Παύλος Γ. Σπυράκης, Γιάννης Κ. Σταματίου (2003), Σύγχρονη Κρυπτογραφία, , Εκδόσεις Ελληνικά Γράμματα
Σελίμης, Γ. (2008). Σχεδιασμός κρυπτογραφικών Συστημάτων με υλικό ειδικού σκοπού. διδακτορική διατριβή 204.
Σερπάνος Δ, Τ. W. (2011). Architecture of Network Systems

Κουκουβίνος(2007), Κρυπτογραφία, Χ., Α. Παπαϊωάννου, Εκδόσεις ΕΜΠ, 2007

ΞΕΝΗ

Campbell MC and Goodstein RC (2001) The moderating effect of perceived risk on consumers' evaluations of product incongruity: preference for the norm. TheJournal of Consumer Research, 28(3): 439-449.

Chaffey , D. , 2007. E-business and E-commerce Management -Pearson Education .

Cho J (2004) Likelihood to abort an online transaction: influences from cognitive evaluations, attitudes, and behavioral variables. Information & Management, 41: 827-838.

Close A., Kukar-Kinney M., Benusa T. (2012): Towards a Theory of Consumer Electronic Shopping Cart Behavior: Motivations of E-Cart Use and Abandonment, Online Consumer Behavior: Theory and Research in Social Media, Advertising and e-tail, Routledge

Davis FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, September: 319-340.

De P, Hu Y and Rahman MS (2010) Technology usage and online sales: An empirical study. Management Science, 56(11): 1930-1945.

Dowling GR (1986) Perceived risk: the concept and its measurements. Psychology & Marketing, 3(3): 193-210.

Dowling GR and Staelin R (1994) A model of perceived risk and intended risk-handling activity. The Journal of Consumer Research, 21(1): 119-134.

Hofacker CF (2008) E-tail constraints and tradeoffs. Direct Marketing: An International Journal, 2(3): 129-143.

Kumar V, George M and Pancras J (2008) Cross-buying in retailing: drivers and consequences. Journal of Retailing, 84(1): 15-27.

Li H, Kuo C and Rusell MG (1999) The impact of perceived channel utilities, shopping orientations, and demographics on the consumer's online buying behavior. Journal of Computer-Mediated Communication, 5(2): 0.
doi:10.1111/j.1083-6101.1999.tb00336.x

Mukherjee A and Nath P (2007) Role of electronic trust in online retailing.European Journal of Marketing, 41(9/10): 1173-1202

Li S and Chatterjee P (2005) Shopping cart abandonment at retail websites – a multi-stage model on online shopping behavior. Paper session presented at the meeting of Marketing Science Conference.
Li H, Kuo C and Rusell MG (1999) The impact of perceived channel utilities, shopping orientations, and demographics on the consumer's online buying behavior. Journal of Computer-Mediated Communication, 5(2): 0. doi:10.1111/j.1083-6101.1999.tb00336.x

Liljander V, Polsa P and Van Riel A (2009) Modeling consumer responses to an apparel store brand: store image as a risk reducer. Journal of Retailing and Consumer Services, 16: 281-290.

Mitchell VW (2001) Re-conceptualizing consumer store image processing using perceived risk. Journal of Business Research, 54: 167-172.

Ouellet M (2010) Recovering lost sales through an automated shopping cart abandonment strategy. Retrieved from listrak website:
http://www.listrak.com/Solutions/Reasons-for-Cart-Abandonment.aspx.

Turban , F. &King , D. &Lee , J. &Viehland , D. , επιμέλεια μετάφρασης Σαμαράς, Γ. , 2006 .Ηλεκτρονικό Εμπόριο: Αρχές –Εξελίξεις – Στρατηγική από την σκοπιά του Manager. Β' Έκδοση. Αθήνα :Εκδόσεις Γκιούρδας.

Tong X (2010) A cross-national investigation of an extended technology acceptance model in the online shopping context. International Journal of Retail & Distribution Management, 38(10): 742-759.

Wood SL (2001) Remote purchase environments: the influence of return policy leniency on two-stage decision processes. Journal of Marketing Research, 38: 157-169.

Shulman JD, Coughlan AT and Savaskan RC (2011) Managing consumer returns in a competitive environment. Management Science, 57(2): 347-362.

Stone RN and Gronhaug K (1993) Perceived risk: further considerations for the marketing discipline. European Journal of Marketing, 27(3): 39-50.

Sweeney JC, Soutar GN and Johnson LW (1999) The role of perceived risk in the quality-value relationship: a study in a retail environment. Journal of Retailing, 75(1): 77-105

Laura S. Egeln, Julie A. Joseph(2012), Shopping Cart Abandonment in Online Shopping, Atlantic Marketing Journal, Volume 1, Issue 1 Inaugural Issue: Winter 2012

Cho, C. H., Kang, J., & Cheon, H. J. (2006). Online shopping hesitation. CyberPsychology & Behavior, 9(3), 261–274.

Close, A. G., & Kukar-Kinney, M. (2010). Beyond buying: Motivations behind consumers' online shopping cart use. Journal of Business Research, 63(9–10), 986–992

Egeln, L. S., & Joseph, J. A. (2012). Shopping cart abandonment in online shopping. Atlantic Marketing Journal, 1(1), 1–14

Holzwarth, M., Janiszewski, C., & Neumann, M. M. (2006). The influence of avatars on online consumer shopping behavior. Journal of Marketing, 70(4), 19–36

Kim, M., & Lennon, S. J. (2011). Consumer response to online apparel stockouts. Psychology and Marketing, 28(2), 115–144.

