



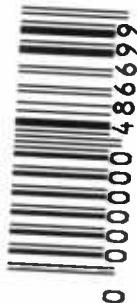
ΑΘΗΝΑΙ
ΒΙΒΛΙΟΘΗΚΗ
στα. 72688
ΑΡ. 00588
ΤΑΞ. Ανδ

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc) στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΚΑΤΑΛΟΓΟΣ



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Ασφάλεια σε υπηρεσίες διαδικτύου βασισμένες σε XML»

Ανδρικόπουλος Παναγιώτης

M3010011

ΑΘΗΝΑ, ΔΕΚΕΜΒΡΙΟΣ 2002



ΟΙΚΟΝΟΜΙΚΟ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΑΘΗΝΩΝ
ΒΙΒΛΙΟΘΗΚΗ
εισ. Ν2688
Αρ. 1558
ταξ. ΗΛΙΑ

**ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ (MSc)
στα ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Ασφάλεια σε υπηρεσίες διαδικτύου βασισμένες σε XML»

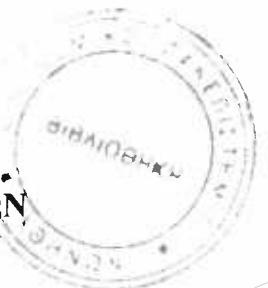
Ανδρικόπουλος Παναγιώτης

M3010011

**Επιβλέπων Καθηγητής: Επικ. Καθ. Δ. Γκρίτζαλης
Εξωτερικός Κριτής: Καθ. Ε. Κιουντούζης**

**ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ**

ΑΘΗΝΑ, ΔΕΚΕΜΒΡΙΟΣ 2002



Ευχαριστίες

Η παρούσα μεταπτυχιακή διατριβή εκπονήθηκε στο Τμήμα Πληροφορικής του Οικονομικού Πανεπιστημίου, στο πλαίσιο του Μεταπτυχιακού Προγράμματος ειδίκευσης στα Πληροφοριακά Συστήματα. Στην προσπάθεια αυτή συνέβαλαν, με διαφορετικό τρόπο ο καθένας, ορισμένοι άνθρωποι τους οποίους θα ήθελα να ευχαριστήσω.

Πρώτα απ' όλα θα ήθελα να ευχαριστήσω τον καθηγητή μου κ. Δημήτρη Γκρίζαλη για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου τη συγκεκριμένη εργασία και για τις πολύτιμες συμβουλές του. Η διδασκαλία του αποτέλεσε το κίνητρο για να ασχοληθώ με τη συγκεκριμένη επιστημονική περιοχή, καθώς και τη βάση για να αντιμετωπίσω τα προβλήματα που προέκυψαν κατά τη διάρκεια της έρευνας.

Ευχαριστώ, επίσης, τον Καθηγητή κ. Ευάγγελο Κιουντούζη για τις πολύτιμες και ουσιώδεις παρατηρήσεις του, που βασικός σκοπός τους ήταν να με βοηθήσουν να αποτυπώσω τον τρόπο σκέψης μου, ώστε να αναδειχθεί πολύ περισσότερο αυτή η προσπάθεια. Θέλω να πιστεύω πως κάτι τέτοιο σε ένα μεγάλο ποσοστό το πέτυχα, και φυσικά το οφείλω σε αυτόν.

Επίσης, θα ήθελα να ευχαριστήσω το Λέκτορα του Πανεπιστημίου Αιγαίου κ. Σπύρο Κοκολάκη, για τη μεγάλη βοήθεια που μου παρείχε καθ' όλη τη διάρκεια της παρούσας εργασίας και για το χρόνο που μου διέθεσε. Τον ευχαριστώ για τις συμβουλές που μου παρείχε σε συγκεκριμένα ζητήματα της εργασίας, αλλά πολύ περισσότερο για τις γενικές συμβουλές του που αφορούσαν στη μέθοδο έρευνας.

Τέλος, αφιερώνω την προσπάθεια αυτή στην οικογένεια μου, η οποία με στήριξε και συνεχίζει να με στηρίζει, δημιουργώντας τις κατάλληλες συνθήκες που μου επιτρέπουν να επιτυγχάνω τους στόχους που θέτω, μικρούς και μεγάλους.



ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ	7
EXECUTIVE SUMMARY	12
 ΚΕΦΑΛΑΙΟ 1 ^ο : ΕΙΣΑΓΩΓΗ.....	16
1.1. Πρόλογος.....	16
1.2. Σκοπός της παρούσας εργασίας	17
1.3. Κίνητρα για την πραγματοποίηση της παρούσας εργασίας.....	17
1.4. Ανάγκη για την πραγματοποίηση της παρούσας εργασίας.....	18
1.5. Προσδιορισμός του ερευνητικού προβλήματος.....	19
1.6. Αντικείμενο και στόχοι της παρούσας εργασίας.....	19
1.6.1. Ζητήματα στα οποία επικεντρώνεται η εργασία	19
1.6.2. Στόχοι της παρούσας εργασίας	20
1.7. Δομή της εργασίας	21
1.8. Συμβολή της εργασίας.....	23
1.9. Ορισμοί θεμελιωδών εννοιών	24
1.10. Οντολογικές και Επιστημολογικές Παραδοχές.....	25
1.10.1. Επιστημολογία και οντολογία της παρούσας εργασίας	26
1.11. Μέθοδος έρευνας	27
 ΚΕΦΑΛΑΙΟ 2 ^ο : ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ.....	29
2.1. Εισαγωγή.....	29
2.2. Τι είναι οι Υπηρεσίες Διαδικτύου	29
2.3. Πώς γεννήθηκε η ανάγκη για ανάπτυξη των Υπηρεσιών Διαδικτύου.....	31
2.4. Ποια είναι τα κίνητρα για την ανάπτυξη Υπηρεσιών Διαδικτύου	32
2.5. Περιγραφή του μοντέλου των Υπηρεσιών Διαδικτύου.	34
2.5.1. Αρχιτεκτονική του μοντέλου.	34
2.5.2. Περιγραφή των οντοτήτων του μοντέλου.....	35
2.5.3. Περιγραφή των διαδικασιών του μοντέλου.	35
2.5.4. Περιγραφή των στοιχείων που συνθέτουν μια Υπηρεσία Διαδικτύου.....	36
2.5.5. Κύκλος ζωής του μοντέλου ανάπτυξης Υπηρεσιών Διαδικτύου.	37
2.6. Πεδίο εφαρμογής του μοντέλου Υπηρεσιών Διαδικτύου.	38
2.6.1. Σε ποιες περιπτώσεις είναι χρήσιμες οι Υπηρεσίες Διαδικτύου.	38
2.6.2. Σε ποιες περιπτώσεις είναι ασύμφορη η χρησιμοποίηση Υπηρεσιών Διαδικτύου.	39
2.7. Το παρόν και το μέλλον των Υπηρεσιών Διαδικτύου.	40
2.8. Συμπέρασμα και ζητήματα προς διερεύνηση.....	42
 ΚΕΦΑΛΑΙΟ 3 ^ο : ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ XML.....	44
3.1. Εισαγωγή.....	44
3.2. Τι είναι η XML.....	44
3.3. Πλεονεκτήματα της XML στη διαχείριση της πληροφορίας.....	46
3.4. Ενοποίηση εφαρμογών στο Διαδίκτυο.....	46
3.5. Ο ρόλος της XML στην ανάπτυξη Υπηρεσιών Διαδικτύου.....	47
3.6. Υπηρεσίες Διαδικτύου βασισμένες στην XML	49
3.6.1. Τεχνολογίες που συμπληρώνουν την XML	49

3.6.2. Η Αρχιτεκτονική των υπηρεσιών.....	50
3.6.3. Η Στοίβα των υπηρεσιών.	51
3.6.4. Περιγραφή των τεχνολογιών.....	53
3.6.4.1. Simple Object Access Protocol (SOAP).	53
3.6.4.2. Web Services Description Language (WSDL).	56
3.6.4.3. Universal Description, Discovery, and Integration (UDDI).	58
3.6.5. Διαδικασίες του μοντέλου των υπηρεσιών.	60
3.6.5.1. Δημοσίευση Υπηρεσιών.....	61
3.6.5.2. Ανακάλυψη Υπηρεσιών.	62
3.6.5.3. Δέσμευση Υπηρεσιών.	64
3.7. Συμπέρασμα.	65
ΚΕΦΑΛΑΙΟ 4^ο : ΑΝΑΠΤΥΞΗ ΥΠΗΡΕΣΙΩΝ ΔΙΑΔΙΚΤΥΟΥ ΒΑΣΙΣΜΕΝΩΝ ΣΕ XML ..	66
4.1. Εισαγωγή.....	66
4.2. Μοντέλα ανάπτυξης Υπηρεσιών Διαδικτύου.	66
4.3. Η αρχιτεκτονική των μοντέλων ανάπτυξης .NET και J2EE.	68
4.4. Λεπτομερής Περιγραφή του .NET.	69
4.4.1. .NET Framework.....	70
4.4.2. Microsoft Visual Studio .NET.	72
4.4.3. .NET Enterprise Servers.....	72
4.4.4. .NET Passport.....	73
4.4.5. Αρχιτεκτονική .NET υπηρεσίας διαδικτύου.	74
4.5. Λεπτομερής Περιγραφή του J2EE.	75
4.5.1. Enterprise Java Beans.....	76
4.5.2. Java Servlets.....	77
4.5.3. JSP.....	77
4.5.4. Electronic Business XML.	78
4.5.5. Java Web Services APIs.....	78
4.5.6. Αρχιτεκτονική Υπηρεσίας Διαδικτύου σύμφωνα με το πρότυπο J2EE.....	79
4.6. Η αγορά των Υπηρεσιών Διαδικτύου.	80
4.7. Συμπέρασμα.	82
ΚΕΦΑΛΑΙΟ 5^ο : ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ ..	83
5.1. Εισαγωγή.....	83
5.2. Τι σημαίνει Ασφάλεια Υπηρεσιών.....	83
5.3. Τι είναι Πολιτική ασφαλείας.....	85
5.4. Πολιτικές ασφαλείας στο μοντέλο υπηρεσιών διαδικτύου.	86
5.5. Ανάλυση των απαιτήσεων ασφάλειας στις Υπηρεσίες Διαδικτύου.....	87
5.5.1. Εμπιστευτικότητα της πληροφορίας.	88
5.5.2. Εγκυρότητα της πληροφορίας.	89
5.5.3. Διαθεσιμότητα Υπηρεσίας.	89
5.5.4. Εμπιστευτικότητα και εγκυρότητα του λογισμικού.	90
5.5.5. Μη αποποίηση της ευθύνης.	91
5.6. Τι είναι μηχανισμός ασφαλείας.....	91
5.7. Επίπεδα εφαρμογής μηχανισμών ασφαλείας.	91
5.6.1. Επίπεδο Διαδικτύου.	92
5.6.2. Επίπεδο Μεταφοράς.	92
5.6.3. Επίπεδο Εφαρμογής.	93
5.8. Συμπέρασμα.	94



ΚΕΦΑΛΑΙΟ 6^ο : ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΙΣ ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ ..	95
6.1. Εισαγωγή.....	95
6.2. Επίπεδο Διαδικτύου.	95
6.2.1. Πρωτόκολλο IPSP - Μηχανισμοί ασφαλείας.....	95
6.2.2. IPSP και Υπηρεσίες Διαδικτύου.	96
6.2.3. Φίλτρα πακέτων (Packet Filters).....	97
6.3. Επίπεδο Μεταφοράς.....	98
6.3.1. Κρυπτογραφία.	99
6.3.2. Πρωτόκολλο SSL - Μηχανισμοί ασφαλείας.....	100
6.3.3. Πιστοποιητικά X.509.	102
6.3.4. Κωδικοί Αυθεντικοποίησης Μηνυμάτων (MACs).	102
6.3.5. SSL και Υπηρεσίες Διαδικτύου.	103
6.4. Επίπεδο εφαρμογής.	104
6.4.1. Kerberos tickets.....	107
6.4.2. XML Κρυπτογραφία.	107
6.4.3. XML Ψηφιακές Υπογραφές.....	109
6.4.4. XML Υπηρεσίες Διαχείρισης Κλειδιών (XKMS).	111
6.4.5. Γλώσσα Σήμανσης Διαβεβαιώσεων Ασφάλειας (SAML).	113
6.4.6. Εκτεταμένη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης (XACML).	114
6.4.7. Υπηρεσία Μη αποποίησης.	115
6.4.8. XML Application Firewalls.	115
6.5. Συμπέρασμα.	116
ΚΕΦΑΛΑΙΟ 7^ο : ΜΟΝΤΕΛΟ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΙΣ ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ ..	118
7.1. Εισαγωγή.....	118
7.2. Στόχοι του προτεινόμενου μοντέλου ασφαλείας.	118
7.3. Περιγραφή του μοντέλου ασφαλείας.	119
7.4. Ανάλυση του μοντέλου ασφαλείας.	121
7.4.1. Αυθεντικοποίηση πελάτη-υπηρεσίας και Έλεγχος πρόσβασης.	123
7.4.2. Κρυπτογράφηση μηνυμάτων.....	124
7.4.3. Έλεγχος ακεραιότητας των μηνυμάτων.	125
7.4.4. Υπηρεσία μη αποποίησης.	125
7.4.5. Ανίχνευση.....	126
7.5. Αξιολόγηση του μοντέλου ασφάλειας – Συμπέρασμα.....	127
ΚΕΦΑΛΑΙΟ 8^ο : ΥΛΟΠΟΙΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ	128
8.1. Εισαγωγή.....	128
8.2. Ασφάλεια στο .NET.	128
8.2.1. Αυθεντικοποίηση.	129
8.2.2. Εξουσιοδότηση.....	131
8.2.3. Κρυπτογράφηση μηνυμάτων.....	132
8.2.4. Έλεγχος ακεραιότητας των μηνυμάτων.	133
8.2.5. Έλεγχος του κώδικα που εκτελείται.....	133
8.2.6. Ψηφιακή υπογραφή και καταγραφή συναλλαγών.	134
8.3. Ασφάλεια στο J2EE.	134
8.3.1. Αυθεντικοποίηση.	136
8.3.2. Εξουσιοδότηση.....	137
8.3.3. Κρυπτογράφηση μηνυμάτων.....	138
8.3.4. Έλεγχος ακεραιότητας των μηνυμάτων.	138
8.3.5. Έλεγχος του κώδικα που εκτελείται.....	139

8.3.6. Ψηφιακή υπογραφή και καταγραφή συναλλαγών.	140
8.4. Σύγκριση των δύο πλατφόρμων.	140
8.5. Συμπέρασμα.	141
ΚΕΦΑΛΑΙΟ 9^ο : ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΑΝΟΙΚΤΑ ΘΕΜΑΤΑ	143
9.1. Σύνοψη.	143
9.2. Συμπεράσματα.	144
9.3. Συμβολή της εργασίας - Ανοικτά θέματα.	146
9.3.1. Διαχείριση πολιτικών ασφαλείας στο περιβάλλον των υπηρεσιών διαδικτύου... 146	
9.3.2. Αναζήτηση μοντέλου εμπιστοσύνης για τις υπηρεσίες διαχείρισης κλειδιών.... 148	
9.3.3. Παρακολούθηση των συμφωνιών που κλείνονται σε επίπεδο υπηρεσίας. 149	
9.3.4. Παροχή υπηρεσιών ασφάλειας από καταλόγους των υπηρεσιών διαδικτύου. 150	
ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ	152
Στην αγγλική γλώσσα.	152
Στην ελληνική γλώσσα.....	154

ΠΙΝΑΚΕΣ

Πίνακας 1.1. : Δομή της διατριβής.....	21
Πίνακας 1.2.: Συμβολή της παρούσας εργασίας	24
Πίνακας 1.3. : Ορισμοί θεμελιωδών εννοιών.....	25
Πίνακας 6.1.: Μηχανισμοί ασφάλειας υπηρεσιών διαδικτύου του επιπέδου μεταφοράς.....	98
Πίνακας 6.2.: Μηχανισμοί ασφάλειας υπηρεσιών διαδικτύου επιπέδου εφαρμογής.	105
Πίνακας 7.1.: Μηχανισμοί ασφάλειας.	122
Πίνακας 8.1.: Υλοποίηση των μηχανισμών ασφάλειας στην πλατφόρμα .NET.	129
Πίνακας 8.2.: Υλοποίηση των μηχανισμών ασφάλειας στις J2EE πλατφόρμες ανάπτυξης..	135

ΣΧΗΜΑΤΑ

Σχήμα 2.1.: Το μοντέλο των Υπηρεσιών Διαδικτύου. [Kreger, 2001]	34
Σχήμα 3.1.: Αρχιτεκτονική μιας Υπηρεσίας Διαδικτύου. [Shohoud, 2003].....	50
Σχήμα 3.2.: Στοίβα πρωτοκόλλων των Υπηρεσιών Διαδικτύου. [Kreger, 2001]	51
Σχήμα 3.3.: Διασύνδεση απομακρυσμένων δικτυακών τόπων. [Iona, 2002]	54
Σχήμα 3.4.: Μέρη ενός SOAP Μηνύματος. [Curbera et al., 2002]	55
Σχήμα 3.5.: Απλό SOAP μήνυμα. [Curbera et al., 2002].....	55
Σχήμα 3.6.: SOAP RPC μήνυμα. [Curbera et al., 2002].....	56
Σχήμα 3.7.: Δομή WSDL εγγράφου. [Gunzer, 2002]	57
Σχήμα 3.8.: Απεικόνιση των συσχετίσεων μεταξύ των στοιχείων ενός WSDL εγγράφου....	58
Σχήμα 3.9.: UDDI XML Schema. [Gunzer, 2002]	60
Σχήμα 3.10.: Τρόποι δημοσίευσης της περιγραφής μιας Υπηρεσίας. [Kreger, 2001].....	61
Σχήμα 3.11.: Δημιουργία UDDI καταχώρησης από ένα WSDL έγγραφο.....	62
Σχήμα 3.12.: Στατική ανακάλυψη Υπηρεσιών Διαδικτύου.	63
Σχήμα 3.13.: Δυναμική ανακάλυψη υπηρεσιών διαδικτύου. [Iona, 2002]	63
Σχήμα 3.14.: Ανάπτυξη εφαρμογής πελάτη για τη στατική δέσμευση μιας Υ.Δ..	64
Σχήμα 3.15.: Δημιουργία μηνύματος για τη δυναμική δέσμευση μιας Υ.Δ. από ένα πελάτη. 64	
Σχήμα 4.1.: Αρχιτεκτονική Web Service εφαρμογών.....	69



Σχήμα 4.2.: Τα συστατικά του Microsoft .NET. [MS .NET].....	70
Σχήμα 4.3.: Αρχιτεκτονική .NET υπηρεσίας.	74
Σχήμα 4.4.: Αρχιτεκτονική υπηρεσίας διαδικτύου σύμφωνα με το J2EE πρότυπο.....	79
Σχήμα 4.5.: Η πορεία της αγοράς των Υπηρεσιών Διαδικτύου. [Evans, 2002].....	81
Σχήμα 6.1.: Το πρωτόκολλο SSL Handshake.	101
Σχήμα 6.2.: Δομή του συντακτικού της XML κρυπτογράφησης.....	108
Σχήμα 6.3.: Δομή του συντακτικού της XML ψηφιακής υπογραφής.....	110
Σχήμα 7.1.: Συστατικά στοιχεία του μοντέλου ασφάλειας των IBM και Microsoft.	119
Σχήμα 7.2.: Έλεγχος Πρόσβασης στο μοντέλο ασφάλειας των IBM και Microsoft	123
Σχήμα 7.3.: Έκδοση Διαπιστευτηρίων στο μοντέλο ασφάλειας των IBM και Microsoft.	124
Σχήμα 7.4.: Κρυπτογράφηση μηνυμάτων στο μοντέλο ασφάλειας των IBM και Microsoft. 125	
Σχήμα 8.1. : .NET Passport Authentication. [Skoularidou et al., 2002]	131
Σχήμα 8.2.: Programmatic Authorization.	132
Σχήμα 8.3.: Αυθεντικοποίηση στο J2EE. [J2EE SEC]	136

ΠΕΡΙΛΗΨΗ

Οι συνεχώς αυξανόμενες απαιτήσεις του δυναμικού ηλεκτρονικού επιχειρείν, υπογραμμίζουν σήμερα την ανάγκη της χρησιμοποίησης του Διαδικτύου ως μέσο που θα μπορεί να υποστηρίζει την άμεση αλληλεπίδραση μεταξύ εφαρμογών, χωρίς να είναι απαραίτητη η ύπαρξη διεπαφών για τους χρήστες. Οι Υπηρεσίες Διαδικτύου (Web Services) αποτελούν ένα νέο παράδειγμα στον τομέα του προγραμματισμού εφαρμογών, που επεκτείνει σημαντικά τις δυνατότητες του διαδικτύου, παρέχοντας έναν τρόπο για την αλληλεπίδραση των εφαρμογών, ανεξάρτητο από πλατφόρμες και γλώσσες προγραμματισμού.

Την τελευταία τριετία, οι μεγάλες εταιρείες πληροφορικής, έχουν εισέλθει δυναμικά στο χώρο των υπηρεσιών διαδικτύου με στόχο τη δημιουργία μιας δομής τεχνολογιών, που θα παρέχει υποστήριξη στην ανάπτυξη των υπηρεσιών αυτών. Ωστόσο, οι επιχειρήσεις παρουσιάζονται ακόμα επιφυλακτικές να επενδύσουν σε εφαρμογές που βασίζονται στο νέο μοντέλο προγραμματισμού.

Οι έρευνες που έχουν γίνει, έδειξαν ότι η ασφάλεια αποτελεί ένα κρίσιμο παράγοντα για τις επιχειρήσεις σε ότι αφορά στην απόφαση να ακολουθήσουν το νέο ρεύμα. Υπάρχουν πολλά αναπάντητα ερωτήματα που αφορούν τόσο σε τεχνολογικά όσο και σε επιχειρησιακά ζητήματα. Για παράδειγμα, μερικά από τα ερωτήματα είναι:

- α) μπορούν οι υφιστάμενες τεχνολογίες (πρωτόκολλα ασφάλειας, firewalls, intrusion detection systems) να παρέχουν επαρκή ασφάλεια;
- β) οι επιθέσεις θα είναι της ίδιας συχνότητας και του ίδιου τύπου, όπως αυτές που δέχεται ένας απλός δικτυακός τόπος;
- γ) με ποιο τρόπο θα είναι δυνατόν ένας πελάτης να εμπιστευθεί μια υπηρεσία την οποία ανακαλύπτει δυναμικά;
- δ) πώς μια επιχείρηση θα μπορεί να παρέχει τις διαβεβαιώσεις που ζητούν οι πελάτες της όταν δεν είναι σίγουρη για τη διαθεσιμότητα και την αξιοπιστία των συνεργαζόμενων υπηρεσιών που τις παρέχονται από τρίτους;
- ε) με ποιο τρόπο μια επιχείρηση θα μπορεί να δημοσιεύσει στο διαδίκτυο με την μορφή υπηρεσίας μια παλαιότερη εφαρμογή που έχει σχεδιαστεί για το τοπικό της δίκτυο;

Οι απαντήσεις στα παραπάνω ερωτήματα δεν είναι ξεκάθαρες και απαιτούν συστηματική έρευνα. Ένα σημαντικό πλήθος λύσεων, άλλωστε, ήδη υπάρχει σε τεχνικό επίπεδο και το βασικό πρόβλημα είναι η οργάνωση τους και η ένταξη τους σε ένα ενιαίο πλαίσιο ασφάλειας, που να μπορεί να αποτελέσει τη βάση για τη δημιουργία μιας στρατηγικής ασφάλειας από

έναν οργανισμό. Με γνώμονα τα παραπάνω, η παρούσα εργασία αποτελεί μια προσπάθεια να διερευνηθεί και να αναλυθεί διεξοδικά το ζήτημα της ασφάλειας στις υπηρεσίες διαδικτύου (βλ. κεφάλαιο 1).

Στην αρχή της εργασίας (βλ. κεφάλαιο 2) γίνεται μια εισαγωγή στις Υπηρεσίες Διαδικτύου. Πρέπει να τονισθεί ότι υπάρχουν αρκετοί διαφορετικοί ορισμοί σε σχέση με το τι εφαρμογές χαρακτηρίζει ο κάθε ερευνητής ως υπηρεσίες διαδικτύου. Γενικά όμως, οι υπηρεσίες διαδικτύου είναι ανεξάρτητες, τμηματοποιημένες εφαρμογές με διεπαφές βασισμένες σε ανοικτά πρότυπα του Διαδικτύου. Είναι χαλαρά συζευγμένες και επικοινωνούν μεταξύ τους μέσω του Διαδικτύου χρησιμοποιώντας τεχνολογίες βασισμένες σε πρότυπα. Οι Υπηρεσίες Διαδικτύου προσφέρουν σε μια επιχείρηση έναν αυτοματοποιημένο τρόπο επικοινωνίας, μέσω ανταλλαγής μηνυμάτων, με τις εφαρμογές πελατών, συνεταιρών, προμηθευτών, ανεξάρτητα από το υλικό, το λειτουργικό σύστημα και το προγραμματιστικό περιβάλλον που διαθέτουν. Με την ανάπτυξη των Υπηρεσιών Διαδικτύου γίνεται πραγματικότητα η δημιουργία ενός περιβάλλοντος, στο οποίο οι εταιρείες μπορούν να τοποθετούν τις τρέχουσες και μελλοντικές εφαρμογές τους, με τη μορφή υπηρεσιών που μπορούν εύκολα και γρήγορα να εντοπιστούν και να καταναλωθούν.

Η αρχιτεκτονική των Υπηρεσιών Διαδικτύου είναι βασισμένη στην αλληλεπίδραση μεταξύ τριών οντοτήτων:

- α) Του χορηγού των υπηρεσιών (Service Provider),
- β) Του καταλόγου υπηρεσιών (Service Registry) και
- γ) Του πελάτη των υπηρεσιών (Service Requestor).

Οι αλληλεπιδράσεις περιλαμβάνουν τις διαδικασίες δημοσίευσης, εύρεσης και δέσμευσης μιας υπηρεσίας. Τα συνθετικά στοιχεία μιας Υπηρεσίας Διαδικτύου, είναι η υπηρεσία (ενότητα λογισμικού) και η περιγραφή της. Σε ένα τυπικό σενάριο, ο χορηγός της υπηρεσίας που είναι ιδιοκτήτης της εφαρμογής μιας Υπηρεσίας Διαδικτύου, διαμορφώνει μια περιγραφή για την υπηρεσία και τη δημοσιεύει στον κατάλογο υπηρεσιών ή σε κάποιο πελάτη που έχει εκδηλώσει ενδιαφέρον. Ο πελάτης χρησιμοποιεί μια διαδικασία αναζήτησης, για να ανακτήσει την περιγραφή της υπηρεσίας τοπικά ή από τον κατάλογο υπηρεσιών, την οποία περιγραφή χρησιμοποιεί έπειτα για να συνδεθεί με την υπηρεσία και να χρησιμοποιήσει την εφαρμογή.

Στη συνέχεια της εργασίας εξετάζονται οι βασικές τεχνολογίες που χρησιμοποιούν οι υπηρεσίες διαδικτύου (βλ. κεφάλαιο 3). Η XML είναι η βασική τεχνολογία που χρησιμοποιείται κυρίως για τρεις λόγους. Αυτοί είναι:

- α) Η συμφωνία σε επίπεδο μονάδων επικοινωνίας (πρωτόκολλο SOAP),



- β) Η περιγραφή της υπηρεσίας (γλώσσα WSDL) και
- γ) Η ανακάλυψη της υπηρεσίας (UDDI πρότυπο).

Το Simple Object Access Protocol βασίζεται στην XML και ικανοποιεί την ανάγκη για διαλειτουργικότητα μεταξύ εφαρμογών, που βρίσκονται στο διαδίκτυο, υποστηρίζοντας την ανταλλαγή των μηνυμάτων. Η γλώσσα περιγραφής υπηρεσιών Web Services Definition Language, είναι ένα XML schema, που καθορίζει τις προδιαγραφές για τα μηνύματα που αποτελούν το μέσο της επικοινωνίας του πελάτη με το χορηγό της υπηρεσίας. Το Universal Description, Discovery and Integration είναι ένα μοντέλο δεδομένων σε XML που ορίζει ένα χώρο αποθήκευσης για καταχώρηση και αναζήτηση περιγραφών υπηρεσιών διαδικτύου.

Κατόπιν, περιγράφονται τα δύο σημαντικότερα μοντέλα ανάπτυξης υπηρεσιών διαδικτύου, που είναι το Microsoft .NET και το Java 2 Enterprise Edition (βλ. κεφάλαιο 4). Το .NET επιτρέπει σε μια επιχείρηση να δημιουργήσει δικές της Υπηρεσίες Διαδικτύου βασισμένες στο XML πρότυπο και είναι αποτέλεσμα αναθεώρησης ενός σημαντικού μέρους της Microsoft υποδομής. Το J2EE υποστηρίζει την ανάπτυξη Υπηρεσιών Διαδικτύου επεκτείνοντας την αρχιτεκτονική του με τη χρήση ενός συνόλου προτύπων που ονομάζονται Java APIs for XML.

Μετά την περιγραφή των δύο μοντέλων ανάπτυξης εξετάζεται αναλυτικά το θέμα της ασφάλειας (βλ. κεφάλαιο 5). Οι βασικές απαιτήσεις ασφάλειας στο μοντέλο των υπηρεσιών διαδικτύου που αναλύονται είναι :

- α) Η εξασφάλιση της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας της πληροφορίας που ανταλλάσσεται με τη μορφή SOAP μηνυμάτων ή είναι αποθηκευμένη σε καταλόγους με τη μορφή WSDL εγγράφων,
- β) Η εξασφάλιση της διαθεσιμότητας των υπηρεσιών,
- γ) Η εξασφάλιση της εγκυρότητας και εμπιστευτικότητας του λογισμικού των υπηρεσιών, και
- δ) Η εξασφάλιση της μη αποποίησης της ευθύνης της οντότητας πελάτη και της οντότητας χορηγού της υπηρεσίας.

Γενικά, στο περιβάλλον του διαδικτύου η εξασφάλιση των απαιτήσεων ασφάλειας περιλαμβάνει στις περισσότερες περιπτώσεις μηχανισμούς των επιπέδων εφαρμογής, μεταφοράς και διαδικτύου. Στην περίπτωση των υπηρεσιών διαδικτύου ωστόσο, οι μηχανισμοί των επιπέδων μεταφοράς και διαδικτύου δεν μπορούν σε αρκετές περιπτώσεις να παρέχουν λύσεις για την ασφάλεια, όπως το επιτυγχάνουν στις παραδοσιακές υπηρεσίες client-server. Οι ιδιαιτερότητες που υπάρχουν, κυρίως στη δομή μιας τοπολογίας από συνεργαζόμενες υπηρεσίες διαδικτύου, υποδεικνύουν την αντιμετώπιση των περισσότερων ζητημάτων ασφάλειας σε επίπεδο εφαρμογής (βλ. κεφάλαιο 6). Η ανάγκη για εξασφάλιση της

επικοινωνίας με τον τελικό χρήστη, καθώς και η ανάγκη εφαρμογής πολιτικών σε περιβάλλοντα που υπάρχουν διαφορετικά πεδία εφαρμογής πολιτικών ασφαλείας (policy domains), καθιστά δύσκολη την εφαρμογή μηχανισμών ασφαλείας σε χαμηλό επίπεδο. Για το λόγο αυτό, η αντιμετώπιση των απαιτήσεων ασφαλείας λαμβάνει χώρα κυρίως στο επίπεδο εφαρμογής.

Τα πρότυπα που ξεχωρίζουν στο επίπεδο εφαρμογής είναι τα πρότυπα **XML ENCryptio**n, **XML Digital Signatures**, **XML Key Management Services**, **Security Assertion Markup Language** και **eXtensible Access Control Markup Language**. Τα πρότυπα XML ENC και XML DS επεκτείνουν τις δυνατότητες των τεχνολογιών κρυπτογράφησης και ψηφιακής υπογραφής, επιτρέποντας τη δυνατότητα ξεχωριστής εφαρμογής τους στο ίδιο έγγραφο από διαφορετικές οντότητες. Το πρότυπο XKMS καθορίζει ένα τρόπο κλήσης διαδικασιών διαχείρισης δημοσίου κλειδιού, μέσω XML μηνυμάτων. Επίσης, τα πρότυπα SAML και XACML υποστηρίζουν από κοινού τη διαδικασία εξουσιοδότησης του τελικού χρήστη σε μια υπηρεσία διαδικτύου.

Η ύπαρξη των παραπάνω τεχνολογιών, ωστόσο δεν αποτελεί από μόνη της λύση για τα ζητήματα ασφάλειας που υπάρχουν. Το πρόβλημα εξακολουθεί να βρίσκεται στον τρόπο με τον οποίο ένας οργανισμός θα επιλέξει τις κατάλληλες λύσεις και θα τις προσαρμόσει στις απαιτήσεις του. Για το λόγο αυτό στη συνέχεια της εργασίας γίνεται αναφορά στη προσπάθεια των εταιρειών IBM και Microsoft να δημιουργήσουν ένα μοντέλο ασφαλείας. Στόχος του μοντέλου αυτού, που ακόμα δεν έχει ολοκληρωθεί, είναι να αποτελέσει στο μέλλον ένα πρότυπο για τους οργανισμούς, που θα τους επιτρέπει να σχεδιάσουν, και εν συνεχεία να υλοποιήσουν την αρχιτεκτονική ασφάλειας που προτείνει, προσαρμόζοντάς την στους στόχους ασφάλειας που έχουν θέσει.

Η ανάλυση του μοντέλου (βλ. κεφάλαιο 7), έδειξε πως με βάση τον τρόπο που έχει σχεδιαστεί, δύναται να αποτελέσει ένα γενικό πλαίσιο ασφάλειας που θα ικανοποιεί τις κύριες απαιτήσεις ασφάλειας των υπηρεσιών διαδικτύου. Διαθέτει δηλαδή τα χαρακτηριστικά εκείνα που το καθιστούν ολοκληρωμένο μοντέλο, σε ότι αφορά την κάλυψη των συγκεκριμένων απαιτήσεων ασφάλειας που εξετάζονται στην έρευνά μας. Ωστόσο, είναι λίγο πρόωρο να αξιολογηθεί. Σίγουρα όμως, απαραίτητη προϋπόθεση για την επιτυχία του, είναι η υποστήριξη του από τους πελάτες και τους χορηγούς των υπηρεσιών διαδικτύου, και ασφαλώς και η συνεργασία με τους οργανισμούς ανάπτυξης προτύπων.

Πάντως, παρά τη μη ύπαρξη ενός μοντέλου ασφάλειας και παρά την ανάγκη για ανάπτυξη νέων προδιαγραφών, υπάρχουν κάποιες έτοιμες υλοποιήσεις ασφάλειας που μπορούν να χρησιμοποιηθούν. Η μελέτη που έγινε στις πλατφόρμες ανάπτυξης .NET και

J2EE (βλ. κεφάλαιο 8) έδειξε ότι παρέχουν υπηρεσίες ασφάλειας, που μπορούν να αξιοποιηθούν από τους υπεύθυνους ανάπτυξης και διαχείρισης των υπηρεσιών διαδικτύου. Βέβαια υπάρχουν ακόμα σημαντικές ελλείψεις, ωστόσο το πιο σημαντικό είναι ότι, όπως φάνηκε, η αντιμετώπιση του ζητήματος της ασφάλειας παρά το γεγονός ότι φαίνεται να είναι επιτακτική ανάγκη για την ανάπτυξη των υπηρεσιών διαδικτύου, εισάγει νέα ζητήματα διαλειτουργικότητας. Η πλατφόρμα .NET εισάγει πολλούς περιορισμούς στο θέμα αυτό. Οι πλατφόρμες J2EE γενικά δεν εισάγουν περιορισμούς στη διαλειτουργικότητα, ωστόσο βρίσκονται ένα βήμα πιο πίσω στην υλοποίηση των SOAP-based μηχανισμών ασφάλειας.

Τέλος, η παρούσα εργασία καταλήγει σε συμπεράσματα και παρουσιάζει ορισμένα ανοικτά θέματα που μπορεί να αποτελέσουν αφορμή για περαιτέρω έρευνα στο μέλλον (βλ. κεφάλαιο 9). Τέτοια θέματα αφορούν στη διαχείριση των κρυπτογραφικών κλειδιών, στη διαχείριση των πολιτικών ασφαλείας, στη παρακολούθηση συμφωνιών που κλείνονται σε επίπεδο υπηρεσίας και στη παροχή υπηρεσιών ασφάλειας από καταλόγους υπηρεσιών.



EXECUTIVE SUMMARY

The continuously increasing requirements of dynamic e-business underline today the necessity to use the Web as a medium that enables direct application-to-application interactions. Web Services constitute a new paradigm in the sector of applications programming that extends considerably Internet capabilities providing a way for application-to application interactions, independent from platforms and programming languages. The last three-year period, the leading companies in Information Technology, have entered dynamically in the sector of Web services aiming at the creation of a technology stack, which will provide support in the development of these services. The enterprises, however, are circumspect to invest in applications that are based on the new programming model.

Recent researches proved that security constitutes a critical factor for the enterprises decision to follow the new computing paradigm. The main reason is that there are a lot of questions related to technological and operational problems. For example, some of these questions are:

- a) Can the existing technologies (security protocols, firewalls, intrusion detection systems) provide sufficient security?
- b) Will the attacks appear to be of the same type and frequency, as those that occur in a simple website?
- c) How will it be possible for a customer to entrust a service that he discovers dynamically?
- d) How enterprises might provide the assurances to their customers, when they are not sure about the availability and the reliability of other supporting services that are provided by third parts?
- e) How an enterprise might expose to the Internet a legacy application that was designed to work in a local network?

The answers in these questions are not evident and require systematic research. Moreover, the basic idea is that the existing solutions need to be organised and integrated in a security framework, which can be used as the base for an enterprise to make strategic plans about security. The aim of this project, is studying and exploiting of security issues in Web Services (see chapter 1).

At the beginning of this project (see chapter 2) we present an introduction to Web Services. It is worth-mentioned that it is rather difficult to select a definition for the term Web



Services from the numerous that have been given. Anyway, in general terms, Web Services are self-contained modular business applications that have open, Internet-oriented, standards-based interfaces. Web Services are loosely coupled, communicating directly with other Web services via the Internet using standards-based technologies. This standards-based communication allows Web Services to be accessed by customers, suppliers, and trading partners independent of hardware, operating system, or even programming environment. The result is an environment where businesses can expose their current and future business applications as Web services that can be easily discovered and consumed by external partners.

The Web Services architecture is based upon the interactions between three roles: a) Service Provider, b) Service Registry and c) Service Requestor. The interactions involve the publish, find and bind operations. These roles and operations act upon the Web Services artifacts: the web service software module and its description. In a typical scenario, a Service Provider hosts an implementation of a Web Service, defines a description for the service and publishes it to a Service Registry. The Service Requestor uses a find operation to retrieve the service description from the Service Registry. Then it uses the service description to bind with the Service Provider and interact with the Web Service application.

Advancing, there is a reference to the basic technologies that support Web Services (see chapter 3). XML is the basic technology in Web Services for the following three reasons: a) communication at the lowest level, b) creating service description and c) enabling service discovery. Simple Object Access Protocol is an XML-based protocol used to define the exchange of information between the Service Requestor and the Service Provider. This is the central communication standard within Web Services. Web Services Definition Language is an XML schema that determines the specifications for the messages that are exchanged between the Service Requestor and the Service Provider. Universal Description, Discovery, and Integration is an XML data model that provides directory services. A Web Service can be registered in a UDDI registry, so that it can be discovered and accessed by a Service Requestor.

Proceeding, we describe the most important models that support Web Services development (see chapter 4). These are the Microsoft .Net and the Java 2 Enterprise Edition. Both .Net and J2EE enable an enterprise to develop its own Web Services based on the XML (eXtensible Markup Language) standard. For J2EE, Web Services support is the result of an extension to its existing architecture, using a set of standards called the Java APIs for XML. For .NET, Web Services support is the result of a revising of the Microsoft infrastructure.



After the general description of Web Services environment, there is a comprehensive study of the security issues (see chapter 5). As it is mentioned, a secure Web Service has to meet important requirements, such as:

- a) Confidentiality, authenticity and integrity of the information that is exchanged between the Service Provider and the Service Requestor (SOAP messages) or that is stored in Service Registries (WSDL documents),
- b) Service availability,
- c) Validity and confidentiality of software, and
- d) Non-repudiation of origin and non-repudiation of destination.

The effort to assure security requirements in Internet environment, includes usually application-level, transport-level and internet-level mechanisms. In the case of Web services, transport-level mechanisms and internet-level mechanisms fail to provide sufficient security solutions, as they achieve in the case of traditional client server applications. The distinguishing characteristics of a web services collaborating topology, indicate the encountering of security issues in application level (see chapter 6). To be more specific, the need to assure communication with the end user, as well as the need to apply security policies in different policy domains, makes difficult to apply security mechanisms in low level. This was the main reason for researchers to concentrate in developing application level mechanisms.

The basic standards in application level are **XML ENCryption**, **XML Digital Signatures**, **XML Key Management Service**, **Security Assertion Markup Language** and **eXtensible Access Control Markup Language**. XML ENC and XML DS standards extend the capabilities of encryption and digital signature technologies, including new protocols for encrypting and signing sections of XML documents. XKMS standard describes the distribution and registration of public keys, so that a Web Service can access an XKMS compliant server in order to receive updated key information for encryption and authentication. Finally, SAML and XACML are standards for asserting authentication and authorization information and defining policies for access control of XML documents correspondingly.

The existence of the afore-mentioned technologies does not constitute a sufficient solution to the security problem. The most important problem is to define how it is possible for an organization to choose the suitable solutions and adapting them in its requirements. Responding to this concern, IBM and Microsoft have collaborated on a proposed Web Services Security plan and roadmap for developing a set of Web Services Security

Specifications that can support a security model. The goal is to create a standard solution, that will allow organizations in the future to build interoperable and secure Web services that leverage and expand upon existing investments in security infrastructure, while allowing them to take full advantage of the integration and interoperability benefits Web service technologies have to offer.

The analysis of the proposed security model (see chapter 7), demonstrated that the way it has been designed, it is capable of constituting a security framework that will satisfy the basic security requirements. In general terms, it incorporates the fundamental characteristics in order to qualify as a comprehensive security model, making the assumption that its objective is to cover the specific requirements we have already mentioned. However, essential prerequisite for the proposed model's success, is that it will be supported by customers, service providers, and certainly by organizations that develop security standards.

Nevertheless, despite the not existence of a security model and despite the ongoing need for development of new specifications, there are some partial solutions to the security problem (see chapter 8). These are some specific security implementations, which are ready to be used. Both .NET and J2EE provide security services that can be exploited by Web Service developers. By examining security services in these platforms we found important deficiencies, however the most important finding was that attempting to implement security solutions may import additional interoperability issues. That is obvious in .NET platform, where authentication and authorization services are provided through Microsoft OSes and identification repositories. J2EE platforms in general do not import these restrictions, but they are one level behind in developing SOAP-based security.

Concluding this project, we present several open scientific issues, that can constitute reasons for further future research (see chapter 9). These have to do with cryptographic key management, security policies management, monitoring of service level agreements and development of security services that can be offered by web service registries.



ΚΕΦΑΛΑΙΟ 1^ο : ΕΙΣΑΓΩΓΗ

1.1. Πρόλογος.

Το Διαδίκτυο αρχικά δημιουργήθηκε για να αποτελέσει ένα μέσο για την αποτελεσματική διανομή και διάδοση της πληροφορίας σε παγκόσμια κλίμακα. Έχοντας ξεκινήσει να λειτουργεί σαν μια γιγαντιαία βιβλιοθήκη, με κατανεμημένο περιεχόμενο, σταδιακά έγινε δημοφιλές και προσιτό σε ένα μεγάλο μέρος του πληθυσμού του πλανήτη. Το γεγονός αυτό, αποτέλεσε και αποτελεί κίνητρο για τις επιχειρήσεις, προκειμένου να διευρύνουν τις επιχειρηματικές τους δραστηριότητες. Ένας από τους κύριους στόχους των περισσότερων επιχειρήσεων πλέον, είναι να αξιοποιήσουν το Διαδίκτυο, όχι μόνο ως μέσο διάδοσης της πληροφορίας, αλλά και ως μέσο που τους επιτρέπει να βελτιώσουν τον τρόπο επικοινωνίας και συναλλαγής με πελάτες, προμηθευτές, διανομείς και συνεργάτες. Γενικά, η ενσωμάτωση στο περιβάλλον του Διαδικτύου εφαρμογών που επιτρέπουν τη διαχείριση των λειτουργιών μιας επιχείρησης, είναι το κύριο χαρακτηριστικό του επιχειρηματικού μοντέλου που ονομάζεται δυναμικό ηλεκτρονικό επιχειρείν (*dynamic e-business*) [Giisolfi, 1992].

Στις μέρες μας, άμεση απαίτηση για την περαιτέρω ανάπτυξη του δυναμικού ηλεκτρονικού επιχειρείν είναι ο επαναπροσδιορισμός του σκοπού που εξυπηρετεί το Διαδίκτυο. Η εξέλιξη του Διαδικτύου την τελευταία δεκαετία σίγουρα έχει επιτρέψει την πραγματοποίηση εξεζητημένων μορφών αλληλεπίδρασης μεταξύ πελατών και κεντρικών υπολογιστικών συστημάτων. Παραδείγματα τέτοιων αλληλεπιδράσεων αποτελούν οι πράξεις που εκτελούνται με απλή συμπλήρωση μιας ηλεκτρονικής φόρμας από τον πελάτη, οι δοσοληψίες μέσω εφαρμογών ηλεκτρονικού εμπορίου και οι σύνθετες ενδοεπιχειρησιακές συναλλαγές. Αυτές όμως, σήμερα, θεωρούνται ως ελάχιστες μόνο από τις δυνατότητες που μπορεί να παρέχει το Διαδίκτυο. Οι δυνατότητες αυτές, άλλωστε, υποστηρίζονται χωρίς να έχει επέλθει αλλαγή στη θεμελιώδη φιλοσοφία του, που το καθορίζει ως μέσο που επιτρέπει την αλληλεπίδραση ανθρώπου-εφαρμογής.

Οι συνεχώς αυξανόμενες ανάγκες του δυναμικού ηλεκτρονικού επιχειρείν υπογραμμίζουν σήμερα την ανάγκη της χρησιμοποίησης του Διαδικτύου ως μέσο το οποίο θα μπορεί να υποστηρίζει την αλληλεπίδραση μεταξύ εφαρμογών [Curtbera et al., 2001]. Την ανάγκη αυτή, φαίνεται πως σταδιακά συμμερίζεται όλο και μεγαλύτερο μέρος της επιστημονικής κοινότητας. Εντούτοις, η νέα αυτή απαίτηση φέρνει στην επιφάνεια πολλά ερωτήματα που αναζητούν λύση. Πρώτα απ' όλα τίθεται το βασικό ερώτημα ποιο είναι το κατάλληλο

πρότυπο για να υποστηρίξει τις αλληλεπιδράσεις μεταξύ εφαρμογών στο περιβάλλον του διαδικτύου με συστηματικό τρόπο. Επίσης, ένα δεύτερο ερώτημα είναι πώς η νέα κατανεμημένη υπολογιστική πλατφόρμα, που θα παρέχει την αλληλεπίδραση αυτή, θα ενσωματωθεί στα προϋπάρχοντα περιβάλλοντα, όπως αυτά παρουσιάζονται ήδη μέσα στα ιδιωτικά δίκτυα.

Οι Υπηρεσίες Διαδικτύου (Web Services) αποτελούν ένα νέο παράδειγμα στον τομέα του προγραμματισμού εφαρμογών, που επεκτείνει σημαντικά τις δυνατότητες του διαδικτύου. Το μοντέλο των υπηρεσιών διαδικτύου επιτυγχάνει να δώσει απάντηση στα ερωτήματα που προβάλλουν εμπόδιο στην ανάπτυξη του δυναμικού ηλεκτρονικού επιχειρείν, παρέχοντας έναν τρόπο για την αλληλεπίδραση των εφαρμογών, ανεξάρτητο από πλατφόρμες και γλώσσες προγραμματισμού.

1.2. Σκοπός της παρούσας εργασίας.

Οι Υπηρεσίες Διαδικτύου αποτελούν στις μέρες μας αντικείμενο μελέτης για τους ερευνητές και πόλο έλξης για τις εταιρείες που κατασκευάζουν λογισμικό και δικτυακό εξοπλισμό. Την τελευταία τριετία, οι μεγάλες εταιρείες πληροφορικής, στην πλειοψηφία τους, έχουν εισέλθει δυναμικά στο χώρο των υπηρεσιών διαδικτύου με στόχο τη δημιουργία μιας δομής τεχνολογιών, που θα παρέχει υποστήριξη στην ανάπτυξη των υπηρεσιών αυτών. Οι προσπάθειες σε γενικές γραμμές έχουν αποδώσει, αφού ήδη οι βασικές τεχνολογίες έχουν προτυποποιηθεί και είναι αποδεκτές από την πλειοψηφία των εταιρειών. Το γεγονός αυτό καθιστά αισιόδοξους αρκετούς, που οραματίζονται ήδη τις επιχειρήσεις στο μέλλον να λειτουργούν με νέους τρόπους, χρησιμοποιώντας νέα επιχειρηματικά μοντέλα, διαφορετικά από τα σημερινά. Εντούτοις, πολλοί ερευνητές τηρούν ακόμα επιφυλακτική στάση, κυρίως γιατί πάρα πολλά ερωτήματα σε τεχνολογικά και επιχειρησιακά ζητήματα παραμένουν αναπάντητα. Ένα από αυτά τα ζητήματα είναι και η ασφάλεια. Ο σκοπός της παρούσας εργασίας είναι η διερεύνηση του ζητήματος της ασφάλειας στις Υπηρεσίες Διαδικτύου.

1.3. Κίνητρα για την πραγματοποίηση της παρούσας εργασίας.

Αδιαμφισβήτητα, το ζήτημα της ασφάλειας συστημάτων και εφαρμογών στις μέρες μας, λαμβάνει συνεχώς μεγαλύτερες διαστάσεις, εξαιτίας της τεράστιας εξάπλωσης του διαδικτύου. Επιπλέον, η ασφάλεια των πληροφοριακών συστημάτων προκαλεί ολοένα

ανξανόμενη ευαισθητοποίηση στις επιχειρήσεις, αλλά και στο ευρύ κοινό λόγω της δημοσιοποίησης αρκετών συμβάντων παραβίασης της ασφάλειας που είχαν μεγάλες οικονομικές συνέπειες σε αρκετές εταιρείες. Στην ετήσια έκθεση του FBI [Power, 2002] για το έτος 2002, το ποσοστό των εταιρειών που διαπίστωσαν μη εξουσιοδοτημένη πρόσβαση στο δικτυακό τους τόπο ή και σφετερισμό του δικαιώματος της πρόσβασης έχει διπλασιαστεί σε σύγκριση με το έτος 1999. Για την ίδια χρονική περίοδο μάλιστα οι συνολικές οικονομικές απώλειες που αφορούν σε παραβιάσεις τις ασφάλειας έχουν τριπλασιαστεί, με πιο εντυπωσιακή την αύξηση των απωλειών που οφείλονται σε επιθέσεις εισβολής στο σύστημα (system penetration) και επιθέσεις τύπου άρνησης της υπηρεσίας (denial of service attacks).

Τα αποτελέσματα αυτά, όπως φαίνεται, έχουν αντίκτυπο στον τομέα ανάπτυξης νέων υπηρεσιών που έχουν ως βάση το διαδίκτυο, όπως είναι οι Υπηρεσίες Διαδικτύου. Από έρευνα της εταιρείας Jupiter Media Metrix¹ σε πλήθος 500 επιχειρήσεων, προέκυψε ότι: α) ένα ποσοστό 60% των επιχειρήσεων επρόκειτο να χρησιμοποιήσει μέσα στο έτος 2002 τις Υπηρεσίες Διαδικτύου για την ενοποίηση των εφαρμογών εντός του δικτύου του, β) ένα 53% επρόκειτο να τις χρησιμοποιήσει για τη σύνδεση των εφαρμογών τους με εφαρμογές γνωστών πελατών, προμηθευτών και συνεργατών, και γ) μόλις ένα 16% επρόκειτο να τις χρησιμοποιήσει για δυναμική αναζήτηση και αλληλεπίδραση με εφαρμογές τρίτων.

Το παραπάνω γεγονός ότι το ζήτημα της ασφάλειας αποτελεί εμπόδιο στην εξάπλωση των Υπηρεσιών Διαδικτύου. Οι επιχειρήσεις δεν είναι ακόμα σίγουρες για τη διαθεσιμότητα και την αξιοπιστία μιας Υπηρεσίας Δικτύου, που τους προσφέρεται από μια άλλη επιχείρηση, και ως εκ τούτου δεν μπορούν να αναλάβουν το ρίσκο που συνεπάγεται η αποτυχία του χορηγού μιας τέτοιας υπηρεσίας να παρέχει ότι υπόσχεται. Αυτό φαίνεται πιο έντονα στην περίπτωση που μια επιχείρηση καλείται να αλληλεπιδράσει με δυναμικό τρόπο με επιχειρήσεις με τις οποίες δεν έχει συνάψει ποτέ επιχειρηματικές σχέσεις.

1.4. Ανάγκη για την πραγματοποίηση της παρούσας εργασίας.

Παρά το γεγονός ότι η ανάπτυξη των υπηρεσιών διαδικτύου είναι ένας τομέας που παρουσιάζει ραγδαία εξέλιξη, το ζήτημα της ασφάλειας δεν έχει ακόμα αντιμετωπιστεί συστηματικά. Μολονότι, πάρα πολλές λύσεις για την ασφάλεια των υπηρεσιών σε τεχνικό επίπεδο υπάρχουν, δεν είναι συστηματοποιημένες και δεν έχουν ενταχθεί σε ένα ενιαίο πλαίσιο που να μπορεί να αποτελέσει τη βάση για τη δημιουργία μιας στρατηγικής ασφάλειας

¹ στην έρευνα αυτή θα γίνει πιο αναλυτική αναφορά στο επόμενο κεφάλαιο

από έναν οργανισμό. Οι τεχνολογίες και οι μηχανισμοί ασφάλειας που υπάρχουν, με τον τρόπο που παρουσιάζονται, δεν συσχετίζονται με συγκεκριμένες απαιτήσεις ασφάλειας και κατά συνέπεια δεν αξιολογούνται σύμφωνα με την ικανότητά τους να καλύψουν συγκεκριμένες απαιτήσεις.

Στην παρούσα εργασία, αφού αρχικά διερευνώνται οι απαιτήσεις ασφάλειας, γίνεται μια προσπάθεια να παρουσιαστούν και να αξιολογηθούν οι λύσεις που υπάρχουν για την αντιμετώπιση του ζητήματος της ασφάλειας στις υπηρεσίες διαδικτύου, με βάση ένα πλαίσιο που περιλαμβάνει τις κυριότερες απαιτήσεις. Το ίδιο επιχειρείται, στο βαθμό που είναι εφικτό, και για τα πρότυπα ή τις τεχνολογίες που είναι αυτή τη στιγμή στο στάδιο της ανάπτυξης.

1.5. Προσδιορισμός του ερευνητικού προβλήματος.

Η προβληματική περιοχή που καλείται να διερευνήσει η παρούσα εργασία έχει τον τίτλο «Ασφάλεια στις Υπηρεσίες Διαδικτύου».

Τα ερωτήματα που αποτελούν αφορμή για έρευνα είναι τα ακόλουθα:

- E1: Με βάση ποιό πλαίσιο απαιτήσεων ασφάλειας μπορεί να αντιμετωπιστεί το πρόβλημα της ασφάλειας στις Υπηρεσίες Διαδικτύου;
- E2: Ποιές τεχνολογίες μπορούν να αποτελέσουν τη βάση για την αντιμετώπιση του προβλήματος;

Τα παραπάνω ερωτήματα έχουν ιδιαίτερη σημασία για τους ειδικούς της επιστήμης των υπολογιστών, για το λόγο αυτό και η παρούσα εργασία απευθύνεται καθαρά σε αυτούς.

1.6. Αντικείμενο και στόχοι της παρούσας εργασίας.

Στην ενότητα αυτή καθορίζονται: α) τα ζητήματα στα οποία θα επικεντρωθεί η εργασία και β) οι στόχοι της παρούσας εργασίας.

1.6.1. Ζητήματα στα οποία επικεντρώνεται η εργασία.

Η ασφάλεια αποτελεί κρίσιμο παράγοντα για τη λειτουργία των υπηρεσιών διαδικτύου, όπως ισχύει άλλωστε για κάθε εφαρμογή που εκτίθεται στο διαδίκτυο. Το μοντέλο των



υπηρεσιών διαδικτύου χαρακτηρίζεται από ιδιαιτερότητες που απαιτούν τη διαφοροποίηση των υφιστάμενων προσεγγίσεων στο ζήτημα της ασφάλειας, οι οποίες κατά κανόνα αφορούν σε παραδοσιακές client-server εφαρμογές.

Στην παρούσα εργασία, προκειμένου να καταστεί σαφές το παραπάνω γεγονός και να προσδιοριστούν οι ιδιαιτερότητες, γίνεται εκτενής περιγραφή του μοντέλου των Υπηρεσιών Διαδικτύου, προτού διερευνηθεί η ασφάλεια στις υπηρεσίες αυτές.

Συγκεκριμένα, τα ζητήματα στα οποία επικεντρώνεται η παρούσα εργασία, με τη σειρά που παραθέτονται, είναι τα εξής:

1. Ορισμός των Υπηρεσιών Διαδικτύου, προσδιορισμός των χαρακτηριστικών τους και μελέτη των προτύπων και των τεχνολογιών που τις υποστηρίζουν.
2. Προσδιορισμός των απαιτήσεων ασφάλειας στο περιβάλλον των Υπηρεσιών Διαδικτύου.
3. Καταγραφή και αξιολόγηση των τεχνικών και των πρακτικών που υπάρχουν.
4. Ανάδειξη των ζητημάτων που παραμένουν ανοιχτά και χρήζουν περαιτέρω διερεύνησης.

1.6.2. Στόχοι της παρούσας εργασίας.

Γενικά, οι στόχοι της παρούσας εργασίας είναι: α) να δοθεί ένας σαφής ορισμός για τις Υπηρεσίες Διαδικτύου, β) να μελετηθούν τα πρότυπα και οι υπάρχουσες τεχνολογίες που σχετίζονται με την ανάπτυξη τέτοιου είδους υπηρεσιών, γ) να αναλυθούν τα ζητήματα ασφάλειας που συνδέονται με τις υπηρεσίες και τις τεχνολογίες που τις υποστηρίζουν, δ) να καταγραφούν και να αξιολογηθούν οι προτεινόμενες λύσεις και αν είναι δυνατόν να προταθούν λύσεις σε τομείς που οι υπάρχουσες λύσεις δεν επαρκούν. Οι δύο πρώτοι στόχοι καλύπτονται όπως θα αναφερθεί στη συνέχεια στα κεφάλαια 2, 3 και 4 της εργασίας. Οι δύο τελευταίοι στόχοι, αφορούν στην ασφάλεια και καλύπτονται στα επόμενα. Προκειμένου να αντιμετωπιστεί πιο συστηματικά το ζήτημα της ασφάλειας, οι δύο τελευταίοι στόχοι είναι απαραίτητο να αναλυθούν περισσότερο και να γίνουν πιο συγκεκριμένοι. Αναλυτικότερα επομένως, οι στόχοι της παρούσας εργασίας σε ότι αφορά την ασφάλεια είναι οι εξής:

- ✓ Προσδιορισμός των απαιτήσεων ασφάλειας, με βάση τις ιδιαιτερότητες των υπηρεσιών.
- ✓ Ανάπτυξη ενός πλαισίου ασφάλειας για την περιγραφή μηχανισμών και τεχνολογιών που υπάρχουν ή είναι υπό ανάπτυξη.

- ✓ Κριτική και αξιολόγηση των λύσεων που υπάρχουν με βάση το παραπάνω πλαίσιο ασφάλειας. Προτάσεις σε επιμέρους ζητήματα.
- ✓ Ανάδειξη των ανοικτών θεμάτων που μπορεί να αποτελέσουν αφορμή για περαιτέρω έρευνα στο μέλλον.

1.7. Δομή της εργασίας.

Η παρούσα εργασία, όπως προκύπτει και από την προηγούμενη παράγραφο, μπορεί εννοιολογικά να χωριστεί σε δύο μέρη (πίνακας 1.1.). Στο πρώτο μέρος δίνεται η γενική περιγραφή των υπηρεσιών διαδικτύου, προκειμένου να αποδοθεί η εικόνα του περιβάλλοντος των υπηρεσιών διαδικτύου, η οποία είναι απαραίτητη για την οριοθέτηση του προβλήματος. Στο δεύτερο μέρος, η εργασία επικεντρώνεται στο ζήτημα της ασφάλειας.

Μέρος Α'	
Κεφάλαιο 2	Υπηρεσίες Διαδικτύου
Κεφάλαιο 3	Υπηρεσίες Διαδικτύου και XML
Κεφάλαιο 4	Ανάπτυξη Υπηρεσιών Διαδικτύου βασισμένων σε XML
Μέρος Β'	
Κεφάλαιο 5	Απαιτήσεις Ασφάλειας στις Υπηρεσίες Διαδικτύου
Κεφάλαιο 6	Τεχνολογίες Ασφάλειας στις Υπηρεσίες Διαδικτύου
Κεφάλαιο 7	Μοντέλο Ασφάλειας για τις Υπηρεσίες Διαδικτύου
Κεφάλαιο 8	Υλοποιήσεις Ασφάλειας
Κεφάλαιο 9	Συμπεράσματα – Ανοικτά θέματα

Πίνακας 1.1. : Δομή της διατριβής

Στο δεύτερο κεφάλαιο ορίζονται οι υπηρεσίες διαδικτύου και γίνεται αναφορά στην αιτία που οδήγησε στην εμφάνισή τους και στα κίνητρα που συμβάλλουν στην υιοθέτησή τους. Επίσης, περιγράφεται η αρχιτεκτονική τους, προσδιορίζεται το πεδίο εφαρμογής τους και επισημαίνονται οι προκλήσεις που δυσχεραίνουν την εξάπλωση τους.

Στο τρίτο κεφάλαιο παρουσιάζονται οι τεχνολογίες και τα πρότυπα που υποστηρίζουν τις υπηρεσίες διαδικτύου, επισημαίνεται η σημασία τους και περιγράφεται αναλυτικά ο τρόπος λειτουργίας των υπηρεσιών.



Στο τέταρτο κεφάλαιο εξετάζονται τα μοντέλα ανάπτυξης που υπάρχουν για τις υπηρεσίες διαδικτύου και δίνεται μια εικόνα της αγοράς, όπου φαίνονται ποιες τάσεις και προοπτικές υπάρχουν στον ερευνητικό και βιομηχανικό χώρο.