Kukar-Kinney, M., & Close, A. G. (2010). The determinants of consumers' online shopping cart abandonment. Journal of the Academy of Marketing Science, 38(2), 240–250

Kibo. (2016). eCommerce Performance Index Vol 31. Retrieved October 31, 2016, from http://www.marketlive.com/in-the-news/press/performance-index-v31.html

Loftus, P. (2001, April 23)). E-commerce (a special report): A buyer's market — Pay for performance; technology allows advertisers to know what an ad is worth — To the dismay of some websites. Wall Street Journal, R16

Rajamma, R. K., Paswan, A. K., & Hossain, M. M. (2009). Why do shoppers abandon shopping cart ; Perceived waiting time, risk, and transaction inconvenience. Journal of Product & Brand Management, 18(3), 188–197

Wu, J.-H., & Hisa, T.-L. (2004). Analysis of e-commerce innovation and impact: A hypercube model. Electronic Commerce Research and Applications, 3(4), 389–404

Kumar, H. (2016). Mobile commerce trends to buy into. Marketing Insights, 28(1), 20–21.

Lee, A. Y., & Aaker, J. L. (2004). Bringing the frame into focus: The influence of regulatory fit on processing fluency and persuasion. Journal of Personality and Social Psychology, 86(2), 205–218.

Silverstein, M., Stanger, P., & Abdelmessih, N. (2001). The next chapter in business-toconsumer e-commerce. Boston, MA: The Boston Consulting Group

Schlosser, A. E., Barnett, T., & Lloyd, S. M. (2006). Converting web site visitors into buyers: How web site investment increases consumer trusting beliefs and online purchase intentions. Journal of Marketing, 70(2), 133–148.

Shobeiri, S., Mazaheri, E., & Laroche, M. (2015). Shopping online for goods vs. services: Where do experiential features help more ; International Journal of Consumer Studies, 39(2), 172–179

Shankar, V., Venkatesh, A., Hofacker, C., & Naik, P. (2010). Mobile marketing in the retailing environment: Current insights and future research avenues. Journal of Interactive Marketing, 24(2), 111–120.

Spacey, J. 2016. Design: Usability vs Functionality, 04.05.2016, http://simplicable.com/new/usability-vs-functionality, 23.11.2016.

Usability Government. Information Architecture basics. https://www.usability.gov/what-and-why/information-architecture.html, 17.06.2016

Moreno, H. 2014. The Gap between UI and UX Design – Know the Difference. 24.04.2014.http://snip.ly/mjj7s#http://www.onextrapixel.com/2014/04/24/the-gap-between-ui-and-ux-design-know-the-difference

Kirakowski, J., McNamara, N. 2006. Functionality, usability, and user experience: Three areas of concern 11.11.06

Chen, E. 2015. What is UX design ; Center for Mit entrepreneurship 28.10.2015 https://miteship.zendesk.com/hc/en-us/articles/206438833-What-is-UX-Design-,

Chandra Shekhar Aryal (2014), Design Principles for Responsive Web, Bachelor's Thesis, Helsinki Metropolia University of Applied Sciences Bachelor of Engineering Information Technology

Swant, M. (2016). Why people choose to shop or not to shop on their phones. Retrieved October 31, 2016, from http://www.adweek.com/news/technology/heres-why-people-choose-shopor-not-shop-their-phones-169419

https://blog.paymill.com/en/checkout-conversion-rate/

Fogg BJ, Marshall J., Laraki O., Osipovich A., Varma C., Fang N., Paul J., Rangnekar A., Shon J., Swani P., Treinen M., (2001), "What Makes Web Sites Credible ; A Report on a Large Quantitative Study", Persuasive Technology Lab Stanford University, 61-63.

Schimmel K & Nicholls J., (2002), "E-Commerce Consumer Perceptions Regarding Online shopping", Journal of Internet Commerce Shopping, Journal of Internet Commerce 1.4 (2002): 23-36.

Schonberg E., Cofino T., Hoch R., Podlaseck M., Spraragen S. L.,(2000) "Measuring Success", Comm. ACM 43(8) 53-57

Fogg BJ, Marshall J., Laraki O., Osipovich A., Varma C., Fang N., Paul J., Rangnekar A., Shon J., Swani P., Treinen M., (2001), “What Makes Web Sites Credible ; A Report on a Large Quantitative Study”, Persuasive Technology Lab Stanford University, 61-63.

Gupta M., Li R., Yin Z., Han J., (2011) “An Overview of Social Tagging and Applications”, Social Network Data Analytics, C.C. Aggarwal, Springer. p. 447-497 Guy M. & Tonkin E., (2006), “Folksonomies: Tidying up Tags” D-Lib Magazine, 12(Number 1): p. 1-15.

Natter M., Mild A., Wagner U., Taudes A., (2008), “Planning New Tariffs at tele.ring: The Application and Impact of an Integrated Segmentation, Targeting, and Positioning Tool, Marketing Science Vol 24, No 4, pp.600-609.

Palmier J., (2002), “Web site usability, design and performance metrics”, Inform. Systems Res. 13(2) 151-167.

Peterson R., Balasubramanian S., Bronnenberg B., (1997), “Exploring the implications of the internet for consumers Marketing”, Journal of the Academy of Marketing Science p. 329-346.

Phat Tri Huynh (2012), “Effects of Web 2.0 Experience on Consumers’ Online Purchase Intention: The Social Networking and Interaction Orientation Factors”, AUT Business School