Στο πέμπτο κεφάλαιο, αφού πρώτα αναφέρονται οι ιδιότητες με βάση τις οποίες ορίζεται στο πλαίσιο της εργασίας η έννοια της ασφάλειας των υπηρεσιών, εντοπίζονται και αναλύονται οι απαιτήσεις ασφάλειας που σχετίζονται με το περιβάλλον των υπηρεσιών διαδικτύου και τις ιδιαιτερότητες που το χαρακτηρίζουν. Η ικανοποίηση κάθε απαίτησης ασφάλειας ξεχωριστά αποτελεί, στη συνέχεια το κλειδί για τη αξιολόγηση των μεθόδων και των τεχνολογιών που αναφέρονται. Τα επίπεδα που χρησιμοποιούνται για την αναζήτηση και καταγραφή των τεχνολογικών λύσεων, που αφορούν κυρίως σε πρωτόκολλα και πρότυπα ασφαλείας, είναι τα επίπεδα της στρωματοποιημένης αρχιτεκτονικής της οικογένειας πρωτοκόλλων του διαδικτύου TCP/IP.

Στο έκτο κεφάλαιο, γίνεται αναφορά στις τεχνολογίες που υπάρχουν σε κάθε επίπεδο, ανάλογα με τις απαιτήσεις ασφαλείας που δύνανται να καλύψουν. Εξετάζονται τα πλεονεκτήματα και τα μειονεκτήματά τους, τα οποία τις καθιστούν αποτελεσματικές ή μη στην κάλυψη των συγκεκριμένων απαιτήσεων, με βάση τις ιδιαιτερότητες του περιβάλλοντος των υπηρεσιών. Από τον έλεγχο της καταλληλότητας των τεχνολογιών που υπάρχουν σε κάθε επίπεδο, προκύπτει ένα σύνολο από λύσεις για την κάλυψη των επιμέρους απαιτήσεων ασφάλειας.

Στο έβδομο κεφάλαιο, υπογραμμίζεται η ανάγκη ύπαρξης ενός μοντέλου που θα μπορέσει να ενοποιήσει τις υπάρχουσες λύσεις για την ασφάλεια των υπηρεσιών διαδικτύου. Στόχος ενός τέτοιου μοντέλου πρέπει να είναι ο καθορισμός μιας στρατηγικής για την ασφάλεια, η οποία στρατηγική θα μπορεί να υιοθετηθεί από τους οργανισμούς που αναπτύσσουν υπηρεσίες διαδικτύου και θα υποστηρίζεται τόσο από τις εταιρείες που παρέχουν υποδομή, όσο και από τους οργανισμούς που αναπτύσσουν πρότυπα. Έπειτα, γίνεται η περιγραφή και η κριτική ενός μοντέλου ασφαλείας για τις υπηρεσίες διαδικτύου, το οποίο αποτελεί πρόταση των εταιρειών IBM και Microsoft.

Στο όγδοο κεφάλαιο καταγράφονται και αξιολογούνται, με βάση τις απαιτήσεις ασφάλειας των υπηρεσιών διαδικτύου, οι υπηρεσίες ασφάλειας που παρέχονται στους χορηγούς και στους πελάτες των υπηρεσιών διαδικτύου από τις πλατφόρμες ανάπτυξης των υπηρεσιών. Συγκεκριμένα, παρουσιάζονται και συγκρίνονται οι υπηρεσίες ασφάλειας που παρέχουν οι πλατφόρμες Microsoft .NET και Java 2 Enterprise Edition.



Τέλος, στο ένατο κεφάλαιο παρατίθενται τα συμπεράσματα από όλα τα προηγούμενα κεφάλαια και αναφέρονται τα ανοικτά ζητήματα που προέκυψαν από την ολοκλήρωση της μελέτης.

1.8. Συμβολή της εργασίας.

Με την παρούσα εργασία επιχειρείται η διερεύνηση του προβλήματος της ασφάλειας στις υπηρεσίες διαδικτύου και η αναζήτηση, η περιγραφή και η αξιολόγηση τεχνικών και μεθόδων που μπορούν να αποτελέσουν μέσα προστασίας. Η κύρια συνεισφορά της παρούσας εργασίας αφορά στο Μέρος Β' και συνίσταται:

- Στη διαμόρφωση ενός πλαισίου που περιλαμβάνει τις απαιτήσεις ασφάλειας για την περιγραφή και την αξιολόγηση των μηχανισμών, των τεχνολογιών και των μοντέλων ασφαλείας.
- Στην περιγραφή και ανάλυση ανοικτών ερευνητικών ζητημάτων που προκύπτουν.

Γενικά, η συμβολή της παρούσας εργασίας έγκειται όχι στην πρόταση νέων λύσεων, αλλά στον τρόπο περιγραφής και ανάλυσης των λύσεων που υπάρχουν. Αυτό που κυρίως επιτυγχάνεται είναι η ένταξη των ζητημάτων ασφάλειας, των προτάσεων, των λύσεων και των διαφαινόμενων τάσεων, σε ένα συγκεκριμένο πλαίσιο, έτσι ώστε να μπορούν να αναλυθούν και να αξιολογηθούν. Άλλωστε, η ανάλυση και η αξιολόγηση της παρούσας κατάστασης στον τομέα της ασφάλειας των υπηρεσιών διαδικτύου είναι απαραίτητη προϋπόθεση για τον προσδιορισμό των μελλοντικών ερευνητικών κατευθύνσεων, που είναι ο δεύτερος τομέας συμβολής της εργασίας.

Στον πίνακα 1.2. παρουσιάζεται η συνεισφορά της διπλωματικής ανά κεφάλαιο (για το Β' μέρος).

Κεφάλαιο	Συμβολή
Κεφάλαιο 5	Διερεύνηση των απαιτήσεων ασφαλείας, με βάση τις ιδιαιτερότητες των υπηρεσιών. Πρόταση για την επίλυση συγκρούσεων σε πολιτικές ασφαλείας. Ορισμός επιπέδων ανάλυσης της ασφάλειας.
Κεφάλαιο 6	Περιγραφή και κριτική μηχανισμών ασφαλείας και τεχνολογιών. Δημιουργία ενός πλαισίου ασφάλειας με βάση τις απαιτήσεις.
Κεφάλαιο 7	Περιγραφή και κριτική του μοντέλου ασφαλείας των IBM και Microsoft, με βάση το πλαίσιο των απαιτήσεων.

Κεφάλαιο 8	Περιγραφή και κριτική των υπηρεσιών ασφαλείας των μοντέλων ανάπτυξης .NET και J2EE, με βάση το πλαίσιο των απαιτήσεων.
Κεφάλαιο 9	Περιγραφή ανοικτών ερευνητικών ζητημάτων.

Πίνακας 1.2.: Συμβολή της παρούσας εργασίας

1.9. Ορισμοί θεμελιωδών εννοιών.

Σημείο αναφοράς στην παρούσα εργασία αποτελούν αρκετές θεμελιώδεις έννοιες, όπως η έννοια πληροφορία. Μερικές από τις θεμελιώδεις έννοιες ορίζονται πιο αναλυτικά στα κεφάλαια της εργασίας, όπου και χρησιμοποιούνται, ωστόσο για λόγους ακρίβειας και ευχρηστίας όλοι οι ορισμοί των θεμελιωδών εννοιών δίνονται στον πίνακα 1.3.

Πληροφορία (Information)	Δεδομένα μαζί με την σημασία που τους αποδίδεται. [Γκρίτζαλης Δ., 2001]
Υπολογιστικό Σύστημα (IT System)	Συλλογή υπολογιστικού υλικού, λογισμικού και τηλεπικοινωνιακού εξοπλισμού, που είναι εγκατεστημένη σε μια συγκεκριμένη τοποθεσία, με ένα συγκεκριμένο λειτουργικό περιβάλλον και ανταποκρίνεται σε ένα συγκεκριμένο σύνολο σκοπών. [Γκρίτζαλης Δ., 2001]
Πληροφοριακό σύστημα (Information System)	Σύνολο το οποίο αποτελείται από πέντε στοιχεία: ανθρώπους, λογισμικό, υλικό, διαδικασίες και δεδομένα, τα οποία αλληλεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση πληροφορίας για την υποστήριξη ανθρώπινων δραστηριοτήτων, στα πλαίσια ενός οργανισμού. [Κοκολάκης, 2000]
Εφαρμογή (Application)	Σύνολο αποτελούμενο από πληροφορίες, λογισμικό καθώς και από τις σχετικές διαδικασίες που έχουν σχεδιαστεί για την επίτευξη ενός συγκεκριμένου συνόλου στόχων. [Γκρίτζαλης Δ., 2001]
Υπηρεσία (Service)	Σύνολο λειτουργιών, που παρέχονται σε ένα χρήστη από ένα υπολογιστικό σύστημα. [Γκρίτζαλης Δ., 2001]
Εξουσιοδότηση (Authorization)	Άδεια που παρέχεται από έναν ιδιοκτήτη (π.χ. τον ιδιοκτήτη μιας πληροφορίας ή τον ιδιοκτήτη ενός συστήματος) για ένα συγκεκριμένο σκοπό. [Γκρίτζαλης Δ., 2001]
Ασφάλεια Πληροφοριών (Information Security)	Προστασία της πληροφορίας, στην ολότητά της και των σχετικών με την ασφάλεια ιδιοτήτων. [Κοκολάκης, 2000] Ως τέτοιες ιδιότητες (attributes) θεωρούνται η εμπιστευτικότητα (confidentiality), η διαθεσιμότητα (availability), η εγκυρότητα (validity) και η μη αποποίηση της ευθύνης (non-repudiation).
Εμπιστευτικότητα (Confidentiality)	Αποφυγή αποκάλυψης πληροφοριών χωρίς την άδεια του ιδιοκτήτη. [Γκρίτζαλης Δ., 2001]
Διαθεσιμότητα (Availability)	Αποφυγή προσωρινής ή μόνιμης άρνησης της εξουσιοδοτημένης προσπέλασης Πληροφοριών (Διαθεσιμότητα Πληροφορίας) ή Υπολογιστικών Πόρων (Διαθεσιμότητα Συστήματος) [Γκρίτζαλης Δ., 2001]
Εγκυρότητα (Validity)	Η απόλυτη ακρίβεια και πληρότητα μιας πληροφορίας. Στις περισσότερες περιπτώσεις η εγκυρότητα περιλαμβάνει

	Ακεραιότητα (Integrity) και την Αυθεντικότητα (Authenticity). [Γκρίτζαλης Δ., 2001]
Ακεραιότητα (Integrity)	Αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας. [Γκρίτζαλης Δ., 2001]
Αυθεντικότητα (Authenticity)	Αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια των εξουσιοδοτημένων τροποποιήσεων της πληροφορίας. [Γκρίτζαλης Δ., 2001]
Μη αποποίηση της ευθύνης (Non-repudiation)	Αποφυγή της άρνησης της ευθύνης του αποστολέα (non-repudiation of origin) ή του παραλήπτη (non-repudiation of destination) μιας πληροφορίας. [Γκρίτζαλης Δ., 2001]
Ασφάλεια Υπολογιστικού Συστήματος (IT System Security)	Ο συνδυασμός της Διαθεσιμότητας Συστήματος και της Ασφάλειας Πληροφοριών, καθώς και των παραμέτρων που αποτελούν τμήμα του υπολογιστικού συστήματος. [Γκρίτζαλης Δ., 2001]
Ασφάλεια Πληροφοριακού Συστήματος (IS Security)	Προστασία των συστατικών στοιχείων ενός πληροφοριακού συστήματος (υλικό, λογισμικό, διαδικασίες, άνθρωποι, δεδομένα) και του πληροφοριακού συστήματος στην ολότητά του. [Κοκολάκης, 2000]
Παραβίαση (Violation)	Ένα γεγονός κατά τη διάρκεια του οποίου μια ή περισσότερες από τις σχετικές με την ασφάλεια ιδιότητες έχουν προσβληθεί. [Γκρίτζαλης Δ., 2001]
Απειλή (Threat)	Μια πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσότερων χαρακτηριστικών της ασφάλειας του πληροφοριακού συστήματος. [Γκρίτζαλης Δ., 2001]
Αδυναμία (Vulnerability)	Ένα σημείο ενός πληροφοριακού συστήματος που μπορεί να επιτρέψει να συμβεί μια Παραβίαση. [Γκρίτζαλης Δ., 2001]
Πολιτική (Policy)	Σύνολο έγκυρων και επίσημων δηλωτικών προτάσεων, που προσδιορίζουν το σύνολο των αποδεκτών πιθανών επιλογών, σε μελλοντικές διαδικασίες λήψεως αποφάσεων. [Κοκολάκης, 2000]
Μέσο προστασίας (Safeguard)	Ένα μέτρο σχεδιασμένο με σκοπό να εμποδίσει μια παραβίαση ή να μειώσει τις επιπτώσεις της. [Γκρίτζαλης Δ., 2001]
Μηχανισμός (Mechanism)	Ο τρόπος υλοποίησης ενός μέσου προστασίας. [Γκρίτζαλης Δ., 2001]

Πίνακας 1.3. : Ορισμοί θεμελιωδών εννοιών

1.10. Οντολογικές και Επιστημολογικές Παραδοχές

Σύμφωνα με τον Κοκολάκη κάθε ερευνητική προσπάθεια βασίζεται σε κάποιες θεμελιώδεις παραδοχές, που ορισμένες φορές μπορεί να μην εκφράζονται ρητά. Οι παραδοχές αυτές περιλαμβάνουν, μεταξύ άλλων [Κοκολάκης, 2000]:

- Οντολογικές παραδοχές, που απαντούν στο ερώτημα: «υπάρχει (αντικειμενική) πραγματικότητα, φυσική και κοινωνική, και ποια είναι η φύση (ουσία) της;»
- Επιστημολογικές παραδοχές, που απαντούν στο ερώτημα: «είναι δυνατή η γνώση της (αντικειμενικής) πραγματικότητας και αν ναι με ποιο τρόπο;»

- Μεθοδολογικές παραδοχές που αφορούν στις μεθόδους και τα μέσα που μπορούν να χρησιμοποιηθούν για την απόκτηση γνώσης και την παρέμβαση στην κοινωνική πραγματικότητα.

Το σύνολο των αποδεκτών παραδοχών από μια επιστημονική κοινότητα, ο Kuhn το αποκάλεσε παράδειγμα (paradigm). Στο χώρο των πληροφοριακών συστημάτων, υπάρχουν αρκετά επιστημολογικά παραδείγματα, τα οποία υιοθετούν πολύ διαφορετικές απόψεις σχετικά με τον τρόπο διεξαγωγής και αξιολόγησης μιας έρευνας [Κοκολάκης, 2000]. Στην παρούσα εργασία ωστόσο, η επιλογή του παραδείγματος που θα υιοθετηθεί, θα γίνει μεταξύ των δύο επικρατέστερων. Αυτά είναι ο Λειτουργισμός και η Ερμηνευτική Προσέγγιση:

- Ο Λειτουργισμός [Κοκολάκης, 2000] βασίζεται στην υπόθεση ότι η μελέτη των κοινωνικών φαινομένων μπορεί να γίνει με τον ίδιο ακριβώς τρόπο που μελετούνται και τα φυσικά φαινόμενα. Η οντολογία του λειτουργισμού είναι ο ρεαλισμός. Σύμφωνα με τον ρεαλισμό υπάρχει μία και μοναδική πραγματικότητα, που είναι ανεξάρτητη από την ερμηνεία του ανθρώπινου παρατηρητή. Η επιστημολογία του λειτουργισμού είναι ο θετικισμός. Σύμφωνα με τον θετικισμό, η μελέτη της αντικειμενικής πραγματικότητας είναι δυνατή μέσω της δομημένης παρατήρησης. Οι μεθοδολογίες που έχουν ως βάση τον λειτουργισμό στηρίζονται στις μεθόδους του πειράματος, της μέτρησης και της επαγωγής.
- Η Ερμηνευτική Προσέγγιση [Κοκολάκης, 2000] βασίζεται στην άποψη ότι δεν υπάρχει μία και μοναδική πραγματικότητα, αλλά διαφορετικές προσλήψεις αυτής (φαινομενολογία). Η οντολογία και η επιστημολογία της ερμηνευτικής προσέγγισης στηρίζονται στις αντίστοιχες παραδοχές της φαινομενολογίας. Οι μεθοδολογίες που έχουν αναπτυχθεί με βάση την ερμηνευτική προσέγγιση δίνουν έμφαση στη συμμετοχή των χρηστών, στον προσδιορισμό των προβλημάτων, στη μάθηση και στην καλύτερη κατανόηση ενός συστήματος και του περιβάλλοντος του.

1.10.1. Επιστημολογία και οντολογία της παρούσας εργασίας.

Η παρούσα εργασία καλείται να δώσει απαντήσεις στα ερωτήματα έρευνας που διατυπώθηκαν στην ενότητα 1.5.. Τα ερωτήματα αυτά είναι σαφές ότι δεν επιδέχονται μοναδικό τρόπο αντιμετώπισης. Επίσης, δεν υπάρχει μία και μοναδική ερμηνεία της βιβλιογραφίας που διαπραγματεύεται τα ζητήματα αυτά, για το λόγο ότι η ασφάλεια των πληροφοριακών συστημάτων είναι κοινωνικό φαινόμενο. Η εφαρμογή του ρεαλισμού στη

μελέτη του φαινομένου αυτού θα έπρεπε να στηριχθεί στην υπόθεση ότι η κοινωνική πραγματικότητα μπορεί να μελετηθεί αντικειμενικά, όμως στην συγκεκριμένη περίπτωση η υποκειμενικότητα είναι αναπόφευκτη. Επομένως, το παράδειγμα που θα υιοθετηθεί είναι η ερμηνευτική προσέγγιση. Αυτό σημαίνει ότι η οντολογία και η επιστημολογία της παρούσας εργασίας έχει τις βάσεις της στην φαινομενολογία.

1.11. Μέθοδος έρευνας

Η μέθοδος έρευνας είναι ένας κανονικός και συστηματικός τρόπος για να εξεταστεί, να αναλυθεί και να ερμηνευτεί ένα ερευνητικό πρόβλημα [Κοκολάκης, 2000]. Αυτό σημαίνει ότι μια μέθοδος έρευνας είναι ένα σύνολο από βήματα.

Η μέθοδος της παρούσας εργασίας καθορίζεται από τα βήματα που ακολουθήθηκαν προκειμένου να απαντηθούν οι ερωτήσεις έρευνας που διατυπώθηκαν στην ενότητα 1.5. Τα βήματα αυτά παρουσιάζονται στη συνέχεια.

Ερώτηση 1: Με βάση ποιό πλαίσιο απαιτήσεων ασφάλειας μπορεί να αντιμετωπιστεί το πρόβλημα της ασφάλειας στις Υπηρεσίες Διαδικτύου;

Βήματα:

1. Εξέταση των ορισμών ασφάλειας υπό το πρίσμα των ιδιαιτεροτήτων που παρουσιάζουν οι υπηρεσίες διαδικτύου
2. Επιλογή ενός συνόλου απαιτήσεων ασφάλειας, με βάση κάποια κριτήρια.
3. Δημιουργία πλαισίου απαιτήσεων.

Ερώτηση 2: Ποιές τεχνολογίες μπορούν να αποτελέσουν τη βάση για την αντιμετώπιση του προβλήματος της ασφάλειας στις Υπηρεσίες Διαδικτύου;

Βήματα:

1. Διερεύνηση των μηχανισμών ασφάλειας που μπορούν να καλύψουν επαρκώς τις απαιτήσεις ασφάλειας του πλαισίου.
2. Εξέταση των υφιστάμενων τεχνικών και τεχνολογιών που μπορούν να υποστηρίξουν τους παραπάνω μηχανισμούς.



3. Ανάλυση και αξιολόγηση των τεχνολογιών και των υλοποιήσεων ως προς τις απαιτήσεις του πλαισίου ασφάλειας.
4. Αναζήτηση ανοικτών ερευνητικών ζητημάτων.



ΚΕΦΑΛΑΙΟ 2^ο : ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ

2.1. Εισαγωγή.

Οι υπηρεσίες διαδικτύου είναι ένα νέο παράδειγμα στον τομέα του προγραμματισμού εφαρμογών που επεκτείνει σε σημαντικό βαθμό τις δυνατότητες του διαδικτύου σε ότι αφορά στην παροχή υπηρεσιών.

Στο κεφάλαιο αυτό δίνεται ένας ορισμός για τις υπηρεσίες διαδικτύου, εξηγείται ο λόγος για τον οποίο αναπτύχθηκαν και αναλύονται τα κίνητρα που ωθούν, κυρίως τις επιχειρήσεις, στην υιοθέτησή τους. Επίσης, δίνεται η γενική περιγραφή του μοντέλου τους, διευκρινίζεται το πεδίο εφαρμογής τους και επισημαίνονται οι προκλήσεις που πρέπει να αντιμετωπιστούν για την αποτελεσματική αξιοποίησή τους.

2.2. Τι είναι οι Υπηρεσίες Διαδικτύου.

Ο όρος Υπηρεσίες Διαδικτύου (Υ.Δ.) είναι εξαιρετικά γενικός. Όπως συμβαίνει με κάθε πολλά υποσχόμενη και μη αυστηρά ορισμένη τεχνολογική κατεύθυνση, η εννοιολογική προσέγγιση του όρου θα παραμείνει για αρκετό καιρό αντικείμενο προσωπικών εκτιμήσεων και διαβουλεύσεων, δημιουργώντας ένα πόλο έλξης γύρω από τον όρο αυτό.

Το Stencil Group² επιτυγχάνει να δώσει έναν ορισμό των Υπηρεσιών Διαδικτύου συνδυάζοντας δύο διαφορετικές οπτικές, την τεχνολογική και την επιχειρησιακή:

- Από τεχνολογική άποψη, οι Υπηρεσίες Διαδικτύου είναι μια στοίβα από καινούρια πρότυπα που περιγράφουν μια αρχιτεκτονική εφαρμογών, προσανατολισμένων σε υπηρεσίες, που συνθέτονται από μικρότερες δομικές μονάδες.
- Από επιχειρησιακή άποψη, οι Υπηρεσίες Διαδικτύου αντιπροσωπεύουν ένα επιχειρηματικό μοντέλο, στο οποίο οι ξεχωριστές διεργασίες που αποτελούν κομμάτι μιας διαδικασίας σε μια ηλεκτρονική επιχείρηση κατανέμονται σε κάθε σημείο του δικτύου αξίας.

Έχοντας υπόψη τις δύο αυτές οπτικές, το Stencil Group δίνει στις Υπηρεσίες Διαδικτύου τον παρακάτω ορισμό:

[Ορισμός 1] *Οι Υπηρεσίες Διαδικτύου είναι επαναχρησιμοποιήσιμες μονάδες λογισμικού με χαλαρή σύζευξη³, οι οποίες συγκεντρώνουν ξεχωριστή λειτουργικότητα, είναι κατανεμημένες*

² Το Stencil Group είναι εταιρεία που παρέχει υπηρεσίες υλοποίησης αλλά και συμβουλευτικές υπηρεσίες σε πελάτες που έχουν το Διαδίκτυο ως βάση της επιχείρησης τους.



και επιτρέπουν την πρόσβαση σε προγράμματα, που χρησιμοποιούν πρότυπα των πρωτοκόλλων του Διαδικτύου. [Sleeper et al., 2001]

Από τον παραπάνω ορισμό μπορεί να εξαχθεί η πληροφορία ότι οι Υπηρεσίες Διαδικτύου α) ακολουθούν τη λογική της αντικειμενοστραφούς σχεδίασης, β) επιτρέπουν ευέλικτη επαναδιαμόρφωση (reconfiguration), γ) μπορούν να λειτουργούν ανεξάρτητα, δ) παράγουν συγκεκριμένη έξοδο για κάθε είσοδο δεδομένων, ε) δεν είναι σχεδιασμένες για άμεση αλληλεπίδραση με το χρήστη (δεν διαθέτουν γραφικό περιβάλλον), στ) χρησιμοποιούν δικτυακά πρωτόκολλα μεταφοράς.

Ένας ακόμα ορισμός στις Υπηρεσίες Διαδικτύου δίνεται από τους ερευνητές του κέντρου ερευνών Watson της IBM στις Η.Π.Α.

[Ορισμός 2] *Oι Υπηρεσίες Διαδικτύου είναι εφαρμογές σε περιβάλλον δικτύου που μπορούν και αλληλεπιδρούν, μέσω καλά ορισμένων διεπαφών, χρησιμοποιώντας πρότυπα των πρωτοκόλλων του Διαδικτύου, σχεδιασμένα για την επικοινωνία εφαρμογής με εφαρμογή και περιγράφονται με χρήση μιας πρότυπης γλώσσας περιγραφής των διαδικασιών.*

[Curbela et al., 2001]

Ο παραπάνω ορισμός συμπληρώνεται από τους ερευνητές της IBM με ένα σύνολο από ιδιότητες, που αναμένεται να εμφανίζει μια υπηρεσία διαδικτύου. Συγκεκριμένα μια Υ.Δ. πρέπει:

- να εμφανίζει χαρακτηριστικά «γκρίζου κουτιού».
- να αποτελείται από μονάδες με χαλαρή σύζευξη.
- να προσφέρει ευέλικτο τρόπο ενοποίησης των εφαρμογών (να ανιχνεύει δηλαδή καταστάσεις στις οποίες υποστηρίζεται ένα περισσότερο αποτελεσματικό πρωτόκολλο).
- να χρησιμοποιεί μηνύματα αντί για API⁴ διεπαφές.

Η ομοιότητα μεταξύ των ορισμών [1] και [2] είναι εμφανής. Ο λόγος είναι ότι και οι δύο ορισμοί είναι προσανατολισμένοι στην έννοια «λογισμικό». Δεν είναι τυχαίο το γεγονός ότι δανείζονται όρους από την Τεχνολογία Λογισμικού. Εντούτοις, οι Υ.Δ. είναι πρώτα από όλα υπηρεσίες και θα ήταν ιδιαίτερα χρήσιμο να υπάρχει ένας ορισμός που να είναι προσανατολισμένος στην έννοια «υπηρεσία». Προς αυτή την κατεύθυνση κινείται περισσότερο ο ορισμός των Υπηρεσιών Διαδικτύου, που δίνεται από τον Graham Glass:

[Ορισμός 3] *Oι Υπηρεσίες Διαδικτύου είναι συλλογή από λειτουργίες, που αποτελούν μια ενιαία οντότητα και βρίσκονται δημοσιευμένες στο Διαδίκτυο, επιτρέποντας τη χρησιμοποίησή τους από άλλα προγράμματα. Οι Υπηρεσίες Διαδικτύου αποτελούν δομικές μονάδες για τη*

³ σελ. 109, Τεχνολογία Λογισμικού, Τόμος Α, Εμμ. Γιακουμάκης, 1994.

δημιουργία ανοικτών κατανεμημένων συστημάτων και επιτρέπουν σε μεμονωμένα άτομα ή οργανισμούς να καταστήσουν ευρέως διαθέσιμα τα ψηφιακά αγαθά που κατέχουν, με τρόπο γρήγορο και οικονομικό.

[Glass, 2000]

Ο ορισμός του Glass δίνει μια περισσότερο ξεκάθαρη άποψη της έννοιας Υπηρεσία Διαδικτύου σε κάποιον που δεν έχει γνώση της Τεχνολογίας Λογισμικού. Ωστόσο, δεν δίνει καμία πληροφορία για τον τρόπο με τον οποίο λειτουργούν οι Υπηρεσίες Διαδικτύου και την καινοτομία που εισάγουν. Ο ορισμός που ακολουθεί έχει ως στόχο να συνθέσει όλους τους παραπάνω ορισμούς σε έναν τελικό. Στο εξής, κάθε αναφορά σε Υπηρεσίες Διαδικτύου στο πλαίσιο της παρούσας εργασίας, θα έχει ως βάση τον ορισμό αυτό:

[Ορισμός 4] *Οι Υπηρεσίες Διαδικτύου είναι ανεξάρτητες, τμηματοποιημένες⁵ εφαρμογές με διεπαφές βασισμένες σε ανοικτά πρότυπα του Διαδικτύου. Είναι χαλαρά συνεζευγμένες και επικοινωνούν μεταξύ τους μέσω του Διαδικτύου χρησιμοποιώντας τεχνολογίες βασισμένες σε πρότυπα. Οι Υπηρεσίες Διαδικτύου προσφέρουν σε μια επιχείρηση έναν αυτοματοποιημένο τρόπο επικοινωνίας, μέσω ανταλλαγής μηνυμάτων, με τις εφαρμογές πελατών, συνεταιρών, προμηθευτών, ανεξάρτητα από το υλικό, το λειτουργικό σύστημα και το προγραμματιστικό περιβάλλον που διαθέτουν. Με την ανάπτυξη των Υπηρεσιών Διαδικτύου γίνεται πραγματικότητα η δημιουργία ενός περιβάλλοντος, στο οποίο οι εταιρείες μπορούν να τοποθετούν τις τρέχουσες και μελλοντικές εφαρμογές τους, με τη μορφή υπηρεσιών που μπορούν εύκολα και γρήγορα να εντοπιστούν και να καταναλωθούν.*

2.3. Πώς γεννήθηκε η ανάγκη για ανάπτυξη των Υπηρεσιών Διαδικτύου.

Το πραγματικό γεγονός που κρύβεται πίσω από την ανάγκη για ανάπτυξη των Υπηρεσιών Διαδικτύου είναι η έλευση μιας νέας εποχής για τον κατανεμημένο προγραμματισμό και μοιραία η πάροδος της προηγούμενης.

Αυτό που κατόρθωσε να πετύχει το παράδειγμα του κατανεμημένου προγραμματισμού τα τελευταία χρόνια ήταν να προσφέρει τη δυνατότητα σε διαφορετικά υπολογιστικά περιβάλλοντα να μοιράζονται από κοινού πληροφορία, μέσω του Διαδικτύου. Το ζητούμενο της νέας εποχής είναι η δυνατότητα τα διαφορετικά υπολογιστικά περιβάλλοντα να μοιράζονται από κοινού και διαδικασίες.

⁴ Application Programming Interface

⁵ σελ. 107, Τεχνολογία Λογισμικού, Τόμος Α, Εμμ. Γιακουμάκης, 1994.

Ανέκαθεν, η ενοποίηση εφαρμογών, που είχαν αναπτυχθεί ξεχωριστά από διαφορετικούς οργανισμούς, ήταν πολύ δύσκολη εξ' αιτίας της ετερογένειας που χαρακτήριζε και χαρακτηρίζει τις γλώσσες προγραμματισμού και τις υπολογιστικές πλατφόρμες. Η ανάπτυξη της three-tier⁶ αρχιτεκτονικής ξεκίνησε σαν μια προσπάθεια να δοθεί κάποια λύση στο συγκεκριμένο πρόβλημα. Οι τεχνολογίες οι οποίες ξεχώρισαν ήταν οι CORBA⁷, DCOM⁸ και RMI⁹, οι οποίες εξακολουθούν να είναι δημοφιλείς. Όλες αυτές ανήκουν στην κατηγορία του ενδιάμεσου λογισμικού (middleware), υποστηρίζουν τη διαλειτουργικότητα ανάμεσα σε διαφορετικές γλώσσες προγραμματισμού και σε ετερογενείς πλατφόρμες, και λειτουργούν με παρόμοιο τρόπο. Εντούτοις, η τυπική χρήση τους εστιάζεται στο περιβάλλον εσωτερικών δικτύων (Intranets). Στο περιβάλλον του Διαδικτύου, υπάρχει ετερογένεια στον τομέα middleware, αφού καμία από τις παραπάνω τεχνολογίες δεν κατάφερε να επικρατήσει. Συνεπώς, τόσο από τη μεριά του πελάτη, όσο και από τη μεριά του εξυπηρετητή, δεν μπορεί να είναι γνωστός ο τύπος του middleware που χρησιμοποιείται.

Το παραπάνω γεγονός αποτελεί τη βασική αιτία που αποφασίστηκε από τους ερευνητές να εγκαταλειφθούν οι υπάρχουσες τεχνολογίες και να επινοηθούν νέες που θα εξυπηρετήσουν τις ανάγκες της νέας εποχής [Günzer, 2002]. Το μοντέλο των Υπηρεσιών Διαδικτύου αναμένεται να επικρατήσει στο χώρο του κατανεμημένου προγραμματισμού, αφού διαθέτει όλα εκείνα τα χαρακτηριστικά που μπορούν να εξασφαλίσουν την επιτυχία. Οι βασικές διαφορές που εμφανίζει συγκρινόμενο με τα προηγούμενα μοντέλα λογισμικού στον χώρο του κατανεμημένου προγραμματισμού είναι ότι α) είναι μη αυστηρά ορισμένο, β) χαρακτηρίζεται από χαλαρή σύζευξη μονάδων και γ) μπορεί να υλοποιηθεί με χρήση διαδεδομένων τεχνολογιών¹⁰, οι οποίες θα αναφερθούν στο επόμενο κεφάλαιο.

2.4. Ποια είναι τα κίνητρα για την ανάπτυξη Υπηρεσιών Διαδικτύου.

Πέρα από τη βασική ανάγκη που αποτελεί την κύρια ώθηση για την ανάπτυξη των Υπηρεσιών Διαδικτύου, τα κίνητρα για την ανάπτυξη τέτοιου είδους υπηρεσιών είναι πολλά. Οι Υπηρεσίες Διαδικτύου:

- Μειώνουν το κόστος πρόσβασης σε δεδομένα που βρίσκονται σε ετερογενή συστήματα.

⁶ Αρχιτεκτονική που προσθέτει ένα middle tier server στο κλασσικό μοντέλο client-server.

⁷ Common Object Request Broker Architecture

⁸ Distributed Component Object Model

⁹ Remote Method Invocation

¹⁰ όπως HTTP και XML.

- Περιορίζουν το χρόνο εισόδου στην αγορά στις επιχειρήσεις, μειώνοντας το χρόνο που απαιτείται για την ανάπτυξη και τον έλεγχο των εφαρμογών.
- Επιτυγχάνουν την καλύτερη δυνατή αξιοποίηση των επενδύσεων μιας επιχείρησης σε υποδομές Internet.
- Επιτρέπουν την ενσωμάτωση στις εφαρμογές της επιχείρησης της λειτουργικότητας των ετερογενών πλατφόρμων ανάπτυξης.¹¹
- Επιτρέπουν τη σύνδεση παλαιών και νέων συστημάτων σε μια επιχείρηση για τις ανάγκες μιας εφαρμογής.
- Επιτυγχάνουν τη συνεχή προσαρμογή των εφαρμογών στις νέες διαδικασίες της επιχείρησης.
- Επιτρέπουν την αντικατάσταση ή τη μετατροπή ενός αγαθού ανάλογα με τις ανάγκες της επιχείρησης¹², χωρίς να επηρεαστούν από αυτό οι πελάτες ή οι διαδικασίες που βρίσκονται σε εξάρτηση από αυτό.
- Διευκολύνουν τις επιχειρήσεις να ενσωματώσουν και να επαναχρησιμοποιήσουν λογισμικό που έχει ήδη κατασκευαστεί από τους ίδιους ή και από άλλους. Αυτό σημαίνει για τις επιχειρήσεις εξοικονόμηση πόρων, αλλά και χρόνου.
- Λειτουργούν τόσο στο περιβάλλον του Διαδικτύου, με το οποίο συνδέεται η πλειοψηφία των επιχειρήσεων, όσο και στο περιβάλλον ενός εσωτερικού δικτύου (Intranet), και γενικά σε κάθε περιβάλλον δικτύου, που χρησιμοποιεί τα πρωτόκολλα του Διαδικτύου.
- Έχουν την υποστήριξη των σημαντικότερων προμηθευτών στον τομέα της τεχνολογίας, συμπεριλαμβανομένης της IBM, της Sun, της Microsoft, της BEA Systems, της Hewlett Packard και της Oracle.
- Δεν καθιστούν ξεπερασμένες τις προηγούμενες τεχνολογίες ενοποίησης εφαρμογών. Απλά καθιστούν δυνατή την ενοποίηση εφαρμογών σε περιπτώσεις που με άλλο τρόπο θα ήταν εξαιρετικά σύνθετη να συμβεί.
- Επιτρέπουν στην ομάδα ανάπτυξης των εφαρμογών να ανταποκρίνεται γρηγορότερα στις ανάγκες τις επιχείρησης.

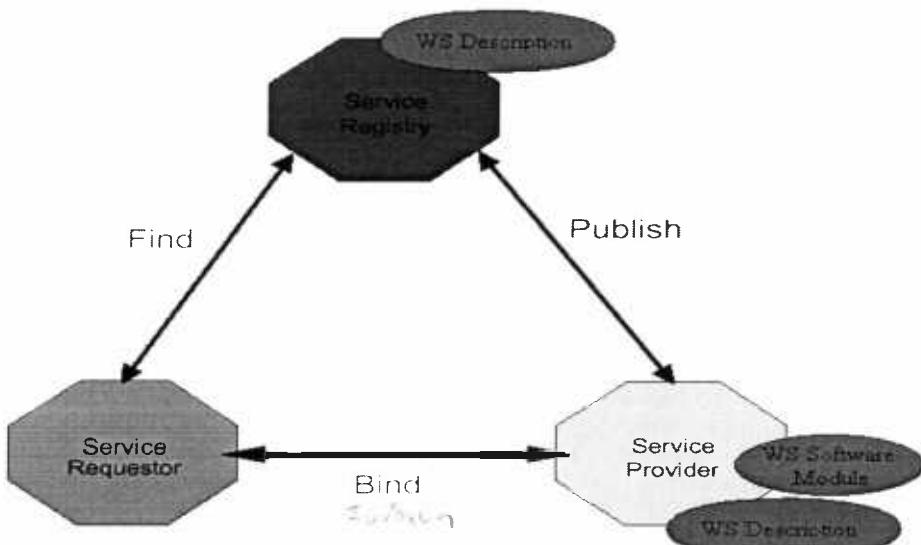
¹¹ όπως .NET, CORBA, J2EE.

¹² για παράδειγμα μια επιχείρηση μπορεί να αποφασίσει πως την συμφέρει να κάνει outsource κάποιο συγκεκριμένο αγαθό παρά να το παράγει η ίδια.

2.5. Περιγραφή του μοντέλου των Υπηρεσιών Διαδικτύου.

2.5.1. Αρχιτεκτονική του μοντέλου.

Η αρχιτεκτονική των Υπηρεσιών Διαδικτύου [Kreger, 2001] είναι βασισμένη στην αλληλεπίδραση μεταξύ τριών οντοτήτων: α) του χορηγού των υπηρεσιών (Service Provider), β) του καταλόγου υπηρεσιών (Service Registry) και γ) του πελάτη των υπηρεσιών (Service Requestor). Οι αλληλεπιδράσεις περιλαμβάνουν τις διαδικασίες δημοσίευσης, εύρεσης και δέσμευσης μιας υπηρεσίας. Τα συνθετικά στοιχεία μιας Υπηρεσίας Διαδικτύου¹³, είναι η υπηρεσία (ενότητα λογισμικού) και η περιγραφή της, και είναι τα μέσα με τα οποία αλληλεπιδρούν ουσιαστικά μεταξύ τους οι οντότητες. Σε ένα τυπικό σενάριο, ο χορηγός της υπηρεσίας που είναι ιδιοκτήτης της εφαρμογής μιας Υπηρεσίας Διαδικτύου, διαμορφώνει μια περιγραφή για την υπηρεσία και τη δημοσιεύει στον κατάλογο υπηρεσιών ή σε κάποιο πελάτη που έχει εκδηλώσει ενδιαφέρον. Ο πελάτης χρησιμοποιεί μια διαδικασία αναζήτησης, για να ανακτήσει την περιγραφή της υπηρεσίας τοπικά ή από τον κατάλογο υπηρεσιών. Στη συνέχεια χρησιμοποιεί την περιγραφή της υπηρεσίας, για να συνδεθεί με την υπηρεσία και να χρησιμοποιήσει την εφαρμογή. Στο σχήμα 2.1 δίνεται μια περισσότερο ξεκάθαρη αντίληψη των σχέσεων μεταξύ οντοτήτων, διαδικασιών και συστατικών μιας υπηρεσίας.



Σχήμα 2.1.: Το μοντέλο των Υπηρεσιών Διαδικτύου. [Kreger, 2001]

2.5.2. Περιγραφή των οντότητων του μοντέλου.

Στην αρχιτεκτονική του σχήματος 2.1. οι τρεις οντότητες που παρουσιάζονται είναι:

- α) Ο χορηγός υπηρεσιών (Service Provider).

Από επιχειρησιακή άποψη, χορηγός είναι ο ιδιοκτήτης της υπηρεσίας. Από άποψη αρχιτεκτονικής σχεδίασης, χορηγός της υπηρεσίας είναι η πλατφόρμα που παρέχει την πρόσβαση στην υπηρεσία.

- β) Ο πελάτης (Service Requestor).

Από επιχειρησιακή άποψη, πελάτης είναι η επιχείρηση που χρησιμοποιεί την υπηρεσία, για να εκτελέσει συγκεκριμένες λειτουργίες που ικανοποιούν ανάγκες της. Από άποψη αρχιτεκτονικής σχεδίασης, πελάτης είναι η εφαρμογή που κάνει αναζητήσεις και καλεί μια υπηρεσία ή ξεκινά μια αλληλεπίδραση με αυτήν. Το ρόλο του πελάτη μπορεί να παίξει ένας “browser” που κατευθύνεται από κάποιο χρήστη ή κάποιο πρόγραμμα που δε διαθέτει διεπαφή για το χρήστη, όπως για παράδειγμα μια άλλη υπηρεσία Διαδικτύου.

- γ) Ο κατάλογος Υπηρεσιών.

Ο κατάλογος υπηρεσιών είναι ένα ευρετήριο περιγραφών των υπηρεσιών, στο οποίο οι χορηγοί των υπηρεσιών μπορούν να δημοσιεύουν τις περιγραφές των υπηρεσιών τους. Οι πελάτες εντοπίζουν την περιγραφή μιας υπηρεσίας και λαμβάνουν την απαραίτητη πληροφορία (binding information) για να δεσμεύσουν (συνδεθούν με) την υπηρεσία. Η δέσμευση μπορεί να γίνει είτε στατικά, είτε δυναμικά. Στην πρώτη περίπτωση, ο ρόλος του καταλόγου υπηρεσιών είναι προαιρετικός, αφού ο χορηγός μιας υπηρεσίας μπορεί να στείλει την περιγραφή της άμεσα στους πελάτες που αιτούνται την υπηρεσία. Επιπλέον, οι πελάτες μπορούν να λάβουν μια περιγραφή υπηρεσιών από άλλες πηγές όπως τοπικά αρχεία, FTP sites, Web sites, ADS¹⁴, DISCO¹⁵ κτλ.

2.5.3. Περιγραφή των διαδικασιών του μοντέλου.

Οι διαδικασίες μέσω των οποίων αλληλεπιδρούν οι οντότητες του μοντέλου των Υπηρεσιών Διαδικτύου (σχήμα 2.1.) είναι:

- α) Δημοσίευση υπηρεσίας.

¹³ με την έννοια της εφαρμογής, όπως δόθηκε στην παράγραφο 1.2. [βλέπε Ορισμό 4]

¹⁴ Advertisement and Discovery of Services

¹⁵ Discovery of Web Services

Για να είναι δυνατή η πρόσβαση σε μια περιγραφή υπηρεσιών πρέπει να δημοσιευθεί έτσι ώστε ο δυνητικός πελάτης της υπηρεσίας να μπορεί να την εντοπίσει. Το πού πρέπει να δημοσιευτεί μια περιγραφή υπηρεσίας ποικίλει, ανάλογα με τις απαιτήσεις της εφαρμογής.

β) Εύρεση υπηρεσίας.

Στη διαδικασία εύρεσης, ο πελάτης που επιθυμεί να γίνει δέκτης μιας υπηρεσίας είτε ανακτά μια περιγραφή υπηρεσιών άμεσα, είτε εκτελεί κάποιο ερώτημα στον κατάλογο υπηρεσιών για τον τύπο υπηρεσίας που αναζητά. Η διαδικασία μπορεί να λάβει χώρα σε δύο διαφορετικές φάσεις του κύκλου ζωής της εφαρμογής του πελάτη. Μπορεί να γίνει α) κατά τη σχεδίαση της εφαρμογής, προκειμένου να ανακτηθεί η περιγραφή της διεπαφής της υπηρεσίας και να χρησιμοποιηθεί κατά την ανάπτυξη του προγράμματος, ή β) κατά το χρόνο εκτέλεσης της εφαρμογής, προκειμένου να ανακτηθούν από το αρχείο περιγραφών οι πληροφορίες που αφορούν στον εντοπισμό της υπηρεσίας και τις παραμέτρους της σύνδεσης και να κληθεί η υπηρεσία.

γ) Δέσμευση (σύνδεση).

Στη διαδικασία της δέσμευσης ο πελάτης καλεί την υπηρεσία ή ξεκινάει μια αλληλεπίδραση με την υπηρεσία, εκτελώντας την εφαρμογή του¹⁶ και χρησιμοποιώντας τις πληροφορίες σύνδεσης που δίνονται από την περιγραφή της υπηρεσίας. (Οι πληροφορίες σύνδεσης είναι απαραίτητες προκειμένου να την εντοπίσει, να την καλέσει, και να αλληλεπιδράσει με αυτή).

2.5.4. Περιγραφή των στοιχείων που συνθέτουν μια Υπηρεσία Διαδικτύου.

Τα στοιχεία που συνθέτουν μια Υπηρεσία Διαδικτύου, είναι η υπηρεσία και η περιγραφή της:

α) Υπηρεσία.

Ο όρος υπηρεσία χρησιμοποιείται για να περιγράψει το κομμάτι της υλοποίησης (κώδικας). Υπηρεσία είναι μια ενότητα λογισμικού που έχει αναπτυχθεί σε κάποια πλατφόρμα, την οποία διαθέτει ο χορηγός της υπηρεσίας και η οποία επιτρέπει την πρόσβαση στην υπηρεσία μέσω του Διαδικτύου. Η υπηρεσία υπάρχει για να καλείται ή να αλληλεπιδρά με τον πελάτη της Υπηρεσίας Διαδικτύου. Μπορεί να λειτουργήσει και ως πελάτης, όταν χρησιμοποιεί στην υλοποίηση της άλλες Υπηρεσίες Διαδικτύου.

β) Περιγραφή της υπηρεσίας.

¹⁶ δηλαδή κατά την φάση εκτέλεσης



Η περιγραφή μιας υπηρεσίας περιέχει τις λεπτομέρειες σε ότι αφορά τη διεπαφή και τον τρόπο υλοποίησης μιας υπηρεσίας. Περιλαμβάνει τύπους δεδομένων (data types), λειτουργίες (operations) και πληροφορίες για τη σύνδεση (binding information) και τη θέση της υπηρεσίας στο δίκτυο (network location). Η περιγραφή μιας υπηρεσίας μπορεί να αποσταλεί άμεσα στον πελάτη ή να δημοσιοποιηθεί στον κατάλογο υπηρεσιών. Τέλος, οι περιγραφές των υπηρεσιών μπορούν να υποστηρίζουν την κατηγοριοποίηση των υπηρεσιών με χρήση μέτα-δεδομένων (meta-data), που θα διευκολύνουν την ανακάλυψη και τη χρησιμοποίηση των υπηρεσιών από τους πελάτες.

2.5.5. Κύκλος ζωής του μοντέλου ανάπτυξης Υπηρεσιών Διαδικτύου.

Ο κύκλος ζωής του μοντέλου ανάπτυξης Υπηρεσιών Διαδικτύου περιλαμβάνει απαιτήσεις που αφορούν στη σχεδίαση, στην ανάπτυξη και στο χρόνο εκτέλεσης και σχετίζονται με κάθε μια από τις οντότητες που αναλύθηκαν προηγουμένως. Με άλλα λόγια, κάθε οντότητα έχει συγκεκριμένες απαιτήσεις σε κάθε φάση του κύκλου ζωής της ανάπτυξης μιας Υπηρεσίας Διαδικτύου. Οι τέσσερις φάσεις του κύκλου ζωής του μοντέλου ανάπτυξης Υπηρεσιών Διαδικτύου [Kreger, 2001] είναι:

1. Κατασκευή

Η φάση της κατασκευής περιλαμβάνει την ανάπτυξη και τους δοκιμαστικούς ελέγχους της υπηρεσίας, τον καθορισμό της περιγραφής των διεπαφών της υπηρεσίας και τον καθορισμό του τρόπου υλοποίησης της υπηρεσίας. Η υλοποίηση Υπηρεσιών Διαδικτύου μπορεί να γίνει με τρεις τρόπους. Ο πρώτος τρόπος είναι η δημιουργία νέων υπηρεσιών από την αρχή. Ο δεύτερος είναι ο μετασχηματισμός παλαιότερων εφαρμογών σε υπηρεσίες Διαδικτύου και ο τελευταίος η σύνθεση νέων υπηρεσιών Διαδικτύου από άλλες εφαρμογές ή και υπηρεσίες Διαδικτύου.

2. Επέκταση

Στη φάση της επέκτασης η υπηρεσία γίνεται διαθέσιμη για πιο αποτελεσματική χρήση. Η φάση αυτή περιλαμβάνει τη δημοσίευση της περιγραφής της υπηρεσίας σε ένα πελάτη ή σε ένα κατάλογο υπηρεσιών και την ανάπτυξη εκτελέσιμων αρχείων της υπηρεσίας για το νέο περιβάλλον εκτέλεσης (Web application server).

3. Εκτέλεση



Κατά τη διάρκεια της φάσης εκτέλεσης, η Υπηρεσία Διαδικτύου είναι διαθέσιμη μέσω του διαδικτύου. Υποστηρίζει πλήρη λειτουργικότητα και ο πελάτης είναι σε θέση να εκτελέσει τις διαδικασίες της εύρεσης και της σύνδεσης με την υπηρεσία.

4. Διαχείριση

Η φάση αυτή αφορά στη διαχείριση των εφαρμογών των Υπηρεσιών Διαδικτύου. Η ασφάλεια, η διαθεσιμότητα, η απόδοση, η ποιότητα της υπηρεσίας και η ικανοποίηση των επιχειρηματικών στόχων είναι παράμετροι που πρέπει να εξετάζονται συνεχώς.

2.6. Πεδίο εφαρμογής του μοντέλου Υπηρεσιών Διαδικτύου.

Το πεδίο εφαρμογής των Υπηρεσιών Διαδικτύου είναι κυρίως το περιβάλλον των επιχειρήσεων, χωρίς αυτό να σημαίνει ότι οι υπηρεσίες αυτές δεν μπορούν να χρησιμοποιηθούν για τις ανάγκες ενός μεμονωμένου χρήστη. Το σημαντικό είναι να μπορεί να γίνει διάκριση των περιπτώσεων στις οποίες η χρησιμοποίηση των Υπηρεσιών Διαδικτύου συμφέρει και των περιπτώσεων εκείνων που ισχύει το ακριβώς αντίθετο. Παρακάτω παρατίθενται περιπτώσεις στις οποίες η χρήση των Υπηρεσιών Διαδικτύου ενδείκνυται, καθώς και περιπτώσεις στις οποίες η χρήση της τεχνολογίας αυτής δεν έχει τίποτα να προσφέρει.

2.6.1. Σε ποιες περιπτώσεις είναι χρήσιμες οι Υπηρεσίες Διαδικτύου.

Υπάρχουν τέσσερις αρκετά συνηθισμένες περιπτώσεις στις οποίες εμφανίζει σημαντικά πλεονεκτήματα η χρήση των Υπηρεσιών Διαδικτύου [Shohoud, 2003]. Αυτές είναι οι εξής:

α) Επικοινωνία εφαρμογών μέσα από firewall.

Κατά την ανάπτυξη μια κατανεμημένης εφαρμογής που υποστηρίζει εκατομμύρια ή χιλιάδες χρηστών που βρίσκονται διασκορπισμένοι σε πολλές περιοχές, υπάρχει πάντα το πρόβλημα της επικοινωνίας μεταξύ πελάτη και εξυπηρετητή εξ' αιτίας της παρουσίας firewall ή και πληρεξούσιων (proxy) εξυπηρετητών. Σε μια τέτοια περίπτωση η χρησιμοποίηση της τεχνολογίας DCOM είναι αρκετά δύσκολη, και η ανάπτυξη εφαρμογών πελάτη με τα χαρακτηριστικά ενός browser που θα καλεί ASP¹⁷ σελίδες είναι μια λύση με πολλά μειονεκτήματα στη διαχείριση. Οι Υπηρεσίες Διαδικτύου θεωρούνται σήμερα η καταλληλότερη λύση.

¹⁷ Active Server Pages



β) Ενοποίηση ετερογενών εφαρμογών.

Συχνά είναι απαραίτητη η ανταλλαγή πληροφοριών μεταξύ μιας εφαρμογής που τρέχει σε έναν τυπικό υπολογιστή και μιας άλλης εφαρμογής που τρέχει για παράδειγμα σε ένα mainframe υπολογιστή. Για να είναι δυνατό κάτι τέτοιο, οι εφαρμογές πρέπει να ενοποιηθούν. Το ίδιο απαιτείται και για εφαρμογές που εκτελούνται σε ίδιες πλατφόρμες, αλλά προέρχονται από διαφορετικούς προμηθευτές. Με τη διάθεση μέρους της λειτουργικότητας των εφαρμογών αυτών με τη μορφή Υπηρεσιών Διαδικτύου, παρέχεται ένας μηχανισμός, μέσω του οποίου άλλες εφαρμογές μπορούν να τις χρησιμοποιήσουν.

γ) Ενοποίηση των λειτουργιών μεταξύ των επιχειρήσεων.

Με την ανάπτυξη των Υπηρεσιών Διαδικτύου, μια επιχείρηση μπορεί να διαθέσει, με τη μορφή υπηρεσιών, κρίσιμες επιχειρησιακές της λειτουργίες σε εξουσιοδοτημένους πελάτες ή προμηθευτές. Αυτό, βέβαια δεν αποτελεί κάποια καινούρια δυνατότητα, αφού κάτι τέτοιο υποστηρίζεται και μέσω της ανταλλαγής EDI¹⁸ μηνυμάτων μεταξύ των επιχειρήσεων. Τα πλεονεκτήματα των Υπηρεσιών Διαδικτύου είναι η ευκολότερη υλοποίησή τους και η δυνατότητα λειτουργίας τους στο περιβάλλον του Διαδικτύου, που είναι ευρέως διαθέσιμο στις επιχειρήσεις σε όλο τον κόσμο, με σχετικά χαμηλό κόστος.

δ) Επαναχρησιμοποίηση λογισμικού.

Η επαναχρησιμοποίηση του λογισμικού αποτελεί δυνατότητα που υπήρχε μέχρι σήμερα με τον εξής περιορισμό. Ήταν εύκολο να επαναχρησιμοποιηθεί ο ίδιος κώδικας, δεν ήταν όμως δυνατό να γίνει το ίδιο και με τα δεδομένα που κρύβονταν πίσω από αυτόν. Οι Υπηρεσίες Διαδικτύου επιτρέπουν την επαναχρησιμοποίηση του κώδικα μαζί με τα δεδομένα που χρειάζεται.

2.6.2. Σε ποιες περιπτώσεις είναι ασύμφορη η χρησιμοποίηση Υπηρεσιών Διαδικτύου.

Από την ανάλυση των παραπάνω περιπτώσεων γίνεται κατανοητό ότι οι Υπηρεσίες Διαδικτύου παρουσιάζουν πολλά πλεονεκτήματα, κυρίως σε περιπτώσεις που υπάρχει ανάγκη για διαλειτουργικότητα και απομακρύσμένη εκτέλεση λειτουργιών. Οπωσδήποτε, όμως, υπάρχουν πολλές περιπτώσεις, στις οποίες οι Υπηρεσίες Διαδικτύου δεν έχουν να προσφέρουν κάποια ωφέλεια. Δυο τυπικά παραδείγματα περιπτώσεων, που η χρήση των Υπηρεσιών Διαδικτύου είναι λανθασμένη επιλογή [Shohoud, 2003], είναι τα παρακάτω:

α) Επικοινωνία εφαρμογών που εκτελούνται στην ίδια μηχανή.

¹⁸ Electronic Data Interchange



Στην περίπτωση αυτή, είναι τις περισσότερες φορές προτιμότερο να χρησιμοποιηθεί ένα απλό API, παρά μια Υπηρεσία Διαδικτύου. Η χρήση της τεχνολογίας COM¹⁹ για παράδειγμα είναι πολύ αποτελεσματική σε αυτή την περίπτωση, γιατί είναι λύση γρήγορη και σχετικά φθηνή.

β) Επικοινωνία ομογενών εφαρμογών που εκτελούνται στο περιβάλλον ενός τοπικού δικτύου.

Στην περίπτωση αυτή η καλύτερη λύση είναι να χρησιμοποιηθεί για την επικοινωνία των εφαρμογών η τεχνολογία DCOM. (Ακόμα και στην περίπτωση .NET εφαρμογών²⁰ που πρέπει να επικοινωνήσουν σε ένα περιβάλλον τοπικού δικτύου, μπορεί να χρησιμοποιηθεί η τεχνολογία .NET remoting πάνω από πρωτόκολλο TCP, χωρίς οι εφαρμογές να χρησιμοποιούνται ως Υπηρεσίες Διαδικτύου).

2.7. Το παρόν και το μέλλον των Υπηρεσιών Διαδικτύου.

Η στάση των επιχειρήσεων σήμερα, απέναντι στην τεχνολογία των Υπηρεσιών Διαδικτύου απεικονίζεται πλήρως στην έρευνα²¹ που πραγματοποίησε σε πλήθος 471 διευθυντών πληροφορικής, η εταιρεία Jupiter Media Metrix, η οποία εδρεύει στην πόλη της Νέας Υόρκης. Από απαντήσεις σε ερωτήματα που αφορούσαν στο έτος 2002, προέκυψε ότι: α) ένα 60% των επιχειρήσεων επρόκειτο να χρησιμοποιήσει μέσα στο έτος αυτό τις Υπηρεσίες Διαδικτύου για την ενοποίηση των εφαρμογών εντός του δικτύου τους, β) ένα 53% επρόκειτο να τις χρησιμοποιήσει για τη σύνδεση των εφαρμογών τους με εφαρμογές γνωστών πελατών, προμηθευτών και συνεργατών, γ) ένα 16% επρόκειτο να τις χρησιμοποιήσει για δυναμική αναζήτηση και αλληλεπίδραση με εφαρμογές τρίτων, δ) ένα 20% για να προσφέρει υπηρεσίες σε τρίτους και τέλος ε) ένα 23% δεν επρόκειτο να αναπτύξει την τεχνολογία μέσα στο 2002.

Με άλλα λόγια, παρατηρείται μια σημαντική τάση των επιχειρήσεων να χρησιμοποιήσουν τις Υπηρεσίες Διαδικτύου. Αυτό όμως που έχει μεγαλύτερη σημασία είναι με ποιο τρόπο αποφασίζουν να αξιοποιήσουν την νέα τεχνολογία οι επιχειρήσεις που έσπευσαν να την ακολουθήσουν. Η έρευνα που έκανε ο Joe Clabby κατέληξε στο συμπέρασμα ότι υπάρχουν εννέα τρόποι, με τους οποίους αξιοποιούν σήμερα οι επιχειρήσεις τις Υπηρεσίες Διαδικτύου. Αυτοί είναι οι εξής [Clabby, 2002]:

1) Για τη γρήγορη εξάπλωση σε νέες αγορές.

¹⁹ Component Object Model

²⁰ Θα αναφερθεί σε επόμενο κεφάλαιο

²¹ τα στοιχεία αυτής της έρευνα υπάρχουν στο site της εταιρείας στην εξής διεύθυνση : http://www.jmm.com/xp/jmm/press/2001/pr_083001.xml

- 2) Για τη δημιουργία νέων οργανωσιακών ικανοτήτων.
- 3) Για τη μείωση του κόστους ανάπτυξης εφαρμογών.
- 4) Για τη δημιουργία ανταγωνιστικού πλεονεκτήματος ή την αποφυγή του ανταγωνισμού.
- 5) Για τη δημιουργία νέων πηγών εσόδων κάνοντας χρήση των πνευματικών κεφαλαίων.
- 6) Για να τροποποιήσουν τα προϊόντα τους, ώστε να τα εστιάσουν στις υπάρχουσες αγορές.
- 7) Για να λύσουν το πρόβλημα ενοποίησης των συστημάτων τους.
- 8) Για τη δυναμική ανάπτυξη και αξιοποίηση παλαιότερων εφαρμογών.
- 9) Για να αυξήσουν την παραγωγικότητά τους σε οργανωσιακό αλλά και σε ατομικό επίπεδο.

Σύμφωνα με τον Clabby οι Υπηρεσίες Διαδικτύου είναι τόσο ευέλικτες, που θα επιτρέψουν στις επιχειρήσεις στο μέλλον να λειτουργούν με νέους διαφορετικούς τρόπους, χρησιμοποιώντας νέα επιχειρηματικά μοντέλα, διαφορετικά από τα σημερινά.

Το ίδιο ενθουσιώδεις είναι οι προμηθευτές και οι αναλυτές προβλέπονταν ένα κόσμο όπου οι επιχειρήσεις θα παρέχουν τις υπηρεσίες τους με τη μορφή Υπηρεσιών Διαδικτύου μέσω δημόσιων καταλόγων που θα παρέχουν απευθείας σύνδεση με αυτές. Σε αυτό το νέο περιβάλλον μια μικρή εταιρεία θα είναι σε θέση να συγκροτήσει μια ολόκληρη επιχείρηση συνθέτοντάς την από Υπηρεσίες Διαδικτύου που δημιουργήθηκαν και διατηρούνται από άλλες επιχειρήσεις.

Εντούτοις, πολλοί ερευνητές όπως ο David Schatsky, διευθυντής και ανώτατος αναλυτής στην εταιρεία Jupiter Media Metrix, θεωρούν ότι η τεράστια διαφημιστική εκστρατεία δεν θα φέρει κανένα αποτέλεσμα, τουλάχιστον σύντομα. Ο λόγος είναι ότι πάρα πολλά ερωτήματα σε τεχνολογικά και επιχειρησιακά ζητήματα παραμένουν αναπάντητα. Μερικά από τα ερωτήματα είναι το πώς θα αντιμετωπιστεί το ζήτημα της ασφάλειας, πώς οι επιχειρήσεις θα είναι σίγουρες για τη διαθεσιμότητα και την αξιοπιστία μιας Υπηρεσίας Δικτύου, που τους προσφέρεται από μια άλλη επιχείρηση, και τέλος ποιος θα αναλάβει την ευθύνη αν μια υπηρεσία αποτύχει να προσφέρει ότι υπόσχεται. Άλλωστε, το να χρησιμοποιήσει μια επιχείρηση τους καταλόγους υπηρεσιών για να ανακαλύψει μια υπηρεσία δυναμικά και να αλληλεπιδράσει με επιχειρήσεις με τις οποίες μπορεί να μην έχει συνάψει ποτέ επιχειρηματικές σχέσεις, είναι σίγουρα αρκετά ριψοκίνδυνο. Το γεγονός ότι μόνο ένα μικρό ποσοστό των επιχειρήσεων φέρεται να είναι έτοιμο να αναλάβει ένα τέτοιο ρίσκο, αποδεικνύει ότι στο μέλλον οι Υπηρεσίες Διαδικτύου έχουν να αντιμετωπίσουν μεγάλες προκλήσεις.



2.8. Συμπέρασμα και ζητήματα προς διερεύνηση.

Από την εισαγωγή που προηγήθηκε στις Υπηρεσίες Διαδικτύου, το συμπέρασμα που προκύπτει για τη συγκεκριμένη τεχνολογία είναι ότι πρόκειται πραγματικά για κάτι καινούριο, σαν φιλοσοφία, στο χώρο της πληροφορικής. Ανεξάρτητα από το αν υπάρχουν τεχνολογίες πάνω στις οποίες μπορεί να στηριχθεί η ιδέα των Υπηρεσιών Διαδικτύου, από μόνη της η ιδέα μπορεί να θεωρηθεί ότι συντελεί σε μια επανάσταση.

Η πρόκληση για να πετύχει η επανάσταση αυτή είναι μεγάλη. Μεγάλες, όμως, είναι και οι προκλήσεις που έχει να αντιμετωπίσει. Στο σημείο αυτό παρατίθενται τα σημαντικότερα ζητήματα προς διερεύνηση, τα οποία συνίστανται από χαρακτηριστικά ερωτήματα που απαιτούν απάντηση [Glass, 2000]:

1. Ανακάλυψη Υπηρεσίας Διαδικτύου.

Πώς μια Υπηρεσία Διαδικτύου θα μπορεί να διαφημίζει τον εαυτό της; Τι θα συμβαίνει αν μια Υπηρεσία Διαδικτύου τροποποιηθεί ή μετακινηθεί; Είναι απαραίτητη η ανάπτυξη νέων προτύπων για να υποστηριχθεί η όλη διαδικασία;

2. Αλληλεπίδραση μεταξύ Υπηρεσιών Διαδικτύου.

Η αλληλεπίδραση μεταξύ των Υπηρεσιών Διαδικτύου θα απαιτεί τη δέσμευση πόρων και από τις δύο πλευρές μέχρι την ολοκλήρωσή της; Τι θα συμβαίνει αν οι αλληλεπιδράσεις είναι μεγάλης χρονικής διάρκειας;

3. Δυνατότητα Κλιμάκωσης.

Είναι δυνατόν να χρησιμοποιηθούν οι μηχανισμοί κλιμάκωσης που ήδη υπάρχουν, όπως η εξισορρόπηση φόρτου; Ποια εμπόδια μπορεί να υπάρξουν; Είναι απαραίτητη η δημιουργία ενός νέου είδους server εφαρμογών (Web Services application server);

4. Δυνατότητα διαχείρισης.

Ποιοι μηχανισμοί είναι απαραίτητοι για τη διαχείριση ενός συστήματος που είναι κατανεμημένο σε τόσο μεγάλο βαθμό; Είναι απαραίτητος ο συντονισμός των διαχειριστών των διαφορετικών Υπηρεσιών Διαδικτύου; Είναι δυνατόν να μεταφερθεί²² η διαχείριση μιας Υπηρεσίας Διαδικτύου σε μια άλλη Υπηρεσία Διαδικτύου;

5. Δυνατότητα Υπολογισμών.

Πώς μπορεί να καθοριστεί ο χρόνος που μπορεί ένας χρήστης να χρησιμοποιεί μια Υπηρεσία Διαδικτύου; Πώς θα υλοποιηθεί η χρέωση των Υπηρεσιών Διαδικτύου; Ποιο μοντέλο χρέωσης θα χρησιμοποιηθεί; Αν μια Υπηρεσία Διαδικτύου αγοραστεί από κάποιον άλλο, πώς καθορίζεται ότι άλλαξε η ιδιοκτησία της; Μπορεί μια υπηρεσία Διαδικτύου να καταναλωθεί

²² να γίνει outsource

πλήρως ή μπορεί να επαναχρησιμοποιηθεί πολλές φορές σαν αποτέλεσμα της συμφωνίας που έχει γίνει;

6. Έλεγχος.

Πώς γίνεται ο έλεγχος λαθών σε ένα σύστημα που περιλαμβάνει πολλές Υπηρεσίες Διαδικτύου, οι οποίες είναι δυναμικές; Πώς επιτυγχάνονται αναμενόμενοι χρόνοι απόκρισης; Πώς γίνεται έλεγχος λαθών σε Υπηρεσίες Διαδικτύου που προέρχονται από διαφορετικούς προμηθευτές, φιλοξενούνται σε διαφορετικά περιβάλλοντα και εκτελούνται σε διαφορά λειτουργικά συστήματα;

7. Εμπιστοσύνη

Πώς μπορεί να υπάρχει μέτρηση της εμπιστοσύνης σε μια Υπηρεσία Διαδικτύου; Τι συμβαίνει όταν μια Υπηρεσία Διαδικτύου τεθεί προσωρινά εκτός λειτουργίας; Είναι σωστή λύση ο εντοπισμός και η χρησιμοποίηση μιας άλλης υπηρεσία στην περίπτωση αυτή; Πώς μπορεί κάποιος να γνωρίζει ποιους προμηθευτές να εμπιστευτεί;

8. Ασφάλεια.

Ποιες είναι οι βασικές παράμετροι ασφάλειας που πρέπει να παρέχει μια Υπηρεσία Διαδικτύου; Πώς εξασφαλίζεται η εμπιστευτικότητα στην επικοινωνία; Πώς αυθεντικοποιούνται οι χρήστες των υπηρεσιών; Πρέπει οι Υπηρεσίες Διαδικτύου να παρέχουν ασφάλεια σε επίπεδο μεθόδων; Αν ένας χρήστης θελήσει να συνδεθεί με ένα χορηγό που προσφέρει υπηρεσίες σε παγκόσμια κλίμακα, πώς γίνεται οι υπηρεσίες αυτές να ενημερωθούν για τα προνόμια του συγκεκριμένου χρήστη;

Στο πλαίσιο της παρούσας εργασίας, τα ζητήματα που θα βρεθούν στο επίκεντρο του ενδιαφέροντος είναι τα ζητήματα της ασφάλειας και της εμπιστοσύνης. Εντούτοις, απαντήσεις στα ζητήματα αυτά δεν μπορούν να δοθούν, αν πρωτύτερα δεν μελετηθούν οι υπάρχουσες τεχνολογίες, στις οποίες στηρίζεται η ανάπτυξη των Υπηρεσιών Διαδικτύου.

ΚΕΦΑΛΑΙΟ 3^ο : ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ XML

3.1. Εισαγωγή.

Η υπάρχουσα τεχνολογική υποδομή του παγκοσμίου ιστού αδιαμφισβήτητα έχει διευκολύνει τον κόσμο των επιχειρήσεων, ωστόσο εξακολουθούν να υπάρχουν ορισμένοι περιορισμοί. Συγκεκριμένα, δεν καλύπτεται η ανάγκη αυτόματης αλληλεπίδρασης μεταξύ εφαρμογών. Οι εφαρμογές εκτελούνται αποκλειστικά με τη χρήση φυλλομετρητών (browsers) και η αναζήτηση της πληροφορίας δεν είναι ευέλικτη, αφού βασίζεται απλά στη σάρωση HTML σελίδων.

Οι Υπηρεσίες Διαδικτύου ήρθαν να καλύψουν τέτοιου είδους κενά, εκμεταλλευόμενες την κατανεμημένη μορφή του διαδικτύου και παρέχοντας ένα νέο μοντέλο ανταλλαγής της πληροφορίας. Σε αυτό το κεφάλαιο δίνεται έμφαση στη σχέση της τεχνολογίας XML με τις Υπηρεσίες Διαδικτύου. Γίνεται αναφορά στα χαρακτηριστικά της XML, που την καθιστούν αυτή τη στιγμή πολύτιμο εργαλείο για την ανάπτυξη Υπηρεσιών Διαδικτύου και παρουσιάζονται οι τεχνολογίες που συμπληρώνουν τις απαιτήσεις για την ανάπτυξη τέτοιων υπηρεσιών (SOAP, WSDL, UDDI).

3.2. Τι είναι η XML.

Η XML (eXtensible Markup Language) είναι μια γλώσσα για τη δόμηση δεδομένων. Αποτελεί ένα σύνολο κανόνων για το σχεδιασμό μορφών κειμένου, το οποίο διευκολύνει τη συλλογή στοιχείων δεδομένων. Η XML [Khare et al., 1997] αποτελεί σύσταση του οργανισμού W3C²³ από το Φεβρουάριο του 1998, ενώ η ανάπτυξη της ξεκίνησε το 1996. Ωστόσο, ως τεχνολογία δεν είναι καινούρια. Η XML αποτελεί υποσύνολο της SGML²⁴, η οποία αναπτύχθηκε στις αρχές της δεκαετίας του '80, τυποποιήθηκε από τον ISO το 1986, και χρησιμοποιήθηκε ευρέως σε προγράμματα με εκτεταμένη τεκμηρίωση. Οι σχεδιαστές της XML επέλεξαν τα καλύτερα τμήματα της SGML, χρησιμοποίησαν την εμπειρία που είχαν αποκτήσει κατά την ανάπτυξη της HTML²⁵ και παρήγαγαν μία γλώσσα, η οποία είναι πιο κανονικοποιημένη και πολύ πιο εύχρηστη.

²³ World Wide Web Consortium

²⁴ Standard Generalized Markup Language

²⁵ Η ανάπτυξη της HTML ξεκίνησε το 1990

Η XML σχεδιάστηκε για να περιγράφει δεδομένα χρησιμοποιώντας αυθαίρετες ετικέτες (tags) και για να είναι κατάλληλη για χρήση στο διαδίκτυο, υποστηρίζοντας γενικούς μηχανισμούς για την επέκταση και τον εμπλουτισμό της HTML. Κύρια χαρακτηριστικά της XML είναι τα εξής:

- Επιτρέπει στο χρήστη να ορίσει τις δικές του ετικέτες στα δεδομένα.
- Οριοθετεί τμήματα δεδομένων και αφήνει την ερμηνεία τους αποκλειστικά στην εφαρμογή που τα διαβάζει.
- Κατηγοριοποιεί τα έγγραφα σε έγκυρα και μη.
- Μπορεί να χρησιμοποιηθεί για να καθορίσει νέες γλώσσες περιγραφής δεδομένων²⁶.
- Δεν χρειάζεται άδεια χρήστης, λειτουργεί ανεξαρτήτως συστήματος υλικού και τυγχάνει ευρείας υποστήριξης
- Αποτελεί τη βάση του RDF²⁷ και του Σημασιολογικού Ιστού²⁸

Η XML συνδύαζει διαφορετικές τεχνολογίες. Η βασική XML είναι η προδιαγραφή που ορίζει τι είναι οι ετικέτες (tags) και τα γνωρίσματα (attributes). Ωστόσο, εκτός από τη βασική XML, η οικογένεια της XML είναι ένα διαρκώς αναπτυσσόμενο σύνολο από λειτουργικές μονάδες, οι οποίες προσφέρουν χρήσιμες υπηρεσίες για τη διεκπεραίωση σημαντικών έργων τα οποία ανακύπτουν συχνά. Οι σημαντικότερες από αυτές [Goldfarb et al., 2000] είναι:

- Το DOM (Document Object Model) και το SAX (Simple API for XML), που είναι μοντέλα, που επιτρέπουν την ανάγνωση XML εγγράφων και την πρόσβαση στο περιεχόμενο και τη δομή τους.
- Η XSL (Extensible Stylesheet Language), που είναι μια προηγμένη γλώσσα μορφοποίησης σελίδων. Χρησιμοποιείται για την απεικόνιση της XML πληροφορίας και βασίζεται στην XSLT (XSL Transformations), μία γλώσσα μετασχηματισμού, η οποία χρησιμοποιείται για την αναδιάταξη, την πρόσθεση και τη διαγραφή ετικετών και γνωρισμάτων.
- Η XQL (XML Query Language), που υποστηρίζει την αναζήτηση και ανάκτηση της ζητούμενης πληροφορίας από XML έγγραφα.
- Η XLL (XML Linking Language), που περιγράφει ένα προκαθορισμένο τρόπο εισαγωγής υπερσυνδέσμων σε αρχεία XML και επιτρέπει την προσπέλαση ή την αναφορά στις εσωτερικές δομές των XML εγγραφών μέσω της Xpath (XML Path Language).

²⁶ Δηλαδή εκτός από markup language, η XML είναι και metalanguage.

²⁷ Resource Description Framework: πρότυπο για την περιγραφή μέτα-δεδομένων (metadata) που αφορούν αντικείμενα που βρίσκονται στο διαδίκτυο

²⁸ Ο όρος semantic web αποτελεί επέκταση του όρου web στην προσπάθεια να περιλάβει το web μόνο καλά ορισμένες πληροφορίες (με τη βοήθεια του προτύπου RDF και άλλων και αφορά προτύπων).

- Τα XML Schemas, που επιτρέπουν στους κατασκευαστές λογισμικού να ορίσουν με ακρίβεια τις δομές των δικών τους μορφών XML.

3.3. Πλεονεκτήματα της XML στη διαχείριση της πληροφορίας.

Η τεχνολογία XML συντελεί στην κλιμάκωση των δυνατοτήτων του διαδικτύου και προσφέρει ευελιξία στη διαχείριση και διάδοση της πληροφορίας. Τα πλεονεκτήματα που εισάγει η χρήση της μεταβάλουν σε μεγάλο βαθμό το τοπίο στον τομέα της ανάπτυξης εφαρμογών. Τα σημαντικότερα πλεονεκτήματα της XML [Seligman et al., 2001] συνοψίζονται στις παρακάτω προτάσεις:

- Η XML διευκολύνει την προσαρμογή ετερογενών δομών δεδομένων σε μια εφαρμογή. Η XML μπορεί να αποτελέσει την υποδομή για ένα διαδεδομένο και οικονομικό τρόπο ανταλλαγής αυτοπροσδιοριζόμενων μηνυμάτων. Οι μετέχοντες σε αυτή την επικοινωνία μπορούν να χρησιμοποιήσουν την XML ως το μέσο για να περιγράφουν οποιαδήποτε δεδομένα, αρκεί προηγουμένως να έχουν συμφωνήσει στο σχήμα που θα χρησιμοποιήσουν και στη σημασία του κάθε στοιχείου (element).
- Οι διαχειριστές των δεδομένων μπορούν να χρησιμοποιήσουν την XML για ενσωμάτωση μετα-δεδομένων (metadata) που μπορούν να απλοποιήσουν το συνταίριασμα ετερογενών βάσεων δεδομένων, ιδιαίτερα όταν το πρόβλημα είναι η ετερογένεια στην αναπαράσταση των γνωρισμάτων, στη σημασιολογία ή στο σχήμα της βάσης.
- Τα εργαλεία της XML συμβάλουν σημαντικά στην ικανότητα των επιχειρήσεων να διαχειρίζονται και να μοιράζονται ημι-δομημένη πληροφορία, που είναι δύσκολο να περιγραφεί βάσει ενός προκαθορισμένου σχήματος.

3.4. Ενοποίηση εφαρμογών στο Διαδίκτυο.

Στην ενότητα 2.5. έγινε μια εισαγωγή στις δυνατότητες που δημιουργούνται για τις επιχειρήσεις με την ανάπτυξη των Υπηρεσιών Διαδικτύου. Συγκεκριμένα, οι επιχειρήσεις στη νέα εποχή των Υπηρεσιών Διαδικτύου, έχουν τη δυνατότητα να:

- Δημοσιεύουν στο διαδίκτυο διεπαφές για τις υπηρεσίες που παρέχουν, έτσι ώστε άλλες επιχειρήσεις να μπορούν να βρουν αυτές τις υπηρεσίες και να τις χρησιμοποιήσουν.
- Αναζητούν και να ανακαλύπτουν δημοσιευμένες διεπαφές άλλων επιχειρήσεων με τις οποίες επιθυμούν συνεργασία μέσω του διαδικτύου.

- Αλληλεπιδρούν με υπηρεσίες που δημοσιεύονται από άλλες επιχειρήσεις, και αντίστροφα να επιτρέπουν σε άλλες επιχειρήσεις να συνεργάζονται με τις δικές τους υπηρεσίες και να καθορίζουν εμπορικές συμφωνίες για ροή εγγράφων και εργασιών.

Τα παραπάνω απαιτούν την εγκαθίδρυση, μεταξύ των επιχειρήσεων, μιας κοινής γλώσσας επικοινωνίας των υπηρεσιών, δηλαδή ενός αποδοτικού μέσου για την ανταλλαγή δεδομένων και την κατανομή λογικής μεταξύ εφαρμογών [Kazutoshi et al., 2002].

Με δεδομένη την ύπαρξη ετερογένειας στις υποδομές, η χρησιμοποίηση κατανεμημένων μοντέλων αντικειμένων²⁹ για τη διανομή λογικής των εφαρμογών είναι μια λύση που δεν μπορεί να κλιμακωθεί στο εύρος του διαδικτύου. Ο βασικός λόγος είναι ότι οι τεχνολογίες αυτές στηρίζονται στη συνεκτική σύνδεση του καταναλωτή της υπηρεσίας με την υπηρεσία, γεγονός που σημαίνει ότι οι προγραμματιστές μπορούν να διατηρήσουν ένα μεγάλο μέρος του πλούτου και της ακρίβειας που έχουν συνηθίσει στο τοπικό μοντέλο προγραμματισμού. Αντίθετα, οι Υπηρεσίες Διαδικτύου δεν είναι συνεκτικά συνδεδεμένες. Η εφαρμογή πρέπει να συνεχίζει να λειτουργεί, ακόμα και αν αλλάξει η υλοποίηση σε οποιαδήποτε πλευρά της σύνδεσης και αυτό τεχνικά μεταφράζεται σε χρήση ασύγχρονης τεχνολογίας που βασίζεται σε ανταλλαγή μηνυμάτων και σε χρήση πρωτοκόλλων του διαδικτύου για να επιτευχθεί παγκόσμια εμβέλεια. [Layman et al., 2001].

Τα συστήματα ανταλλαγής μηνυμάτων ενθυλακώνουν τις θεμελιώδεις μονάδες επικοινωνίας σε αυτοπροσδιοριζόμενα πακέτα (μηνύματα), τα οποία τοποθετούν στην άκρη του διαύλου επικοινωνίας. Σε ένα σύστημα ανταλλαγής μηνυμάτων, η μόνη υπόθεση που κάνει ο αποστολέας είναι ότι ο παραλήπτης είναι σε θέση να κατανοήσει το μήνυμα που αποστέλλεται. Ο αποστολέας δεν κάνει υποθέσεις σχετικά με το τι θα γίνει μετά την παραλαβή του μηνύματος ούτε για το τι θα συμβεί μεταξύ του ιδίου και του παραλήπτη. Τα πλεονεκτήματα αυτού του μοντέλου επικοινωνίας στην περίπτωση των Υπηρεσιών Διαδικτύου είναι εμφανή. Για παράδειγμα, επιτρέπεται να τροποποιηθεί ο παραλήπτης, ανά πάσα στιγμή, χωρίς να δημιουργηθεί πρόβλημα με τον αποστολέα, εφόσον είναι σε θέση να κατανοήσει τα ίδια μηνύματα. Ο παραλήπτης μπορεί να αναβαθμίσει και να βελτιώσει τις τρέχουσες εφαρμογές, χωρίς να δημιουργήσει πρόβλημα σε αυτές. Επίσης, ο αποστολέας δεν χρειάζεται ειδικό λογισμικό για να είναι σε θέση να μιλά με τον παραλήπτη. Εφόσον μπορεί να αποστέλλει μηνύματα με την κατάλληλη μορφή, ο παραλήπτης μπορεί να ανταποκρίνεται.

3.5. Ο ρόλος της XML στην ανάπτυξη Υπηρεσιών Διαδικτύου.

²⁹ CORBA, DCOM ή RMI

Το κλειδί για τη λειτουργία των Υπηρεσιών Διαδικτύου, με βάση την ανάλυση που προηγήθηκε και η οποία αφορούσε στην ενοποίηση εφαρμογών στο διαδίκτυο, είναι η συμφωνία σε μια απλή μορφή περιγραφής δεδομένων για την ανταλλαγή μηνυμάτων με χρήση των πρωτοκόλλων του διαδικτύου. Σύμφωνα και με τον Bosworth [Bosworth, 2001], χωρίς την καθιέρωση κάποιου πρότυπου σύνταξης, που θα αποτελέσει τη βάση για τη δημιουργία μιας γλώσσας επικοινωνίας (*lingua franca*), η οποία θα χρησιμοποιηθεί για την ανταλλαγή μηνυμάτων, δεν είναι δυνατόν να επιτευχθεί η αποτελεσματική και αποδοτική ενοποίηση υπηρεσιών.

Τα σημαντικά πλεονεκτήματα που παρουσιάζει η XML στη διαχείριση και διάδοση των πληροφοριών (βλ. ενότητα 3.3.), συντέλεσαν στο να θεωρηθεί απαραίτητη για την επικοινωνία των εφαρμογών. Έτσι η τεχνολογία XML, σήμερα, είναι η βάση για την ανάπτυξη Υπηρεσιών Διαδικτύου.

Οι Υπηρεσίες Διαδικτύου χρησιμοποιούν XML για τρεις λόγους [Layman et al., 2001]. Αυτοί είναι: α) η συμφωνία σε επίπεδο μονάδων επικοινωνίας, β) η περιγραφή υπηρεσίας και γ) η ανακάλυψη υπηρεσίας. Συγκεκριμένα:

α) Σε επίπεδο μονάδων επικοινωνίας είναι απαραίτητο οι εφαρμογές που επικοινωνούν να χρησιμοποιούν την ίδια γλώσσα. Η επεκτασιμότητα και η ευελιξία της XML επιτρέπουν την περιγραφή δεδομένων που περιέχονται σε μια μεγάλη ποικιλία από ετερογενείς εφαρμογές. Επειδή, η XML είναι αυτο-περιγραφόμενη, τα δεδομένα μπορούν να ανταλλαχθούν και να τύχουν επεξεργασίας, χωρίς να υπάρχει περιγραφή των εισερχόμενων δεδομένων προκαθορισμένη από την εφαρμογή. Ωστόσο, οι εφαρμογές πρέπει να χρησιμοποιούν ένα σύνολο κανόνων σχετικά με τον τρόπο που θα εμφανίζονται οι διαφορετικοί τύποι δεδομένων, καθώς και σχετικά με τον τρόπο εμφάνισης των εντολών. Το πρωτόκολλο Simple Object Access Protocol (SOAP)³⁰ βασίζεται στην γλώσσα XML και αντιπροσωπεύει ένα κοινό σύνολο κανόνων σχετικά με τον τρόπο εμφάνισης και επέκτασης των δεδομένων και των εντολών.

β) Εφόσον οι εφαρμογές ακολουθούν τους ίδιους γενικούς κανόνες σχετικά με τον τρόπο εμφάνισης των τύπων δεδομένων και των εντολών, χρειάζονται και ένα τρόπο περιγραφής των συγκεκριμένων δεδομένων και των εντολών που αποδέχονται. Για παράδειγμα, δεν αρκεί μια εφαρμογή να δέχεται ακέραιους αριθμούς. Ήα πρέπει να υπάρχει τρόπος ώστε να καθορίζεται ρητά ότι εάν λάβει δύο ακέραιους, θα τους πολλαπλασιάσει. Η γλώσσα Web

Services Description Language (WSDL)³⁰ είναι μια γραμματική XML που μπορεί να χρησιμοποιηθεί για την περιγραφή³¹ μιας υπηρεσίας διαδικτύου.

γ) Τέλος, είναι απαραίτητο ένα σύνολο κανόνων για τον τρόπο εντοπισμού της περιγραφής μιας υπηρεσίας. Το πρότυπο Universal Description Discovery and Integration (UDDI)³⁰ ορίζει ένα μοντέλο δεδομένων σε XML, καθώς και SOAP διεπαφές (SOAP APIs), για την καταχώρηση και αναζήτηση αρχείων περιγραφής υπηρεσιών διαδικτύου.

3.6. Υπηρεσίες Διαδικτύου βασισμένες στην XML.

Ο ορισμός που δόθηκε στην ενότητα 2.2. για τις Υπηρεσίες Διαδικτύου δεν αναφέρεται σε συγκεκριμένα πρότυπα που πρέπει να τις υποστηρίζουν. Ωστόσο, η ανάμειξη της XML τεχνολογίας αποτελεί γεγονός αυτονόητο σε οποιαδήποτε αναφορά σχετική με Υπηρεσίες Διαδικτύου στις μέρες μας. Σε πολλές περιπτώσεις η τεχνολογία XML αποτελεί σημείο αναφοράς για τον ορισμό των Υπηρεσιών Διαδικτύου. Ένας διαδεδομένος ορισμός για τις Υπηρεσίες Διαδικτύου είναι ο παρακάτω:

Oι Υπηρεσίες Διαδικτύου είναι XML αναπαραστάσεις προγραμμάτων, αντικειμένων ή κειμένων που είναι προσπελάσιμα μέσω του Internet για απ' ευθείας αλληλεπίδραση μεταξύ εφαρμογών. Οι υπηρεσίες αυτές αν και μπορούν να προσπελαστούν με χρήση φυλλομετρητών (browsers), δεν απαιτούν ούτε τη χρήση φυλλομετρητή ούτε τη χρήση της γλώσσας HTML. Οι υπηρεσίες διαδικτύου βασισμένες σε XML παρέχουν έναν ανεξάρτητο από δεδομένα μηχανισμό παρουσίασης των υπηρεσιών της επιχείρησης, με χρήση πρότυπων πρωτοκόλλων των δικτύων Internet, Intranet και Extranet. [Ioma, 2002]

Μολονότι ο σκοπός της παρούσας εργασίας είναι να εξετάσει τις Υπηρεσίες Διαδικτύου που βασίζονται στην XML, δεν τίθεται θέμα νιοθέτησης του παραπάνω ορισμού, αφού ο ορισμός αυτός υπερκαλύπτεται από τον ορισμό που έχει δοθεί στο κεφάλαιο 2.

3.6.1. Τεχνολογίες που συμπληρώνουν την XML.

Οι τεχνολογίες και τα πρότυπα που επιτρέπουν τη διαλειτουργικότητα μεταξύ των Υπηρεσιών Διαδικτύου περιλαμβάνουν εκτός από την XML:

³⁰ στη συνέχεια θα αναφερθούν περισσότερα για το SOAP, την WSDL και το UDDI.

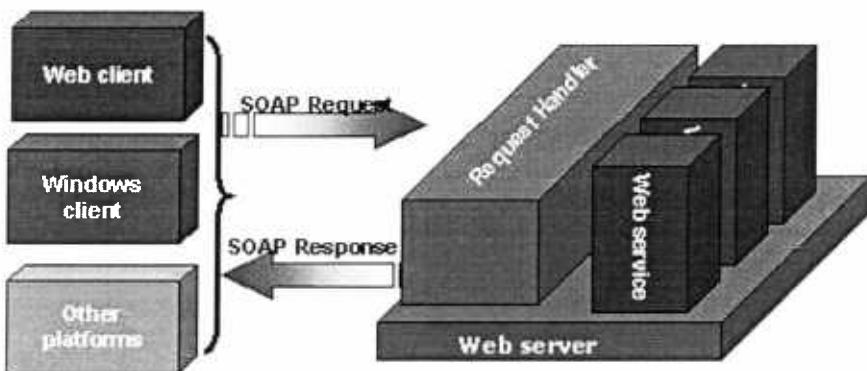
³¹ βλέπε περιγραφή υπηρεσίας (κεφάλαιο 1^ο)



- Το πρωτόκολλο SOAP (Simple Object Access Protocol), που αποτελεί ένα πρωτόκολλο επικοινωνίας εφαρμογών βασισμένο σε XML.
- Τη γλώσσα WSDL (Web Services Description Languages), που είναι ένα XML schema για περιγραφή των μηνυμάτων, λειτουργιών και την αντιστοίχηση πρωτοκόλλων υπηρεσιών διαδικτύου.
- Το πρότυπο UDDI (Universal Description Discovery and Integration), που ορίζει ένα χώρο αποθήκευσης για καταχώρηση και αναζήτηση περιγραφών υπηρεσιών διαδικτύου.

3.6.2. Η Αρχιτεκτονική των υπηρεσιών.

Ανεξάρτητα από τα εργαλεία ή τις γλώσσες προγραμματισμού που χρησιμοποιούνται για την ανάπτυξη μιας Υπηρεσίας Διαδικτύου, η αρχιτεκτονική μιας τέτοιας υπηρεσίας δίνεται στο σχήμα 3.1. [Shohoud, 2003].



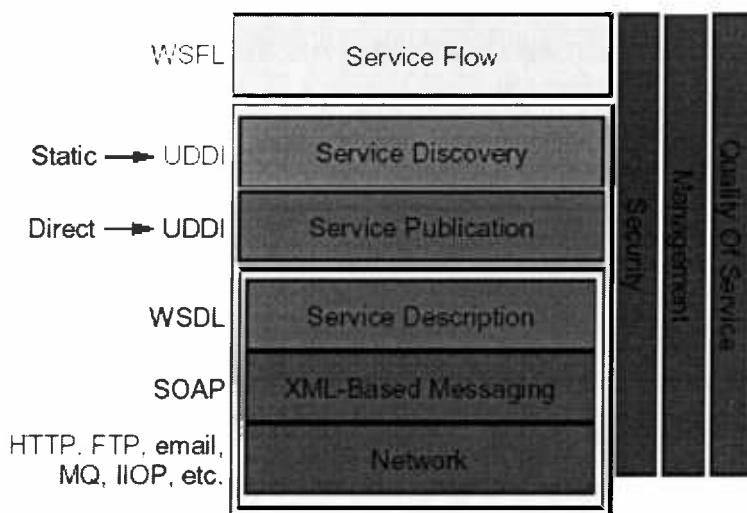
Σχήμα 3.1.: Αρχιτεκτονική μιας Υπηρεσίας Διαδικτύου. [Shohoud, 2003]

Ο χρήστης έχει τη δυνατότητα να δημιουργήσει μια υπηρεσία με τη γλώσσα προγραμματισμού που επιθυμεί (π.χ. VB 6 ή VB.NET) και στη συνέχεια να τη δημοσιεύσει (με τη χρήση του SOAP Toolkit ή του .NET built-in support). Μια εφαρμογή πελάτης, που λειτουργεί σε οποιαδήποτε πλατφόρμα και είναι γραμμένη σε οποιαδήποτε γλώσσα, μπορεί να καλέσει την υπηρεσία, προσπελάζοντας το WSDL αρχείο που περιγράφει την υπηρεσία και διατυπώνοντας μια αίτηση, με τη μορφή SOAP μηνύματος, που βασίζεται στην περιγραφή της υπηρεσίας. Η Υπηρεσία Διαδικτύου που βρίσκεται σε κάποιον Web Server λαμβάνει την αίτηση του πελάτη ως τμήμα μιας HTTP POST αίτησης. Ο Web Server προωθεί την αίτηση σε ένα διαχειριστή αιτήσεων (Web Service request handler).

επεξεργασία. Ο διαχειριστής αιτήσεων είναι υπεύθυνος για την ανάλυση του SOAP μηνύματος-αίτησης, την κλήση της Υπηρεσίας Διαδικτύου και τη δημιουργία ενός SOAP μηνύματος-απόκρισης. Ο Web Server παίρνει το μήνυμα-απόκριση και το στέλνει στον πελάτη σαν τμήμα μιας HTTP απόκρισης.

3.6.3. Η Στοίβα των υπηρεσιών.

Για να εκτελεστούν οι διαδικασίες δημοσίευση, εύρεση, δέσμευση, που περιγράφηκαν στην ενότητα 2.5.3., είναι απαραίτητη η ύπαρξη μιας στοίβας Υπηρεσιών Διαδικτύου που να περιλαμβάνει πρότυπα σε κάθε επίπεδο [Kreger, 2001]. Στο σχήμα 3.2. παρουσιάζεται η θεμελιώδης στοίβα μιας Υπηρεσίας Διαδικτύου. Τα ανώτερα επίπεδα «χτίζονται» επάνω στις δυνατότητες που τους προσφέρουν τα κατώτερά τους. Οι κατακόρυφες στήλες αναπαριστάνουν τις απαιτήσεις που πρέπει να καλύπτονται σε κάθε επίπεδο της στοίβας. Αριστερά από κάθε επίπεδο αναφέρονται οι τεχνολογίες που συναντώνται στο επίπεδο αυτό.



Σχήμα 3.2.: Στοίβα πρωτοκόλλων των Υπηρεσιών Διαδικτύου. [Kreger, 2001]

Το χαμηλότερο επίπεδο στη στοίβα των Υπηρεσιών Διαδικτύου είναι το επίπεδο δικτύου. Οι Υπηρεσίες Διαδικτύου που είναι δημοσιοποιημένες στο διαδίκτυο χρησιμοποιούν τα συνηθισμένα πρωτόκολλα δικτύων. Το πρωτόκολλο HTTP είναι το *de facto* πρότυπο που χρησιμοποιείται από τις υπηρεσίες αυτές. Άλλα πρωτόκολλα του διαδικτύου που μπορούν να χρησιμοποιηθούν είναι το πρωτόκολλο SMTP και το πρωτόκολλο FTP. Σε ένα Intranet

περιβάλλον (domain) μπορούν να χρησιμοποιηθούν και άλλα πρωτόκολλα, όπως είναι το IIOP³² που χρησιμοποιεί η τεχνολογία CORBA.

Το επόμενο επίπεδο (XML-based messaging) χρησιμοποιεί την XML ως βάση του πρωτοκόλλου ανταλλαγής μηνυμάτων. Στο επίπεδο αυτό το πρωτόκολλο SOAP έχει επιλεγεί ως το καταλληλότερο γιατί αποτελεί πρότυπο μηχανισμό ενθυλάκωσης (standardized enveloping mechanism) για απλά μηνύματα επικοινωνίας (communicating document-centric messages) αλλά και για μηνύματα που καλούν απομακρυσμένες διαδικασίες (SOAP RPCs). Επιπλέον, είναι ιδιαίτερα απλό στη χρήση του και υποστηρίζει τις τρεις διαδικασίες που περιλαμβάνει μια Υπηρεσία Διαδικτύου (δημοσίευση, εύρεση, δέσμευση).

Το επίπεδο περιγραφής της υπηρεσίας είναι στην πραγματικότητα μια στοίβα από έγγραφα περιγραφής των υπηρεσιών. Η γλώσσα WSDL είναι το *de facto* πρότυπο που χρησιμοποιείται για την περιγραφή μιας XML-based υπηρεσίας. Η WSDL περιγραφή μιας υπηρεσίας είναι η ελάχιστη προϋπόθεση για την υποστήριξη διαλειτουργικών Υπηρεσιών Διαδικτύου.

Στο επίπεδο δημοσίευσης μιας υπηρεσίας ανήκει οποιαδήποτε ενέργεια που καθιστά διαθέσιμο σε ένα πελάτη ένα WSDL έγγραφο. Το πιο απλό παράδειγμα σε αυτό το επίπεδο είναι η απευθείας αποστολή μιας WSDL περιγραφής (π.χ. μέσω e-mail) από το χορηγό της υπηρεσίας στον πελάτη. Αυτή η διαδικασία καλείται άμεση δημοσίευση (direct publication). Εναλλακτικά, ο χορηγός μιας υπηρεσίας μπορεί να δημοσιεύσει το WSDL έγγραφο με την περιγραφή μιας υπηρεσίας στην WSDL registry ενός τοπικού υπολογιστή, σε μια ιδιωτική UDDI registry, ή στον κόμβο ενός UDDI operator.

Οι μηχανισμοί του επίπεδου ανακάλυψης μιας υπηρεσίας ποικίλουν ανάλογα με τους μηχανισμούς δημοσίευσης μιας υπηρεσίας. Για το λόγο αυτό το επίπεδο ανακάλυψης μιας υπηρεσίας είναι άμεσα εξαρτώμενο από το επίπεδο δημοσίευσης. Ομοίως με πριν, στο επίπεδο αυτό ανήκει οποιαδήποτε διαδικασία, η οποία επιτρέπει σε ένα πελάτη να αποκτήσει πρόσβαση στην περιγραφή μιας υπηρεσίας και να την κάνει διαθέσιμη στην εφαρμογή του. Το πιο απλό παράδειγμα ανακάλυψης μιας υπηρεσίας είναι η στατική ανακάλυψη κατά την οποία ο πελάτης αποκτά το WSDL έγγραφο από ένα τοπικό αρχείο. Η στατική ανακάλυψη προϋποθέτει ότι η υπηρεσία έχει δημοσιευτεί άμεσα ή ότι έχει συμβεί προηγούμενη διαδικασία εύρεσης. Εναλλακτικά της στατικής ανακάλυψης, μια υπηρεσία μπορεί να ανακαλυφθεί από την WSDL registry ενός τοπικού υπολογιστή, από μια ιδιωτική UDDI registry, ή από τον κόμβο ενός UDDI operator.

³² Internet Inter-ORB Protocol

Τέλος, το ανώτερο επίπεδο στη στοίβα των Υπηρεσιών Διαδικτύου είναι το επίπεδο ροής υπηρεσιών. Στο επίπεδο αυτό περιγράφεται με ποιο τρόπο περισσότερες υπηρεσίες συνεργάζονται και επικοινωνούν μεταξύ τους συνθέτοντας μια καινούρια υπηρεσία. Η γλώσσα Web Services Flow Language (WSFL) είναι μια γραμματική XML που δημιουργήθηκε από την IBM και έχει προταθεί και ως πρότυπο. Η WSFL θεωρεί δύο τύπους συνθέσεων Υπηρεσιών Διαδικτύου: Ο πρώτος τύπος (flow models) προσδιορίζει το κατάλληλο πρότυπο για τη χρήση μιας συλλογής υπηρεσιών, κατά τέτοιο τρόπο ώστε η προκύπτουσα σύνθεση να περιγράφει τον τρόπο επίτευξης ενός ιδιαίτερου επιχειρησιακού στόχου. Ουσιαστικά, το αποτέλεσμα είναι η περιγραφή της επιχειρησιακής διαδικασίας. Ο δεύτερος τύπος (global models) προσδιορίζει το πρότυπο αλληλεπίδρασης μιας συλλογής από υπηρεσίες Διαδικτύου. Σε αυτήν την περίπτωση, το αποτέλεσμα είναι η περιγραφή των αλληλεπιδράσεων μεταξύ συνεργατών.

3.6.4. Περιγραφή των τεχνολογιών.

Στην ενότητα αυτή παρουσιάζονται αναλυτικά οι τεχνολογίες:

- Simple Object Access Protocol (SOAP).
- Web Services Description Language (WSDL).
- Universal Description Discovery and Integration (UDDI).

3.6.4.1. *Simple Object Access Protocol (SOAP)*.

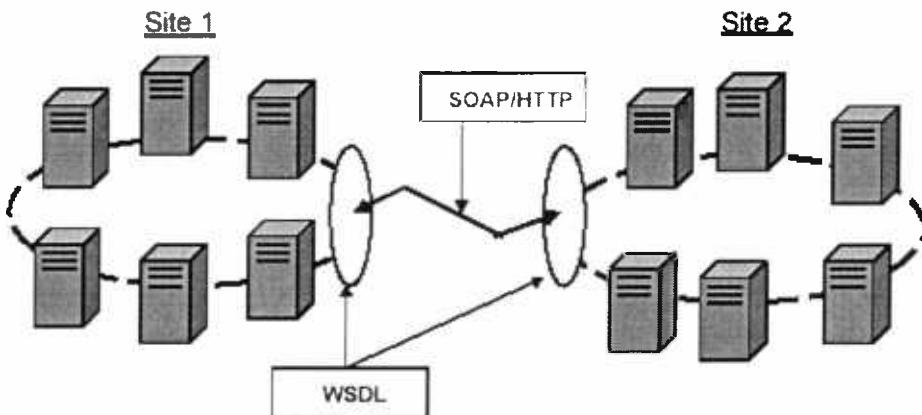
Το πρωτόκολλο SOAP είναι ένα πλαίσιο ανταλλαγής μηνυμάτων βασισμένο στην XML. Είναι ειδικά σχεδιασμένο για την ανταλλαγή μηνυμάτων μέσω διαδικτύου. Είναι απλό στη χρήση, και εντελώς ανεξάρτητο από λειτουργικό σύστημα, γλώσσα προγραμματισμού ή πλατφόρμα κατανεμημένων συστημάτων. Το SOAP δεν εισάγει κάποιο νέο πρωτόκολλο μεταφοράς και στηρίζεται στα HTTP, SMTP και MQSeries.

Το SOAP εκτός από το να παρέχει σε επίπεδο μεταφοράς μια αντιστοίχηση για την ανταλλαγή XML μηνυμάτων μέσω του διαδικτύου, επιτρέπει σε μια επιχείρηση να:

- Δημοσιοποιήσει τις υπηρεσίες της για ανταλλαγή XML εταιρικών δεδομένων.
- Ανακαλύψει την τοποθεσία και τη μορφή υπηρεσιών άλλων επιχειρήσεων.
- Καθορίσει ιδιότητες των ανταλλασσόμενων μηνυμάτων που σχετίζονται με την ποιότητα της υπηρεσίας.



Στο σχήμα 3.3. φαίνεται πώς το SOAP παρέχει έναν ανεξάρτητο και γενικό τρόπο επικοινωνίας για τη σύνδεση δύο ή περισσότερων πυλών ή εταιρικών δικτυακών τόπων. Τα σημερινά συστήματα αποτελούνται από ένα συνδυασμό πολλών διαφορετικών κατηγοριών υλικού και λογισμικού. Το SOAP και η XML βοηθούν στη συμφωνία ενός κοινού τρόπου ανταλλαγής δεδομένων μεταξύ ετερογενών συστημάτων. Το WSDL χρησιμοποιείται για την περιγραφή των υπηρεσιών και το SOAP για τη μετάδοση της πληροφορίας.



Σχήμα 3.3.: Διασύνδεση απομακρυσμένων δικτυακών τόπων. [Iona, 2002]

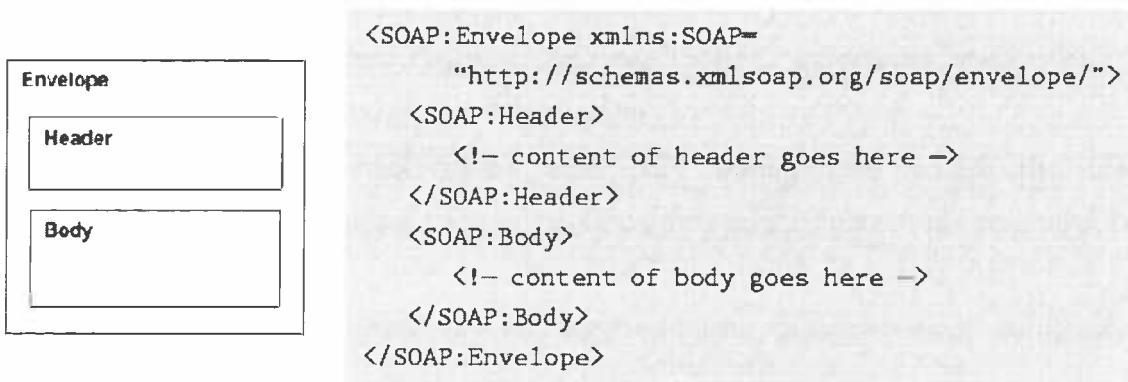
Η τρέχουσα έκδοση της προδιαγραφής SOAP (V1.1) είναι διαθέσιμη³³ από το World Wide Web Consortium (W3C). Το SOAP αναπτύσσεται συνεχώς και κάποιες λεπτομέρειες μπορεί να αλλάξουν στο προσεχές μέλλον.

Τα μηνύματα SOAP αποτελούνται από τρία βασικά μέρη:

- Τον Φάκελο (Envelope).
- Την Επικεφαλίδα (Header), που είναι προαιρετική.
- Το Σώμα (Body).

Το σχήμα 3.4. απεικονίζει τα τρία μέρη από τα οποία αποτελείται ένα SOAP μήνυμα.

³³ στη διεύθυνση <http://www.w3.org/TR/SOAP>



Σχήμα 3.4.: Μέρη ενός SOAP Μηνύματος. [Curbera et al., 2002]

Ο φάκελος είναι υποχρεωτικός και ουσιαστικά ορίζει την αρχή και το τέλος του μηνύματος (αν και τα μηνύματα μπορεί να περιέχουν συνδέσμους σε αντικείμενα εκτός του φακέλου). Περιέχει πληροφορίες για το περιεχόμενο του μηνύματος και πώς να γίνει η επεξεργασία του. Η επικεφαλίδα είναι προαιρετική και περιέχει επιπλέον πληροφορία που σχετίζεται με την ασφάλεια, τις συναλλαγές και την ποιότητα των υπηρεσιών. Περιλαμβάνει ένα μηχανισμό με τον οποίο τα συναλλασσόμενα μέρη διαπραγματεύονται για την υποστήριξη μιας συγκεκριμένης επικεφαλίδας ή ενός συνόλου επικεφαλίδων. Ένα SOAP μήνυμα μπορεί να έχει περισσότερες από μια επικεφαλίδες. Το σώμα περιέχει τα δεδομένα του πραγματικού μηνύματος.

Στο απλούστερο επίπεδο λειτουργικότητάς του, το SOAP μπορεί να χρησιμοποιηθεί σαν ένα απλό πρωτόκολλο ανταλλαγής μηνυμάτων. Το σχήμα 3.5. απεικονίζει ένα απλό SOAP μήνυμα (e-ticket) που μεταφέρεται μέσω του πρωτοκόλλου HTTP.

```

POST /travelservice
SOAPAction: "http://www.acme-travel.com/checkin"
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn

<SOAP:Envelope xmlns:SOAP=
    "http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP:Body>
        <et:eTicket xmlns:et=
            "http://www.acme-travel.com/eticket/schema">
            <et:passengerName first="Joe" last="Smith"/>
            <et:flightInfo airlineName="AA"
                flightNumber="1111"
                departureDate="2002-01-01"
                departureTime="1905"/>
        </et:eTicket>
    </SOAP:Body>
</SOAP:Envelope>

```

Σχήμα 3.5.: Απλό SOAP μήνυμα. [Curbera et al., 2002]

Μια σημαντικότερη δυνατότητα που προσφέρει το SOAP είναι η απομακρυσμένη κλήση διαδικασιών (Remote Procedure Calls). Η υποστήριξη RPC μηνυμάτων προϋποθέτει τον καθορισμό ενός RPC πρωτοκόλλου που να καθορίζει:

- πώς θα γίνει η αντιστοίχηση τύπων των μεταβλητών μεταξύ της SOAP αναπαράστασής τους (XML) και της αναπαράστασής τους μέσα στην εφαρμογή (π.χ. κλάση Java).
- πού αντιστοιχεί η πληροφορία κάθε RPC τμήματος (αναγνωριστικό αντικειμένου, όνομα εντολής, παράμετροι που χρησιμοποιεί).

Το σχήμα 3.6. απεικονίζει ένα SOAP RPC μήνυμα.

```

POST /travelservice
SOAPAction: "http://www.acme-travel.com/flightinfo"
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn

<SOAP:Envelope xmlns:SOAP=
    "http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP:Body>
        <m:GetFlightInfo
            xmlns:m="http://www.acme-travel.com/flightinfo"
            SOAP:encodingStyle=
                "http://schemas.xmlsoap.org/soap/encoding/"
            xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            xmlns:xsi=
                "http://www.w3.org/2001/XMLSchema-instance">
            <airlineName xsi:type="xsd:string">UL
            </airlineName>
            <flightNumber xsi:type="xsd:int">506
            </flightNumber>
        </m:GetFlightInfo>
    </SOAP:Body>
</SOAP:Envelope>
```

Σχήμα 3.6.: SOAP RPC μήνυμα. [Curbera et al., 2002]

3.6.4.2. Web Services Description Language (WSDL).

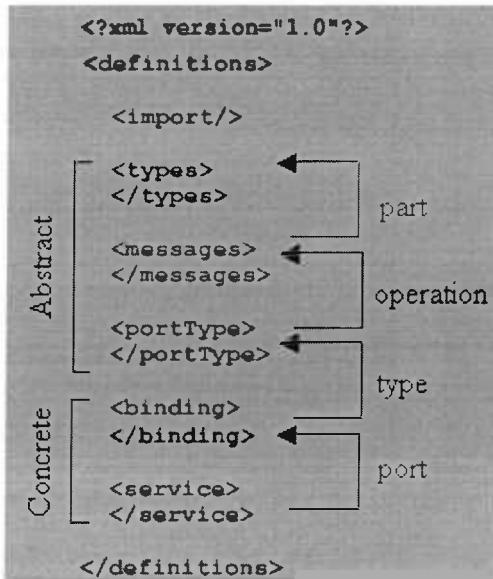
Η γλώσσα WSDL είναι ένα XML schema, που αναπτύχθηκε από τη Microsoft και την IBM με σκοπό να ορίσει το XML μήνυμα, τη λειτουργία και το πρωτόκολλο αντιστοίχησης μιας υπηρεσίας διαδικτύου που προσπελαύνεται χρησιμοποιώντας SOAP ή κάποιο άλλο XML πρωτόκολλο. Το συντακτικό του WSDL επιτρέπει τον αφαιρετικό ορισμό τόσο των μηνυμάτων όσο και των λειτουργιών των μηνυμάτων, έτσι ώστε να μπορούν να αντιστοιχηθούν σε πολλαπλές φυσικές υλοποιήσεις [Curbera et al., 2002].

Ένα WSDL έγγραφο παρέχει στον πελάτη την πληροφορία που χρειάζεται για να καλέσει μια Υπηρεσία Διαδικτύου, η οποία περιλαμβάνει [Shohoud, 2003]:



- Τη διεύθυνση στην οποία βρίσκεται η υπηρεσία.
- Το πρωτόκολλο μέσω του οποίου είναι προσπελάσιμη η υπηρεσία.
- Τον τρόπο επικοινωνίας (απλό μήνυμα ή RPC).
- Τη μορφή του μηνύματος (encoded ή literal).
- Τα ονόματα των διαδικασιών (μεθόδων) της υπηρεσίας που μπορεί να καλέσει και τους τύπους των παραμέτρων που λαμβάνουν.

Στο σχήμα 3.7. φαίνεται η δομή ενός WSDL εγγράφου [Gunzer, 2002]. Το κύριο πεδίο του εγγράφου είναι το πεδίο *definitions*. Περιλαμβάνει έξι υποπεδία που το καθένα περιέχει αναφορές στα άλλα. Η περιγραφή δίπλα σε κάθε αναφορά που παριστάνεται με βέλος, είναι το όνομα του γνωρίσματος του πεδίου που την περιέχει.

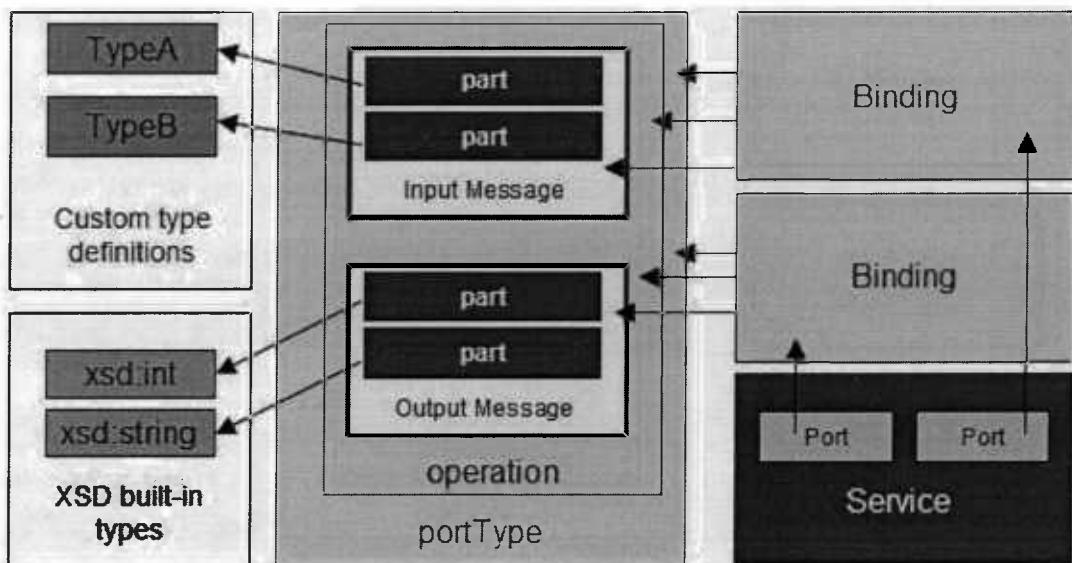


Σχήμα 3.7.: Δομή WSDL εγγράφου. [Gunzer, 2002]

Το πεδίο *import* διαχωρίζει ένα WSDL έγγραφο σε πολλαπλά ανεξάρτητα έγγραφα. Στο πεδίο *types* περιέχονται όλοι οι ορισμοί των τύπων δεδομένων που σχετίζονται με την αποστολή και λήψη ενός μηνύματος. Το πεδίο *message* μπορεί να εμφανίζεται πολλές φορές σε ένα WSDL έγγραφο και αποτελείται από το πεδίο *name* και ένα ή περισσότερα πεδία *part* που είναι τμήματα των δεδομένων ενός μηνύματος. Κάθε *port type* αποτελεί κάποιο σύνολο των διαθέσιμων διαδικασιών της υπηρεσίας. Το πεδίο *port type* περιλαμβάνει το πεδίο *operation* που αποτελείται από το γνώρισμα *name* και ένα προαιρετικό γνώρισμα που καθορίζει τη σειρά των παραμέτρων που χρησιμοποιεί η διαδικασία. Βάσει των προδιαγραφών καθορίζεται ο τύπος της διαδικασίας, ο οποίος αφορά στον τρόπο μετάδοσης (μονόδρομη, αίτηση-απόκριση, πρόσκληση, κοινοποίηση) και περιγράφεται με χρήση των

υποπεδίων *input*, *output* και *fault*. Στο πεδίο *binding* καθορίζεται το πρωτόκολλο που χρησιμοποιείται για να κληθεί μια διαδικασία και η μορφή των μηνυμάτων που ανταλλάσσονται προς τις δύο κατευθύνσεις. Τέλος, το πεδίο *service* αποτελείται από το πεδίο *name* και από το πεδίο *port* που μπορεί να εμφανίζεται περισσότερες από μια φορές. Κάθε *port* καθορίζει δύο πράγματα: τη διεύθυνση της υπηρεσίας και το *binding* που χρησιμοποιεί το *port* αυτό.

Στο σχήμα 3.8. [Shohoud, 2003] παρουσιάζονται τα στοιχεία που αποτελούν ένα WSDL έγγραφο και η συσχέτισή τους.



Σχήμα 3.8.: Απεικόνιση των συσχετίσεων μεταξύ των στοιχείων ενός WSDL εγγράφου.

Όπως φαίνεται, μια υπηρεσία έχει ένα η περισσότερα *ports* και για κάθε *port* υπάρχει ένα συγκεκριμένο *binding*. Κάθε *binding* ορίζει το πρωτόκολλο επικοινωνίας και τον τύπο μηνύματος παρέχοντας συστάσεις στο *port type*, στις διαδικασίες που περιλαμβάνει αυτό και στα μηνύματα που ορίζονται από την κάθε διαδικασία. Σημειώνεται ότι κάθε *port type* περιλαμβάνει πολλές ή και καμία διαδικασίες, κάθε διαδικασία καθορίζει δύο μηνύματα (προς και από) και κάθε μήνυμα αποτελείται από πολλά ή κανένα *parts* κάποιου τύπου δεδομένων (XSD built-in ή custom).

3.6.4.3. Universal Description, Discovery, and Integration (UDDI).

Το πρότυπο UDDI, ορίζει ένα μοντέλο δεδομένων σε XML, καθώς και SOAP διεπαφές (SOAP APIs) για την καταχώρηση και αναζήτηση πληροφορίας μιας επιχείρησης.

συμπεριλαμβανομένης της πληροφορίας που σχετίζεται με τις υπηρεσίες που παρέχει η επιχείρηση στο διαδίκτυο. Το UDDI directory είναι σχεδιασμένο σαν ένας τηλεφωνικός κατάλογος. Συγκεκριμένα το UDDI directory:

- υποστηρίζει αναζητήσεις με βάση την κατηγορία της επιχείρησης, την κατηγορία των προϊόντων της ή τη γεωγραφική της θέση.
- παρέχει γενικές πληροφορίες για την επιχείρηση, όπως διευθύνσεις, τηλέφωνα επικοινωνίας, ή αναγνωριστικά της επιχείρησης.
- παρέχει πληροφορίες για την τεχνική υποστήριξη των υπηρεσιών διαδικτύου της επιχείρησης.

Η πρόσβαση στις υπηρεσίες του UDDI ευρετηρίου εξασφαλίζεται με τη δημοσίευση μιας διεπαφής με τη μορφή SOAP-based Υπηρεσίας Διαδικτύου. Η SOAP διεπαφή διαιρείται σε δύο λογικά τμήματα, το SOAP Publisher's API και το Inquiry API. Οι επιχειρήσεις που θέλουν να καταχωρήσουν στο UDDI directory τις Υπηρεσίες Διαδικτύου που παρέχουν χρησιμοποιούν το SOAP Publisher's API. Αντίθετα, οι επιχειρήσεις που ψάχνουν στο UDDI directory προκειμένου να ανακαλύψουν κάποια υπηρεσία χρησιμοποιούν το API που υποστηρίζει την αναζήτηση μιας υπηρεσίας (Inquiry API). Το Inquiry API αποτελείται από δύο μέρη. Το πρώτο χρησιμοποιείται για την κατασκευή προγραμμάτων που επιτρέπουν την αναζήτηση και την περιήγηση στις πληροφορίες μιας UDDI registry και το δεύτερο για την αντιμετώπιση καταστάσεων αποτυχίας. Από τη στιγμή που βάσει των κριτηρίων που έχουν τεθεί βρεθεί η επιθυμητή επιχείρηση, το UDDI μπορεί να παρέχει πληροφορία εύρεσης των υπηρεσιών της επιχείρησης, δίνοντας ουσιαστικά ένα «δείκτη» στο WSDL αρχείο που περιγράφει τις υπηρεσίες διαδικτύου που παρέχει η συγκεκριμένη επιχείρηση.

Κεντρική ιδέα στο UDDI είναι η καταχώρηση της πληροφορίας ανά επιχείρηση. Κάθε αρχείο καταχώρησης (XML αρχείο) αποτελείται από πεδία που περιγράφονται από τέσσερις δομές δεδομένων (data structures). Στο σχήμα 3.9. [Gunzer, 2002] φαίνονται οι σχέσεις μεταξύ των δομών αυτών. Οι δομές δεδομένων είναι:

■ Business entities

Η δομή δεδομένων *businessEntity* αποτελεί δομή για πληροφορίες σχετικές με την εταιρεία που δημοσιεύει μια Υπηρεσία Διαδικτύου. Αυτές μπορεί να περιλαμβάνουν το όνομα της επιχείρησης, ορισμένες πληροφορίες επικοινωνίας, την κατηγορία της επιχείρησης και τις υπηρεσίες που προσφέρει.

■ Business services

Η δομή δεδομένων *businessService* αποτελεί δομή για την περιγραφή σε επιχειρηματικούς όρους κάθε μιας από τις υπηρεσίες που προσφέρονται από την

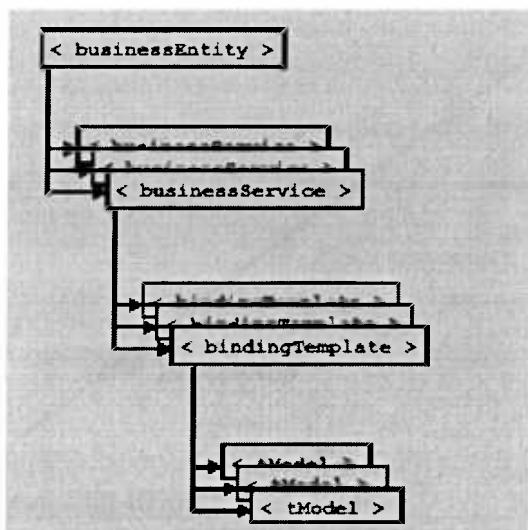
επιχείρηση. Απαιτεί τον καθορισμό του λάχιστον ενός ονόματος για την υπηρεσία και ενός τρόπου πρόσβασης στην υπηρεσία (binding template).

- Binding templates

Η δομή δεδομένων *bindingTemplates* αποτελείται από μια ή περισσότερες δομές *bindingTemplate*, που κάθε μία περιγράφει ένα τρόπο με τον οποίο μπορεί να αποκτηθεί πρόσβαση σε μια υπηρεσία.

- tModels

Η δομή δεδομένων *tModels* περιγράφει σε τεχνικό επίπεδο προδιαγραφές που επιτρέπουν στα δύο μέρη που μετέχουν στην επικοινωνία να διαπιστώσουν αν υπάρχει συμβατότητα μεταξύ τους. Κάθε WSDL έγγραφο καθορίζεται σε ένα tModel στοιχείο. Κάθε τέτοιο tModel στοιχείο χαρακτηρίζεται τύπου “wsdlSpec” και περιλαμβάνει ένα γνώρισμα <overviewDoc> που δείχνει στο αντίστοιχο WSDL έγγραφο.



Σχήμα 3.9.: UDDI XML Schema. [Günzer, 2002]

3.6.5. Διαδικασίες του μοντέλου των υπηρεσιών.

Στην ενότητα αυτή περιγράφονται οι διαδικασίες που πρέπει να υποστηρίζει το μοντέλο Υπηρεσιών Διαδικτύου και οι οποίες είναι:

- Δημοσίευση Υπηρεσίας.
- Ανακάλυψη Υπηρεσίας.
- Δέσμευση Υπηρεσίας.

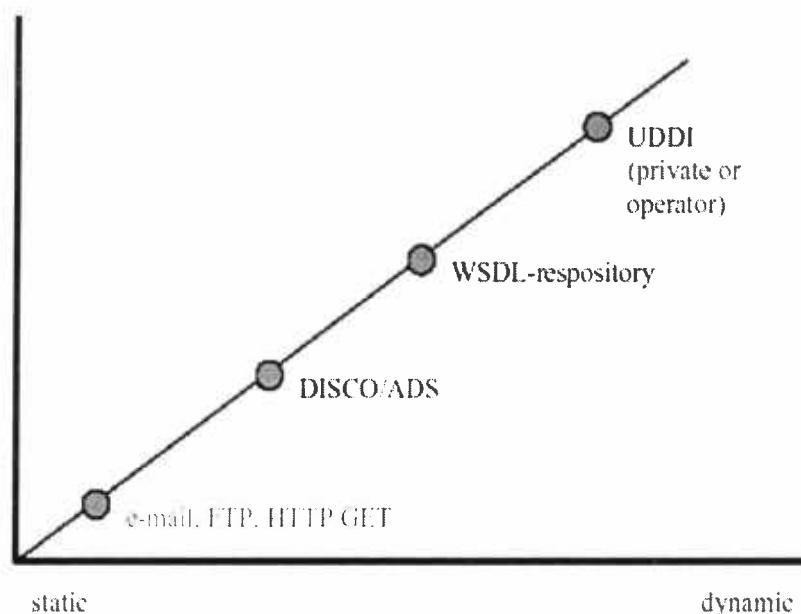
3.6.5.1. Δημοσίευση Υπηρεσιών.

Η δημοσίευση μιας Υπηρεσίας Διαδικτύου περιλαμβάνει τη διαδικασία της δημιουργίας της περιγραφής της υπηρεσίας και τη διαδικασία δημοσίευσης της περιγραφής αυτής [Kreger, 2001].

3.6.5.1.1.

Ένα WSDL αρχείο περιγραφής μιας υπηρεσίας γράφεται εξ' ολοκλήρου από τους προγραμματιστές ή παράγεται με τη χρήση κάποιου εργαλείου ή συντίθεται με βάση τον ορισμό που δίνεται για τη διεπαφή της υπηρεσίας από τα διεθνή πρότυπα, αν φυσικά υπάρχουν. Το ίδιο ισχύει σε γενικές γραμμές και για μια UDDI καταχώρηση.

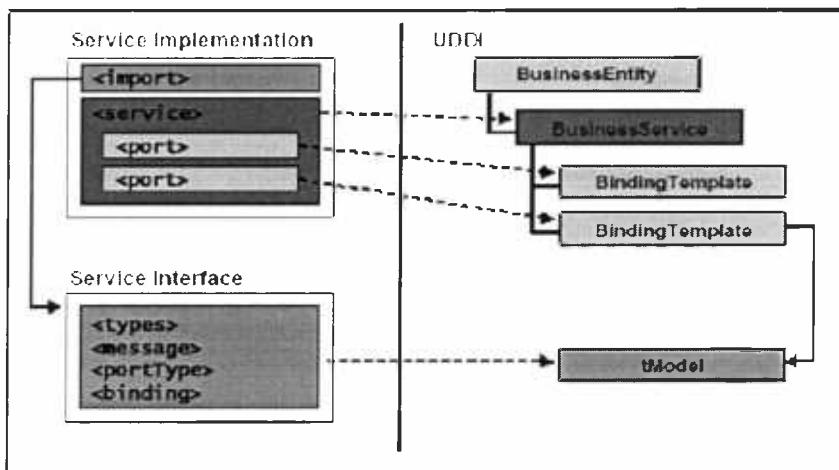
Η δημοσίευση της περιγραφής μιας υπηρεσίας μπορεί να γίνει με αρκετούς τρόπους. Στο σχήμα 3.10. παρουσιάζονται ορισμένοι από αυτούς (μετακίνηση πάνω στην ευθεία της γραφικής παράστασης προς τα δεξιά σημαίνει μετάβαση από ένα στατικό σε ένα πιο δυναμικό τρόπο δημοσίευσης της υπηρεσίας).



Σχήμα 3.10.: Τρόποι δημοσίευσης της περιγραφής μιας Υπηρεσίας. [Kreger, 2001]

Σύμφωνα με τη γραφική παράσταση ένας δυναμικός τρόπος δημοσίευσης της περιγραφής μιας υπηρεσίας είναι η καταχώρηση του WSDL αρχείου σε μια ιδιωτική UDDI registry ή στον κόμβο ενός UDDI operator. Γενικά, οι επιχειρήσεις που θέλουν να καταχωρήσουν το WSDL αρχείο με την περιγραφή μιας Υπηρεσίας Διαδικτύου σε ένα UDDI repository μπορούν να χρησιμοποιήσουν το SOAP API που παρέχει το ίδιο το UDDI. Στο σχήμα 3.11.

φαίνεται με ποιο τρόπο γίνεται η αντιστοίχηση της πληροφορίας ενός WSDL αρχείου σε ένα UDDI σχήμα.

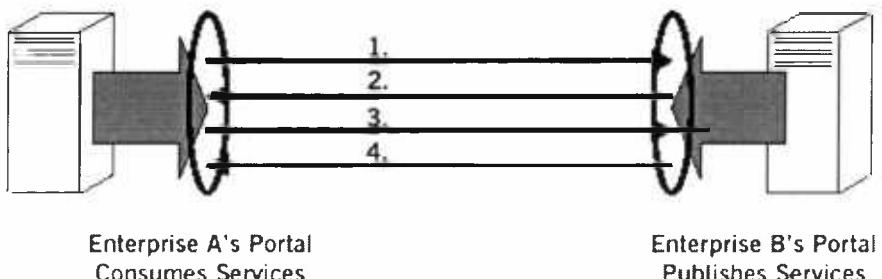


Σχήμα 3.11.: Δημιουργία UDDI καταχώρησης από ένα WSDL έγγραφο.

3.6.5.2. Ανακάλυψη Υπηρεσιών.

Η ανακάλυψη υπηρεσιών μπορεί να γίνει είτε στατικά με χρήση του πρωτοκόλλου SOAP, είτε δυναμικά μέσω ενός UDDI ευρετηρίου. Το σχήμα 3.12. δείχνει το μηχανισμό με τον οποίο επιτυγχάνεται στατικά η ανακάλυψη των υπηρεσιών μιας εταιρείας με χρήση SOAP.

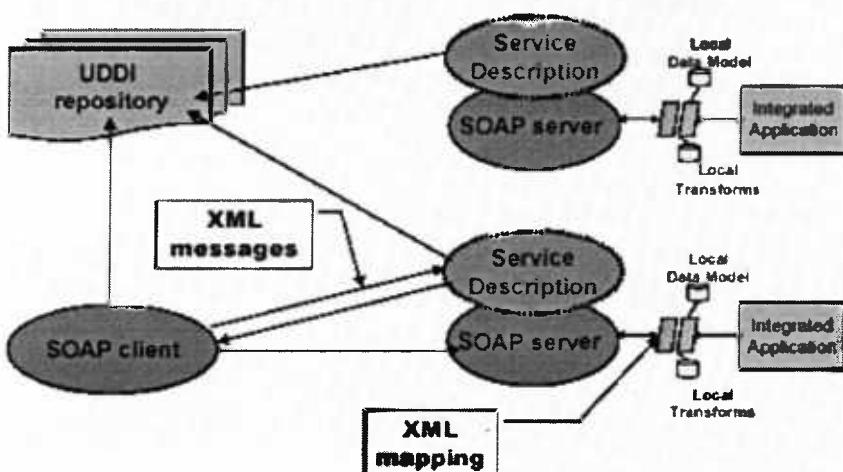
1. Η επιχείρηση Α χρησιμοποιεί ένα URL που παρέχεται από την επιχείρηση Β για να ανακτήσει μια λίστα με τις υπηρεσίες που δημοσιεύει η Β.
2. Η επιχείρηση Α «κατεβάζει» τα XML schemas (συνήθως σε WSDL) που περιγράφουν τη μορφή των μηνυμάτων που αναμένονται από τις υπηρεσίες της εταιρείας Β.
3. Η επιχείρηση Α σχηματίζει το ανάλογο XML μήνυμα και το αποστέλλει μέσω SOAP στην επιχείρηση Β.
4. Η επιχείρηση Β στέλνει μια απάντηση, μέσω SOAP, την οποία η επιχείρηση Α ερμηνεύει χρησιμοποιώντας την πληροφορία για το XML schema που έλαβε στο βήμα 2.



Σχήμα 3.12.: Στατική ανακάλυψη Υπηρεσιών Διαδικτύου.

Με αυτόν τον τρόπο, δύο επιχειρήσεις που δένονται πιθανότατα με κάποιο συμβόλαιο μπορούν να ανταλλάξουν πληροφορία για τις υπηρεσίες που παρέχουν ή επιθυμούν να καταναλώσουν.

Αντίθετα, η μέθοδος δυναμικής ανακάλυψης υπηρεσιών με χρήση του UDDI εξυπηρετεί τη συνεργασία δύο τυχαίων επιχειρήσεων, που δεν έχουν συνάψει στο παρελθόν κάποια εμπορική συμφωνία.



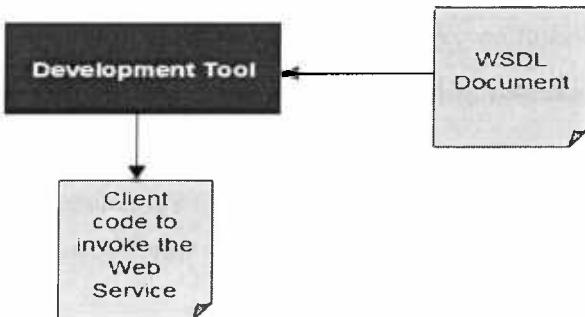
Σχήμα 3.13.: Δυναμική ανακάλυψη υπηρεσιών διαδικτύου. [Iona, 2002]

Στο σχήμα 3.13. φαίνεται πώς μια επιχείρηση μπορεί να αποκτήσει πρόσβαση στην Υπηρεσία Διαδικτύου μιας άλλης επιχείρησης με τη μέθοδο της δυναμικής ανακάλυψης. Το UDDI δημοσιεύει μια SOAP διεπαφή για να παρέχει πρόσβαση στους πιθανούς πελάτες των υπηρεσιών των επιχειρήσεων που φιλοξενεί. Ο πελάτης (SOAP client) πραγματοποιεί αναζήτηση στο UDDI ευρετήριο θέτοντας κάποια κριτήρια και ζητώντας, αν υπάρχουν, καταχωρημένα αρχεία (XML αρχεία) επιχειρήσεων που πληρούν τα κριτήρια του. Αν βρει έστω και ένα τέτοιο αρχείο (για κάποια επιχείρηση) μπορεί να προσπελάσει το tModel που δείχνει στο WSDL αρχείο της υπηρεσίας που τον ενδιαφέρει. Από το σημείο αυτό και μετά ο

SOAP client επικοινωνεί απ' ευθείας με το SOAP server που φιλοξενεί την υπηρεσία, μέσω SOAP μηνυμάτων που δημιουργεί με βάση τις προδιαγραφές που ορίζονται από το WSDL έγγραφο.

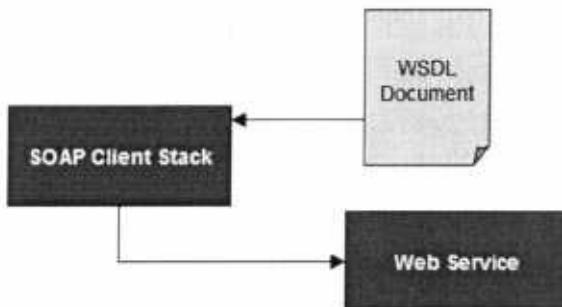
3.6.5.3. Δέσμευση Υπηρεσιών.

Η δέσμευση των Υπηρεσιών Διαδικτύου μιας εταιρείας από έναν πελάτη μπορεί να γίνει στατικά ή δυναμικά. Ουσιαστικά, αυτό εξαρτάται από τη φάση του κύκλου ζωής της εφαρμογής του πελάτη κατά την οποία λαμβάνονται οι πληροφορίες δέσμευσης (binding information) της υπηρεσίας. Όταν ο πελάτης λαμβάνει υπόψη του τις πληροφορίες δέσμευσης μιας υπηρεσίας κατά το σχεδιασμό της εφαρμογής του, η δέσμευση της υπηρεσίας γίνεται στατικά. Στο σχήμα 3.14. [Shohoud, 2003] φαίνεται πώς ένα WSDL έγγραφο χρησιμοποιείται κατά τη φάση ανάπτυξης μιας εφαρμογής πελάτη από το εργαλείο ανάπτυξης (π.χ. wsdl.exe).



Σχήμα 3.14.: Ανάπτυξη εφαρμογής πελάτη για τη στατική δέσμευση μιας Υ.Δ..

Όταν οι πληροφορίες δέσμευσης μιας Υπηρεσίας Διαδικτύου λαμβάνονται κατά το χρόνο λειτουργίας της εφαρμογής (run time), η δέσμευση της υπηρεσίας γίνεται δυναμικά. Στο σχήμα 3.15. [Shohoud, 2003] περιγράφεται η περίπτωση αυτή.



Σχήμα 3.15.: Δημιουργία μηνύματος για τη δυναμική δέσμευση μιας Υ.Δ. από ένα πελάτη.

3.7. Συμπέρασμα.

Η γλώσσα XML είναι αναμφισβήτητα σήμερα η βάση για την ανάπτυξη Υπηρεσιών Διαδικτύου, αφού αποτελεί το πρότυπο μέσω του οποίου εξασφαλίζεται η συμφωνία, σε μια απλή μορφή περιγραφής δεδομένων, για την ανταλλαγή μηνυμάτων μέσω των ήδη υπαρχόντων πρωτοκόλλων του διαδικτύου. Τα πρωτόκολλα SOAP και HTTP είναι ικανά να ικανοποιήσουν την ανάγκη για διαλειτουργικότητα μεταξύ εφαρμογών, που βρίσκονται στο διαδίκτυο, υποστηρίζοντας την ανταλλαγή XML μηνυμάτων. Επίσης, επαρκής κρίνεται και η γλώσσα περιγραφής των υπηρεσιών WSDL, η οποία καθορίζει τις προδιαγραφές για τα μηνύματα που αποτελούν το μέσο της επικοινωνίας του πελάτη με το χορηγό της υπηρεσίας. Εντούτοις, υπάρχουν ακόμα πολλές ελλείψεις προκειμένου να καλυφθεί ολόκληρο το φάσμα των απαιτήσεων που εισάγει το ηλεκτρονικό επιχειρείν. Οι υπάρχουσες τεχνολογίες πρέπει να επεκταθούν προκειμένου να καλυφθούν ζητήματα όπως η ασφάλεια των υπηρεσιών, η αξιοπιστία στην ανταλλαγή των μηνυμάτων, η απαίτηση για βελτίωση της ποιότητα των υπηρεσιών και η ανάγκη διαχείρισης των επίπεδων της στοίβας των υπηρεσιών διαδικτύου. Πρόσθετες απαιτήσεις τέλος, είναι και αυτές που επιβάλουν τη βελτίωση των υποδομών στο διαδίκτυο. Αυτές περιλαμβάνουν την υποστήριξη ευφυούς συμπεριφοράς των υπηρεσιών ανάλογα με την κατάσταση του περιβάλλοντος, την υποστήριξη τρίτων οντοτήτων³⁴, τη δυνατότητα ενσωμάτωσης εφαρμογών ή πληροφορίας που είναι διαθέσιμες μέσω υπηρεσιών διαδικτύου σε portlets³⁵ και την ανάγκη διαχείρισης των ροών των υπηρεσιών.

³⁴ για παράδειγμα μιας υπηρεσίας διαδικτύου που θα έχει τον ρόλο της ενδιάμεσης οντότητας η οποία θα υποστηρίζει την μη αποποίηση (non repudiation) του πελάτη.

³⁵ περιοχές ορθογωνίου σχήματος σε μια ιστοσελίδα που εμφανίζεται εξατομικευμένη πληροφορία από πολλές πηγές.

ΚΕΦΑΛΑΙΟ 4^ο : ΑΝΑΠΤΥΞΗ ΥΠΗΡΕΣΙΩΝ ΔΙΑΔΙΚΤΥΟΥ ΒΑΣΙΣΜΕΝΩΝ ΣΕ XML

4.1. Εισαγωγή.

Στο προηγούμενο κεφάλαιο έγινε μια σύντομη περιγραφή των τεχνολογιών XML, SOAP, WSDL και UDDI. Οι τεχνολογίες αυτές, μολονότι δεν αποτελούν τη μοναδική πρόταση στο χώρο των Υπηρεσιών Διαδικτύου, θεωρούνται σήμερα από την πλειοψηφία των ειδικών ως η καλύτερη επιλογή για τη σύνθεση τέτοιου είδους υπηρεσιών. Ο βασικότερος λόγος είναι, ότι οι τεχνολογίες αυτές απολαμβάνουν την αποδοχή των μεγαλύτερων εταιρειών που κατασκευάζουν λογισμικό σήμερα. Χαρακτηριστικό είναι το γεγονός, ότι εταιρείες όπως η Microsoft και η Sun Microsystems συμφώνησαν τόσο στη χρησιμότητα των εν λόγω τεχνολογιών όσο και στην πρόβλεψη ότι θα αποτελέσουν στο μέλλον τη βάση για την ανάπτυξη των περισσοτέρων εφαρμογών.

Στο κεφάλαιο αυτό δίνεται μια συνοπτική περιγραφή των διαφορετικών προσεγγίσεων που υπάρχουν από την πλευρά των μεγάλων εταιρειών πληροφορικής στο θέμα της ανάπτυξης Υπηρεσιών Διαδικτύου. Μεγαλύτερη έμφαση δίνεται σε δύο μοντέλα ανάπτυξης Υπηρεσιών Διαδικτύου, που είναι και τα δημοφιλέστερα σήμερα. Το .NET, που υποστηρίζεται από την εταιρεία Microsoft, και το J2EE, που είναι το μοντέλο ανάπτυξης που υποστηρίζουν αρκετές εταιρείες με επικεφαλής την εταιρεία Sun Microsystems.

4.2. Μοντέλα ανάπτυξης Υπηρεσιών Διαδικτύου.

Με την αναγγελία των Υπηρεσιών Διαδικτύου, αρκετοί οργανισμοί και κυρίως οι μεγάλοι προμηθευτές που δραστηριοποιούνται στο χώρο των τεχνολογιών, ξεκίνησαν τις προσπάθειες τους με σκοπό να προσαρμόσουν την υπάρχουσα τεχνολογική τους υποδομή στις απαιτήσεις της νέας εποχής. Μέχρι στιγμής, ανάμεσα στα αποτελέσματα των προσπαθειών αυτών, ξεχωρίζουν δύο σημαντικά μοντέλα ανάπτυξης εφαρμογών, τα οποία ενσωματώνουν τη δυνατότητα ανάπτυξης Υπηρεσιών Διαδικτύου. Τα δύο αυτά μοντέλα είναι το Microsoft .NET και το Java 2 Enterprise Edition (J2EE).

Το .NET είναι προϊόν της εταιρείας Microsoft και αποτελεί εξελιγμένο απόγονο του Windows DNA, που ήταν η προηγούμενη πλατφόρμα της Microsoft για την ανάπτυξη εφαρμογών που καλύπτουν επιχειρησιακές ανάγκες. Το .NET ανάμεσα στις πολλές δυνατότητες που προσφέρει, επιτρέπει σε μια επιχείρηση να δημιουργήσει δικές της Υπηρεσίες Διαδικτύου βασισμένες στο XML πρότυπο. Η υποστήριξη Υπηρεσιών Διαδικτύου

στην περίπτωση του .NET είναι το αποτέλεσμα αναθεώρησης ενός σημαντικού μέρους της Microsoft υποδομής.

Το J2EE είναι πρότυπο που σχεδιάστηκε για την απλοποίηση σύνθετων προβλημάτων που σχετίζονται με την ανάπτυξη, επέκταση και διαχείριση multi-tier εφαρμογών. Αποτελεί πρωτοβουλία μιας ομάδας εταιρειών που έχει ως επικεφαλής την εταιρεία Sun Microsystems. Με βάση τις προδιαγραφές που ορίζει το πρότυπο, η Sun Microsystems και άλλες εταιρείες ανάμεσα στις οποίες και οι IBM, BEA και Oracle, έχουν υλοποιήσει προϊόντα που χρησιμοποιούνται για την ανάπτυξη εφαρμογών, συμπεριλαμβανομένων και Υπηρεσιών Διαδικτύου. Στην περίπτωση του J2EE, η υποστήριξη της ανάπτυξης Υπηρεσιών Διαδικτύου πραγματοποιήθηκε απλά με την επέκταση μιας ήδη αποδεδειγμένης αρχιτεκτονικής, χρησιμοποιώντας ένα σύνολο από πρότυπα που ονομάζονται Java APIs for XML.

Σήμερα, ο ανταγωνισμός ανάμεσα στα δύο μοντέλα ανάπτυξης είναι έντονος, αφού αποτελούν στην ουσία τις δύο εναλλακτικές επιλογές για κάθε επιχείρηση, ενώ παρέχουν σχεδόν και τις ίδιες δυνατότητες. Τα .NET και J2EE έχουν σχεδιαστεί και τα δύο για να εκμεταλλευτούν νέες δυνατότητες που μπορεί να προσφέρει το Internet και στηρίζονται σε παρόμοιες αρχές αρχιτεκτονικής σχεδίασης. Ωστόσο, υπάρχει μια βασική διαφορά στη φιλοσοφία των δύο μοντέλων, η οποία σχετίζεται και με τον τρόπο με τον οποίο φαίνεται πως αντιμετωπίζουν τον ανταγωνισμό. Το J2EE στοχεύει στην ευρεία αποδοχή του στην αγορά, στηριζόμενο σε ανοικτά πρότυπα. Αντίθετα, το .NET επιδιώκει την ευρεία αποδοχή του στην αγορά στηρίζοντας παράλληλα την πολιτική της Microsoft που επιδιώκει την επικράτηση ενός λειτουργικού συστήματος (Microsoft Windows). Το επικίνδυνο σημείο μιας τέτοιας πολιτικής σε ότι αφορά ένα χρήστη ή μια επιχείρηση είναι να υποστεί «κλείδωμα» (lock-in) στον συγκεκριμένο προμηθευτή. Όπως φαίνεται όμως, οι αποφάσεις, που έχουν παρθεί από τις μεγάλες εταιρείες, κινούνται προς την κατεύθυνση της αποφυγής ενός τέτοιου σεναρίου.

Η ίδρυση³⁶ του ανεξάρτητου οργανισμού WS-I (Web Services Interoperability Organization), έπειτα από συνεννόηση των εταιρειών IBM, BEA Systems και Microsoft ουσιαστικά εξασφαλίζει τη διαλειτουργικότητα μεταξύ διαφορετικών υλοποιήσεων των Υπηρεσιών Διαδικτύου, καθώς και τη συμμόρφωση σε συγκεκριμένα πρότυπα.

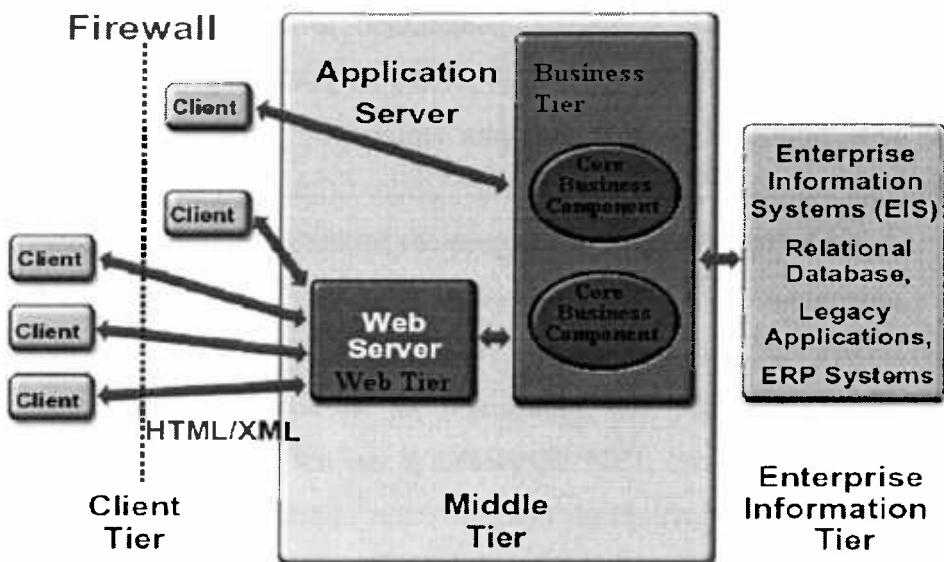
³⁶ “Consortium to Promote Strategy to Foster New Online Services”, New York Times, February 6, 2002.



4.3. Η αρχιτεκτονική των μοντέλων ανάπτυξης .NET και J2EE.

Η αρχιτεκτονική των Web Service εφαρμογών βασίζεται στο μοντέλο ανάπτυξης των τριών επιπέδων (3-tier architecture) [Mariucci, 2000]. Αυτό σημαίνει ότι η λογική των εφαρμογών είναι διανεμημένη σε στοιχεία (components), που καθένα εκτελείται σε μια από τις τρεις διαφορετικές τοποθεσίες που περιλαμβάνονται στην αρχιτεκτονική. Στο σχήμα 4.1. δίνεται η γενική περιγραφή της αρχιτεκτονικής του μοντέλου ανάπτυξης εφαρμογών στην πλατφόρμα .NET, αλλά και σε πλατφόρμες που στηρίζονται στις προδιαγραφές του J2EE. Τα επίπεδα της αρχιτεκτονικής είναι:

- Client tier. Το επίπεδο αυτό περιλαμβάνει τα components της εφαρμογής που εκτελούνται στη μηχανή του πελάτη της υπηρεσίας. Είναι υπεύθυνο για την επικοινωνία του χρήστη με το επίπεδο Middle tier και παρέχει σε αυτόν ένα γραφικό περιβάλλον ελέγχου των λειτουργιών.
- Middle tier. Το επίπεδο αυτό περιλαμβάνει components που εκτελούνται στη μηχανή που βρίσκεται ο Application Server της εφαρμογής (Windows 2000 Server ή J2EE Server αντίστοιχα). Στο Middle tier τοποθετείται η επιχειρησιακή λογική (business logic) της εφαρμογής, που είναι το τμήμα του κώδικα που εξυπηρετεί το σκοπό για τον οποίο αναπτύχθηκε η εφαρμογή, σε αντιδιαστολή με το τμήμα του κώδικα που παρέχει υποδομή και σύνδεση στην εφαρμογή. Το Middle tier χωρίζεται σε δύο επίπεδα, το Web tier και το Business tier. Το Web tier υποστηρίζει το Client tier επιτρέποντας την έμμεση πρόσβαση του πελάτη στα επίπεδα Business tier και Enterprise Information System tier. Στο Business tier τοποθετείται η βασική επιχειρησιακή λογική (core business logic) της εφαρμογής, που αφορά στη διαχείριση της συναλλαγής, σε επιχειρηματικούς κανόνες, στην ταυτόχρονη υποστήριξη πελατών κ.ά.
- Enterprise Information System (EIS) tier. Το επίπεδο αυτό περιλαμβάνει components που εκτελούνται στη μηχανή κάποιου Database Server ή κάποιου legacy συστήματος. Είναι υπεύθυνο για τη διαχείριση κοινών πόρων και την εξασφάλιση της φυσικής πρόσβασης σε αυτούς.



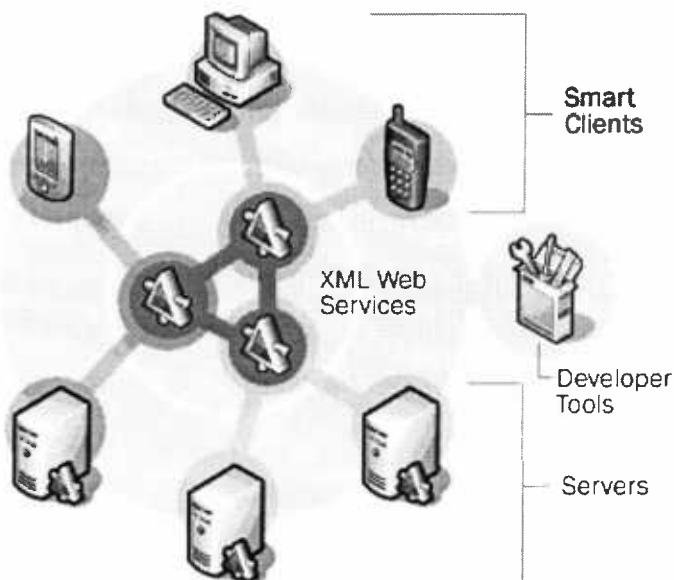
Σχήμα 4.1.: Αρχιτεκτονική Web Service εφαρμογών.

4.4. Λεπτομερής Περιγραφή του .NET.

Το Microsoft .NET είναι ένα προϊόν λογισμικού, που επεκτείνει την ιδέα του Internet και του λειτουργικού συστήματος μετατρέποντας το ίδιο το Internet σε βάση ενός νέου λειτουργικού συστήματος. Αυτό επιτρέπει, ουσιαστικά, στους προγραμματιστές να δημιουργούν προγράμματα που ξεπερνούν τα όρια των μηχανών στα οποία εκτελούνται και να χρησιμοποιούν σε όλη της την έκταση τη δυνατότητα σύνδεσης του Internet στις εφαρμογές τους. Τα βασικά συστατικά του Microsoft .NET (Σχήμα 4.2.) είναι:

1. Servers. Στους servers συγκαταλέγονται όλοι οι servers της οικογένειας Microsoft Windows 2000 και οι .NET Enterprise Servers, (π.χ. Microsoft BizTalk Server) που έχουν δημιουργηθεί για την ανάπτυξη και διαχείριση υπηρεσιών διαδικτύου που βασίζονται στην XML.
2. Developer Tools. Στα εργαλεία ανάπτυξης .NET εφαρμογών ανήκει: α) το μοντέλο προγραμματισμού .NET Framework, που επιτρέπει στους προγραμματιστές να γράψουν εφαρμογές, οι οποίες μπορούν να δημοσιευτούν στο διαδίκτυο, παρέχοντας πρόσβαση στη λειτουργικότητά τους σε προγραμματιστές άλλων εφαρμογών, μέσω πρωτοκόλλων όπως το SOAP και το HTTP, β) το Visual Studio .NET, το οποίο παρέχει ένα ενοποιημένο περιβάλλον ανάπτυξης εφαρμογών για τον προγραμματισμό με το .NET Framework.

3. XML Web Services. Είναι θεμελιώδεις Υπηρεσίες Διαδικτύου, που μπορούν να χρησιμοποιηθούν από άλλες υπηρεσίες διαδικτύου ή να «καταναλωθούν» άμεσα από έξυπνες client συσκευές. Μια τέτοια υπηρεσία είναι το MapPoint .NET που παρέχει ταξιδιωτικές πληροφορίες, υψηλής ποιότητας χάρτες κ.ά. Οι υπηρεσίες αυτές προσφέρονται από την Microsoft και τους εμπορικούς συνεργάτες της.
4. Smart Client software. Έξυπνες χαρακτηρίζονται όλες οι συσκευές που μπορούν και «καταναλώνουν», δηλαδή χρησιμοποιούν, XML Υπηρεσίες Διαδικτύου. Η Microsoft, κάνοντας το πρώτο βήμα με τη δημιουργία των Microsoft Windows XP, των Windows XP Embedded και των Windows CE .NET, έχει δημιουργήσει και συνεχίζει να δημιουργεί μια νέα γενιά λογισμικού client για έξυπνες συσκευές.



Σχήμα 4.2.: Τα συστατικά του Microsoft .NET. [MS .NET]

Στη συνέχεια αναλύονται περισσότερο τα συστατικά της τεχνολογίας .NET που έχουν ιδιαίτερη σημασία για την ανάπτυξη Υπηρεσιών Διαδικτύου.

4.4.1. .NET Framework.

Το .NET Framework είναι ένα πολυγλωσσικό περιβάλλον ανάπτυξης και εκτέλεσης στοιχείων (.NET managed components). Η έννοια «στοιχείο» είναι δανεισμένη από το μοντέλο λογισμικού Component Object Model (COM) της Microsoft και σημαίνει τμήμα κώδικα πολλαπλής χρήσης, που καλύπτει από απλές λειτουργίες μέχρι και ολόκληρες

εφαρμογές. Στο .NET Framework, όλα τα στοιχεία μπορούν να είναι υπηρεσίες διαδικτύου, αν και οι υπηρεσίες διαδικτύου είναι απλά ένα είδος στοιχείων. Το .NET Framework αποτελείται από τρία κύρια μέρη [Layman et al., 2001]:

- Το περιβάλλον χρόνου εκτέλεσης κοινής γλώσσας (Common Language Runtime).
- Ένα ιεραρχικό σύνολο ενοποιημένων βιβλιοθηκών κλάσεων.
- Μια προηγμένη έκδοση των Active Server Pages, που ονομάζεται ASP.NET.

Το περιβάλλον χρόνου εκτέλεσης κοινής γλώσσας (CLR) αφορά στο χρόνο ανάπτυξης και εκτέλεσης ενός στοιχείου. Κατά την εκτέλεση του στοιχείου, το περιβάλλον χρόνου εκτέλεσης είναι υπεύθυνο για τη διαχείριση της εκχώρησης μνήμης, την εκκίνηση και τον τερματισμό νημάτων και διεργασιών, την εφαρμογή της πολιτικής ασφαλείας, καθώς και την ικανοποίηση κάποιων εξαρτήσεων που μπορεί να έχει το στοιχείο αυτό σε άλλα στοιχεία. Κατά το χρόνο ανάπτυξης, ο ρόλος του CLR αλλάζει λίγο. Επειδή αυτοματοποιεί πολλές εργασίες (όπως τη διαχείριση της μνήμης), το περιβάλλον χρόνου εκτέλεσης απλοποιεί κατά πολύ την εμπειρία του προγραμματιστή, ιδιαίτερα σε σύγκριση με το COM. Επιπλέον, συντελεί στη σημαντική μείωση του όγκου του κώδικα που πρέπει να συντάξει ένας προγραμματιστής, για να μετατρέψει μια επιχειρησιακή λογική σε στοιχείο που μπορεί να χρησιμοποιηθεί ξανά. Το πιο σημαντικό όμως για το .NET Framework είναι το γεγονός ότι παρέχει κοινό περιβάλλον χρόνου εκτέλεσης για όλες τις γλώσσες προγραμματισμού. Αυτό είναι ιδιαίτερα σημαντικό να σκεφτεί κανείς ότι σχεδόν όλες οι γλώσσες προγραμματισμού έχουν περιβάλλον χρόνου εκτέλεσης³⁷.

Οι κλάσεις του Πλαισίου .NET παρέχουν ένα ενοποιημένο, ιεραρχικό σύνολο από βιβλιοθήκες κλάσεων (API), προσανατολισμένο σε αντικείμενα και με δυνατότητες επέκτασης για χρήση από τους προγραμματιστές. Δημιουργώντας ένα κοινό σύνολο API σε όλες τις γλώσσες προγραμματισμού, το .NET Framework επιτρέπει τη μεταβίβαση, το χειρισμό και τον εντοπισμό σφαλμάτων μεταξύ των γλωσσών. Έτσι, όλες οι γλώσσες προγραμματισμού, από την JScript έως την C++, εξισώνονται και οι προγραμματιστές είναι ελεύθεροι να επιλέξουν τη γλώσσα που θέλουν να χρησιμοποιήσουν.

Οι ASP.NET σελίδες στηρίζονται στις κλάσεις προγραμματισμού του .NET Framework, και παρέχουν ένα μοντέλο εφαρμογής, με τη μορφή ενός συνόλου στοιχείων ελέγχου και υποδομής, το οποίο απλοποιεί τη δημιουργία διαδικτυακών εφαρμογών. Συγκεκριμένα, η

³⁷ Το σύστημα προγραμματισμού της Visual Basic έχει χρόνο εκτέλεσης (που ονομάζεται VBRUN), η Visual C++ έχει χρόνο εκτέλεσης (MSVCRT), το ίδιο και η Visual FoxPro, η Jscript, η SmallTalk, η Perl, η Python και η Java.

τεχνολογία ASP.NET επιτρέπει, όπως και η ASP, τη δημιουργία δυναμικών ιστοσελίδων με την εισαγωγή ερωτημάτων που εκτελούνται σε μια σχεσιακή βάση δεδομένων, όμως προσφέρει και επιπλέον δυνατότητες. Η ASP.NET τεχνολογία υποστηρίζει την ανταλλαγή SOAP μηνυμάτων μέσω του πρωτοκόλλου HTTP, παρέχοντας τη δυνατότητα αυτόματης δημιουργίας αρχείων WSDL για τις υπηρεσίες διαδικτύου. Αυτό καθιστά δυνατή την υλοποίηση ενός web service listener, ο οποίος παρέχει στους πελάτες πρόσβαση στις .NET υπηρεσίες. Ουσιαστικά λοιπόν, ο ρόλος της ASP.NET τεχνολογίας είναι να διευκολύνει τους προγραμματιστές στο να μπορούν να παρέχουν το λογισμικό ως υπηρεσία. Χρησιμοποιώντας τις δυνατότητες υπηρεσιών διαδικτύου της ASP.NET, οι προγραμματιστές μπορούν απλώς να συντάξουν την επιχειρησιακή τους λογική και η υποδομή ASP.NET αναλαμβάνει την παροχή αυτής της υπηρεσίας μέσω του SOAP.

4.4.2. Microsoft Visual Studio .NET.

Το Visual Studio .NET παρέχει ένα σύγχρονο και πλούσιο σε δυνατότητες περιβάλλον προγραμματισμού, προσφέροντας στους προγραμματιστές τα εργαλεία για την ενοποίηση λύσεων σε πολλά λειτουργικά συστήματα και γλώσσες. Με το Visual Studio .NET [MS .NET], οι προγραμματιστές μπορούν να μετατρέψουν εύκολα μια υπάρχουσα επιχειρησιακή λογική σε υπηρεσίες διαδικτύου βασισμένες σε XML, συγκεντρώνοντας διαδικασίες και καθιστώντας τις διαθέσιμες σε οποιαδήποτε πλατφόρμα. Επίσης, οι προγραμματιστές μπορούν να ενσωματώσουν εύκολα άλλες υπηρεσίες διαδικτύου που περιλαμβάνονται και είναι διαθέσιμες σε ανεξάρτητους καταλόγους UDDI.

Τέλος, τα ενσωματωμένα εργαλεία ADO.NET διευκολύνουν την αποστολή XML μηνυμάτων μεταξύ της εφαρμογής και μιας αποθήκης δεδομένων (π.χ. βάση δεδομένων του SQL Server ή της Oracle). Αυτό επιτυγχάνεται μέσω μιας όχι μόνιμης σύνδεσης, που χαρακτηρίζεται από έξυπνη διαχείριση της κατάστασης.

4.4.3. .NET Enterprise Servers.

Στην οικογένεια των .NET εξυπηρετητών περιλαμβάνονται οι παρακάτω [Warren et al. 2001]:



- Ο Microsoft Application Center 2000, που υποστηρίζει την ανάπτυξη και διαχείριση Internet εφαρμογών με υψηλό βαθμό διαθεσιμότητας και κλιμάκωσης.
- Ο Microsoft BizTalk Server 2002, που υποστηρίζει την ανάπτυξη XML-based υπηρεσιών, που στηρίζονται σε ανοιχτά πρότυπα, όπως είναι το SOAP.
- Ο Microsoft Commerce Server 2002, που αποτελεί μια γρήγορη λύση για την ανάπτυξη εφαρμογών ηλεκτρονικού εμπορίου.
- Ο Microsoft Content Management Server 2001 που επιτρέπει τη διαχείριση περιεχόμενου στις δυναμικές ιστοσελίδες μιας ηλεκτρονικής επιχείρησης.
- Ο Microsoft Exchange Server 2000, που επιτρέπει τη μετάδοση μηνυμάτων και τη συνεργασία εφαρμογών οπουδήποτε και οποτεδήποτε.
- Ο Microsoft Host Integration Server 2000, που λειτουργεί ως γέφυρα δεδομένων και εφαρμογών με legacy συστήματα.
- Ο Microsoft Internet Security and Acceleration Server 2000, που υποστηρίζει τη γρήγορη και ασφαλή σύνδεση με το Διαδίκτυο.
- Ο Microsoft Mobile Information 2001 Server, που χρησιμοποιείται για την υποστήριξη εφαρμογών σε κινητές συσκευές.
- Ο Microsoft SharePoint Portal Server 2001, που επιτρέπει στις επιχειρήσεις να αναζητούν, να μοιράζονται και να δημοσιεύουν πληροφορίες.
- Ο Microsoft SQL Server 2000, που επιτρέπει την αποθήκευση, την ανάκτηση και την ανάλυση της δομημένης XML πληροφορίας.

4.4.4. .NET Passport.

Το .NET Passport είναι μια υπηρεσία η οποία επιτρέπει στους χρήστες να δημιουργήσουν ένα μοναδικό όνομα εισόδου και έναν κωδικό πρόσβασης για χρήση σε όλες τις τοποθεσίες και τις υπηρεσίες που συμμετέχουν στο .NET Passport [MS .NET]. Με τον τρόπο αυτό η Microsoft προσφέρει ένα κοινό περιβάλλον στο οποίο μπορούν να βασιστούν άλλες υπηρεσίες διαδικτύου, προκείμενου να λαμβάνουν τα απαραίτητα διαπιστευτήρια³⁸ που τους εξασφαλίζουν επαρκή ασφάλεια.

Το .NET Passport εκχωρεί ένα μοναδικό αναγνωριστικό σε κάθε λογαριασμό κατά την εγγραφή. Πρόκειται για ένα μοναδικό αριθμό μήκους 64 bit τον οποίο αποστέλλει η υπηρεσία σε κάθε συμμετέχουσα τοποθεσία στην οποία εισέρχεται ένας πελάτης. Με την εγγραφή του

³⁸ πληροφορία η οποία χρησιμοποιείται για να αποδειχθεί η ταυτότητα μιας οντότητας σε μια άλλη.

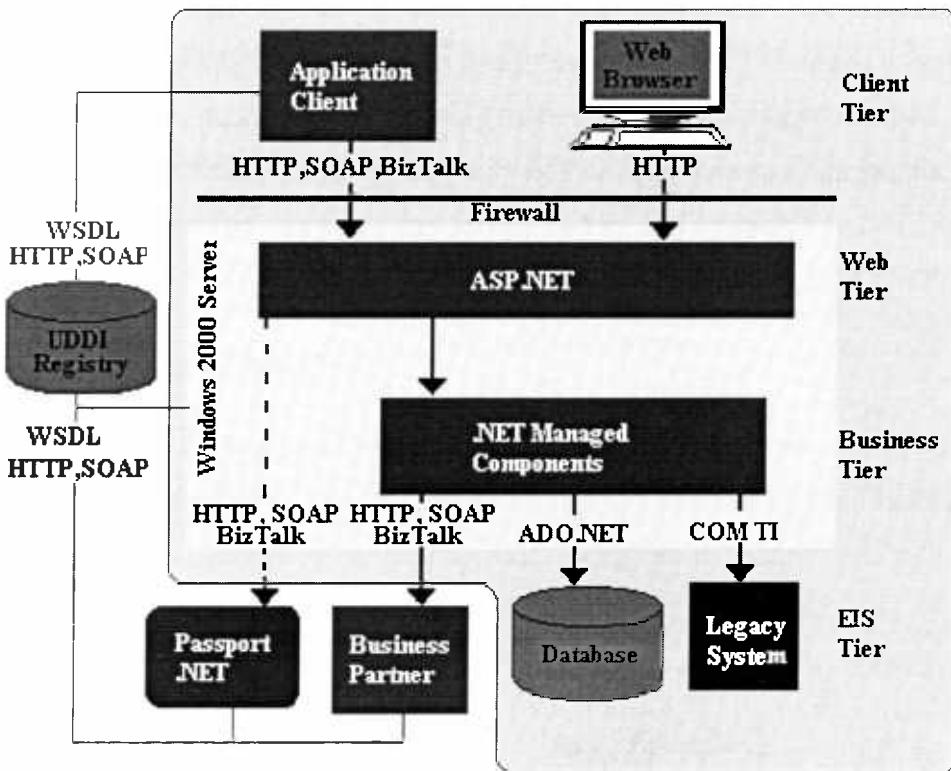


σε κάθε συμμετέχουσα τοποθεσία, ο πελάτης πρέπει να συμπληρώσει μια δήλωση προστασίας του ιδιωτικού απορρήτου, στην οποία καθορίζει τον τρόπο με τον οποίο επιθυμεί να χρησιμοποιηθούν οι πληροφορίες που συλλέγονται για αυτόν.

Στόχος της Microsoft είναι να προσφέρει μέσα στο έτος 2003 την υπηρεσία Passport .NET ως Υπηρεσία Διαδικτύου, έτσι ώστε να μπορεί να καλείται μέσω του πρωτοκόλλου SOAP. Με αυτό τον τρόπο ελπίζει πως θα απαλλάξει τους χορηγούς των υπηρεσιών διαδικτύου από την ενσωμάτωση μηχανισμών αυθεντικοποίησης στην επιχειρησιακή λογική των υπηρεσιών τους.

4.4.5. Αρχιτεκτονική .NET υπηρεσίας διαδικτύου.

Όσα αναφέρθηκαν στην ενότητα αυτή συνθέτουν τη συνολική εικόνα της αρχιτεκτονικής μιας .NET υπηρεσίας διαδικτύου (Σχήμα 4.3.).



Σχήμα 4.3.: Αρχιτεκτονική .NET υπηρεσίας.

To Business tier της υπηρεσίας αποτελείται από τμήματα κώδικα που ονομάζονται .NET Managed Components. Με χρήση των εργαλείων ADO.NET το Business tier συνδέεται με τη βάση δεδομένων (π.χ. βάση SQL server 2000), ενώ δίνεται και η δυνατότητα σύνδεσης του με legacy συστήματα (π.χ. Mainframe systems), μέσω της υπηρεσίας COM Transaction

Integrator του Microsoft Host Integration Server 2000. Η .NET υπηρεσία μπορεί να ενσωματώνει τη λειτουργία κάποιας άλλης Υπηρεσίας Διαδικτύου, που έχει αναπτυχθεί από κάποιον εμπορικό συνεργάτη. Συγκεκριμένα, το Business tier της εφαρμογής αποστέλλει SOAP ή BizTalk μηνύματα που πραγματοποιούν κλήση διαδικασιών της απομακρυσμένης υπηρεσίας, μέσω του HTTP πρωτοκόλλου. Τα BizTalk είναι XML μηνύματα, που έχουν την ίδια δομή με τα SOAP μηνύματα, αλλά περιέχουν περισσότερη πληροφορία για την πραγματοποίηση μιας συναλλαγής.

Η επικοινωνία μιας client εφαρμογής με το Web Tier της υπηρεσίας γίνεται μέσω SOAP ή BizTalk μηνυμάτων που χρησιμοποιούν το πρωτόκολλο HTTP. Το επίπεδο Web tier περιλαμβάνει την τεχνολογία ASP.NET, που όπως ήδη αναφέρθηκε αναλαμβάνει την παροχή μιας .NET υπηρεσίας στους πελάτες. Η Microsoft έχει ανακοινώσει ότι μέσα στο 2003 η υπηρεσία .NET Passport θα επεκταθεί, προκειμένου να υποστηρίξει το πρωτόκολλο SOAP, παρέχοντας την δυνατότητα σε μια .NET υπηρεσία να παρέχει τις υπηρεσίες του .NET Passport στους πελάτες της.

Τέλος, η τεχνολογία WSDL επιτρέπει τη δημοσίευση μιας .NET υπηρεσίας σε ένα UDDI κατάλογο, προκειμένου να μπορεί εύκολα να αναζητηθεί και να ανακαλυφθεί από έναν πελάτη. Το UDDI επιτρέπει την πρόσβαση στο WSDL έγγραφο μιας υπηρεσίας το οποίο παρέχει την απαραίτητη πληροφορία για την κατάλληλη σύνταξη των XML μηνυμάτων.

4.5. Λεπτομερής Περιγραφή του J2EE.

Το πρότυπο Java 2 Enterprise Edition (J2EE) αποτελεί ένα σύνολο συντονισμένων προδιαγραφών και πρακτικών, με στόχο τον καθορισμό μιας βασικής υποδομής (core infrastructure) και ενός μοντέλου αρχιτεκτονικής (component model) για την ανάπτυξη Internet εφαρμογών. Τα κύρια συστατικά του J2EE προτύπου είναι τα εξής:

- J2EE Application Programming Model. Είναι ένα πρότυπο μοντέλο προγραμματισμού για την ανάπτυξη multi-tier εφαρμογών.
- J2EE Platform. Είναι ένα πρότυπο περιβάλλον ανάπτυξης εφαρμογών που περιλαμβάνει ένα σύνολο από πρότυπα που πρέπει να υποστηρίζει κάθε J2EE πλατφόρμα ανάπτυξης εφαρμογών. Συγκεκριμένα, πρέπει να υποστηρίζονται όλα τα πρότυπα της Java (Java APIs), τα πρότυπα HTML και HTTP, το πρότυπο XML και το RMI-IOP πρότυπο, που καθορίζει τη χρήση του CORBA IIOP πρωτοκόλλου για την απομακρυσμένη κλήση μεθόδων (Remote Method Invocation).

- J2EE Compatibility Test Suite. Είναι λογισμικό που εκτελείται στην J2EE πλατφόρμα ενός κατασκευαστή και επαληθεύει τη συμβατότητα της πλατφόρμας με το J2EE πρότυπο.
- J2EE Reference Implementation. Είναι προϊόν, όχι για εμπορική χρήση, που επιδεικνύει τις δυνατότητες του J2EE και παρέχει ένα λειτουργικό ορισμό (operational definition) του προτύπου.

Στη συνέχεια αναλύονται περισσότερο τα συστατικά του προτύπου J2EE που έχουν ιδιαίτερη σημασία για την ανάπτυξη Υπηρεσιών Διαδικτύου.

4.5.1. Enterprise Java Beans.

Τα Enterprise Java Beans (EJBs) είναι αντικείμενα, που έχουν γνωρίσματα και μεθόδους, και αποτελούν μονάδες επιχειρησιακής λογικής (business logic units). Το business tier μιας J2EE εφαρμογής συγκροτείται από τέτοιες μονάδες επιχειρησιακής λογικής. Τα EJBs μιας εφαρμογής συνυπάρχουν μέσα σε ένα EJB container, το οποίο παρέχει υπηρεσίες όπως διαχείριση συναλλαγών, ασφάλεια συναλλαγών, διαχείριση των συνδέσεων, εξισορρόπηση φόρτου μεταξύ των συνδέσεων, δυνατότητα αποθήκευσης πληροφοριών συνόδου και ανάκαμψη από αποτυχίες. Υπάρχουν τρεις τύποι EJBs, αυτοί είναι [Kao, 2001]:

- Session EJBs.
- Entity EJBs.
- Message-Driven EJBs.

Ένα Session EJB αντιστοιχεί σε ένα μοναδικό πελάτη του κεντρικού υπολογιστή της εφαρμογής (application server). Ο πελάτης αυτός έχει πρόσβαση στην εφαρμογή με την κλήση των μεθόδων του Session EJB. Τα Session EJBs, εκτελούν στοιχειώδεις επιχειρησιακές λειτουργίες στον κεντρικό υπολογιστή, καλούν άλλα EJBs και γενικά αφαιρούν πολυπλοκότητα από τον πελάτη. Όταν ολοκληρωθεί η σύνοδος με τον πελάτη, το Session EJB τερματίζει τη λειτουργία του και χάνει τη σύνδεση του με αυτόν.

Ένα Entity EJB αναπαριστά τα δεδομένα μιας βάσης δεδομένων με αντικειμενοστραφή τρόπο, αποκρύπτοντας την πολυπλοκότητα της βάσης. Το στιγμιότυπο ενός Entity EJB σε οποιαδήποτε χρονική στιγμή επιμένει (persist) σε μια κατάσταση, που είναι αποθηκευμένη σε εκείνη τη γραμμή του πίνακα της βάσης που αντιστοιχεί σε αυτό. Τα Entity EJB υποστηρίζουν ταυτόχρονη πρόσβαση.



Τα Message-Driven EJBs είναι αντικείμενα που μπορούν να δέχονται μηνύματα μέσω μιας υπηρεσίας μηνυμάτων της Java. Παρέχουν ένα μηχανισμό στις J2EE εφαρμογές για να επικοινωνούν με παλαιότερες εφαρμογές που βασίζονται στην ανταλλαγή μηνυμάτων (message-based legacy systems).

4.5.2. Java Servlets.

Τα Java Servlets είναι αντικείμενα της Java που επεκτείνουν τις δυνατότητες ενός εξυπηρετητή μιας υπηρεσίας διαδικτύου. Είναι τεχνολογία ανεξάρτητη από πλατφόρμες [Armstrong et al., 2002]. Όταν ένας πελάτης της υπηρεσίας πραγματοποιεί μια αίτηση στην υπηρεσία, ο αποδέκτης του SOAP μηνύματος είναι ένα αντικείμενο Java Servlet. Το Java Servlet, αφού πρώτα επεξεργαστεί την αίτηση, καλεί ένα ή περισσότερα EJB αντικείμενα. Τα EJB αντικείμενα εκτελούν τις απαραίτητες λειτουργίες και επιστρέφουν τα δεδομένα στο Java Servlet. Το Java Servlet τοποθετεί τα δεδομένα αυτά σε ένα XML έγγραφο, το οποίο και στέλνει ως απάντηση στον πελάτη, μέσω του πρωτοκόλλου HTTP.

Στα χαρακτηριστικά των Java Servlets είναι ότι επιτρέπουν την αποθήκευση δεδομένων μεταξύ των αιτήσεων και την επιστροφή σε παλαιότερους υπολογισμούς. Επίσης, παρέχουν τη δυνατότητα παρακολούθησης μιας συνόδου και αποθήκευσης και διαχείρισης κωδικοποιημένης πληροφορίας για τον πελάτη (cookies).

4.5.3. JSP.

Οι Java Server Pages (JSP) είναι τεχνολογία του διαδικτύου, η οποία παρέχει ένα μηχανισμό για την ανάπτυξη server εφαρμογών, που μπορούν να παράγουν ιστοσελίδες με δυναμικό περιεχόμενο, σε απόκριση της αίτηση ενός πελάτη [Maddox et al., 2002]. Η δημιουργία των ιστοσελίδων επιτυγχάνεται μέσω μιας ισχυρής γλώσσας κειμένου που ενσωματώνει στοιχεία από την HTML και από τη λογική των Java εφαρμογών. Η HTML χρησιμοποιείται ως το μέσο προβολής της στατικής πληροφορίας και το πρότυπο που καθορίζει το μορφότυπο των ιστοσελίδων. Το δυναμικό περιεχόμενο των JSP παράγεται ενσωματώνοντας κώδικα από την εφαρμογή, που είναι γραμμένη σε Java, σε ετικέτες παρόμοιες με αυτές της XML.

Η τεχνολογία των Java Server Pages, παρέχει ένα αλληλεπιδραστικό (Interactive) περιβάλλον διεπαφής για το χρήστη που επιθυμεί να χρησιμοποιήσει απευθείας μια υπηρεσία

διαδικτύου. Με την τεχνολογία των JSP, η ίδια υπηρεσία διαδικτύου που μπορεί να κληθεί από μια εφαρμογή μέσω ενός SOAP μηνύματος, μπορεί να κληθεί και να επιστρέψει την αντίστοιχη πληροφορία σε έναν τελικό χρήστη με τη μορφή ιστοσελίδας.

4.5.4. Electronic Business XML.

Το Electronic Business XML είναι ένα πρότυπο, που συστάθηκε από τους οργανισμούς OASIS³⁹ και UN/CEFACT⁴⁰, για το οποίο παρέχει υποστήριξη το J2EE. Το ebXML καθορίζει ένα πλαίσιο που επιτρέπει στις επιχειρήσεις να εντοπίζουν η μία την άλλη και να πραγματοποιούν πολύπλοκες συναλλαγές που βασίζονται σε καλά ορισμένα XML μηνύματα [HP, 2001]. Το ebXML προσφέρει δυνατότητες που δεν περιλαμβάνονται στο πρότυπο SOAP, αν και μπορούν να ενσωματωθούν σε αυτό. Συγκεκριμένα, το πρότυπο ebXML καθορίζει ένα πλαίσιο συναλλαγών που σχετίζεται με πρότυπες επιχειρησιακές διαδικασίες που ελέγχονται από καθορισμένες ή αμοιβαία διαπραγματευόμενες συμφωνίες μεταξύ των επιχειρήσεων.

Το ebXML πρότυπο καθορίζει ένα τόπο αποθήκευσης και αναζήτησης της πληροφορίας των επιχειρήσεων που παρέχει λειτουργικότητα ίδια με την UDDI registry και ονομάζεται ebXML registry. Εντούτοις, μια επιπλέον δυνατότητα του ebXML προτύπου σε σύγκριση με άλλα υπάρχοντα πρότυπα είναι η διατήρηση μιας ebXML αποθήκης (repository). Στο ebXML repository αποθηκεύονται πληροφορίες που σχετίζονται με τη λειτουργία μιας επιχείρησης. Με την προσθήκη αυτή, απαραίτητη προϋπόθεση για να συμβεί μια συναλλαγή είναι να συμφωνήσει ο προμηθευτής της υπηρεσίας με τους όρους του πελάτη που περιλαμβάνονται στις πληροφορίες που βρίσκονται στο ebXML repository.

4.5.5. Java Web Services APIs.

Το πρότυπο J2EE παρέχει ένα σύνολο από προδιαγραφές, που αφορούν σε διεπαφές (APIs), οι οποίες υποστηρίζουν βασικές λειτουργίες που σχετίζονται με την ανάπτυξη και διαχείριση Υπηρεσιών Διαδικτύου. Οι περισσότερες από αυτές που περιγράφονται στη συνεχεία, περιλαμβάνονται στην τρέχουσα έκδοση του J2EE προτύπου [Shannon, 2001], ενώ οι υπόλοιπες ήδη υπάρχουν και πρόκειται να συμπεριληφθούν στην επόμενη έκδοση [Shannon, 2002]. Συνοπτικά:

³⁹ Organization for the Advancement of Structural Information Standards

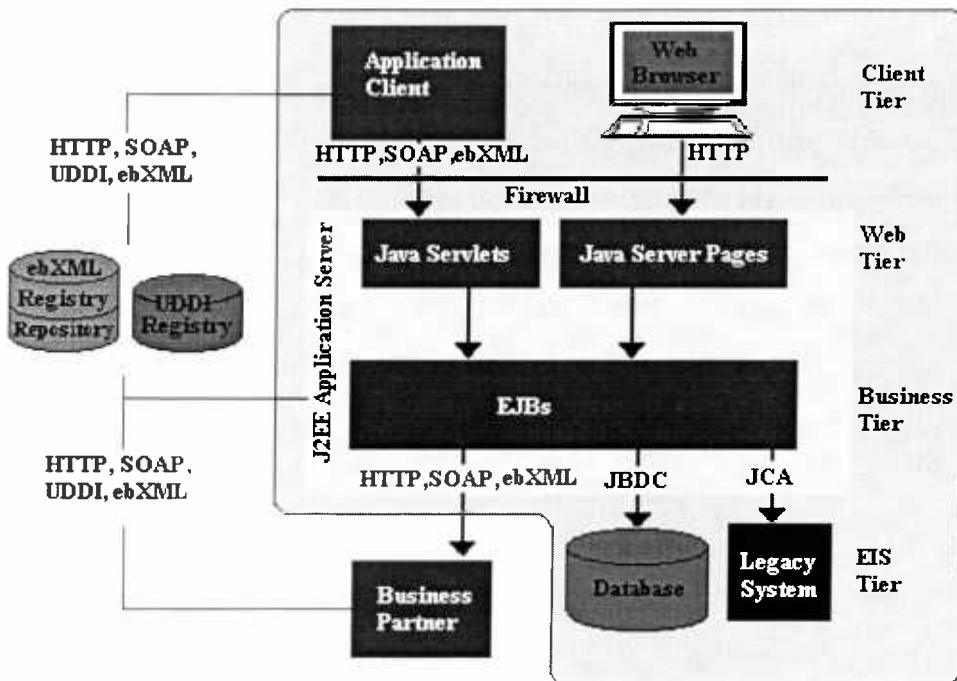
⁴⁰ United Nations Center For Trade Facilitation And Electronic Business



- Το JAXP είναι μια Java διεπαφή που χρησιμοποιείται για την ανάγνωση, τροποποίηση και δημιουργία XML εγγράφων.
- Το JAXR είναι μια Java διεπαφή που υποστηρίζει τις λειτουργίες που επιτρέπουν οι κατάλογοι υπηρεσιών UDDI και ebXML και οι οποίες είναι δημοσίευση, αναζήτηση και τροποποίηση στοιχείων.
- Το JWSDL είναι μια Java διεπαφή που υποστηρίζει τη διαχείριση WSDL εγγράφων. Για τον ίδιο σκοπό μπορεί επίσης να χρησιμοποιηθεί το JAXP, ωστόσο το JWSDL είναι απλούστερο και γρηγορότερο στη χρήση.
- Το JAX/RPC είναι μια Java διεπαφή που χρησιμοποιείται για τη λήψη και αποστολή SOAP μηνυμάτων που επιτρέπουν την απομακρυσμένη κλήση διαδικασιών.
- Το JAXM είναι ομοίως μια Java διεπαφή που χρησιμοποιείται για τη λήψη και αποστολή απλών (document-oriented) SOAP μηνυμάτων.
- Το JAXB είναι μια Java διεπαφή που χρησιμοποιείται για τη μετατροπή ενός XML σχήματος σε μία ή περισσότερες κλάσεις της Java και το αντίστροφο.
- Το JDBC είναι μια Java διεπαφή που παρέχει πρόσβαση σε σχεσιακές βάσεις δεδομένων που υποστηρίζουν SQL.

4.5.6. Αρχιτεκτονική Υπηρεσίας Διαδικτύου σύμφωνα με το πρότυπο J2EE.

Με βάση τα παραπάνω μπορεί να δοθεί η συνολική εικόνα της αρχιτεκτονικής μιας υπηρεσίας διαδικτύου που στηρίζεται στο J2EE πρότυπο (Σχήμα 4.4.).



Σχήμα 4.4.: Αρχιτεκτονική υπηρεσίας διαδικτύου σύμφωνα με το J2EE πρότυπο.

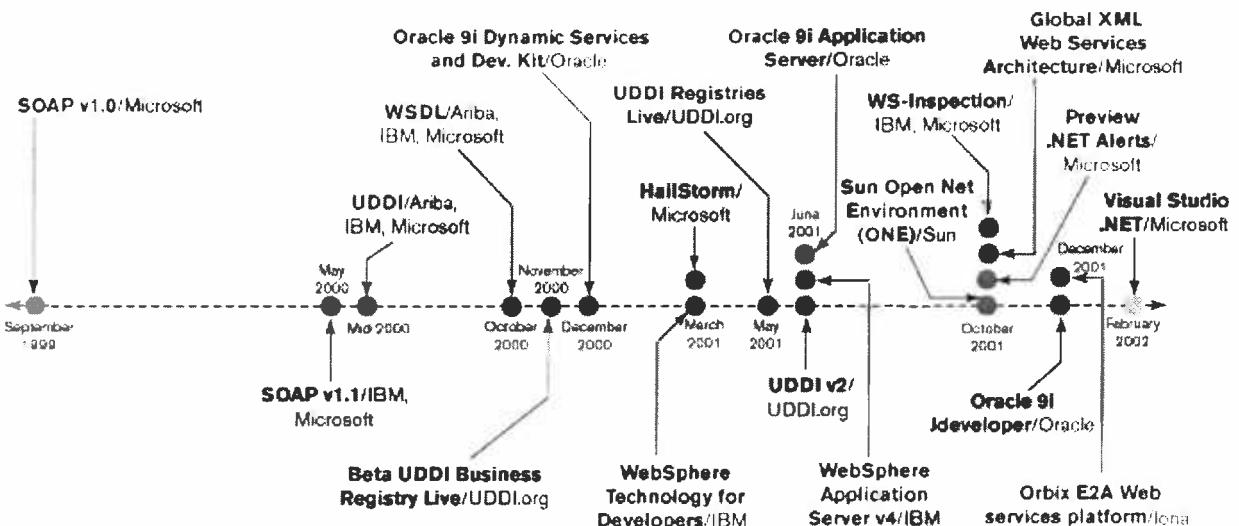
To Business tier της υπηρεσίας αποτελείται από τμήματα κώδικα, που είναι τα EJBs. Το Business Tier συνδέεται με τη βάση δεδομένων, μέσω του JDBC ενώ παρέχεται και η δυνατότητα σύνδεσης του με legacy συστήματα, μέσω της τεχνολογίας J2EE Connector Architecture. Η τεχνολογία αυτή, επιτρέπει την εύρεση του κατάλληλου adaptor για τη σύνδεση με ένα υπάρχον σύστημα. Η υπηρεσία μπορεί να ενσωματώνει τη λειτουργία κάποιας άλλης Υπηρεσίας Διαδικτύου, που έχει αναπτυχθεί από κάποιον εμπορικό συνεργάτη. Συγκεκριμένα, το Business tier της εφαρμογής αποστέλλει SOAP ή ebXML μηνύματα που πραγματοποιούν κλήση διαδικασιών της απομακρυσμένης υπηρεσίας, μέσω του HTTP πρωτοκόλλου.

Η δέσμευση της υπηρεσίας από μια client εφαρμογή γίνεται με αποστολή ενός SOAP ή ebXML μηνύματος μέσω του πρωτοκόλλου HTTP. Τα SOAP μηνύματα παραλαμβάνονται και εξυπηρετούνται από τα Java Servlets, τα οποία συνιστούν μαζί με τις σελίδες JSP το Web tier επίπεδο της εφαρμογής. Οι JSP σελίδες παρέχουν πρόσβαση στην υπηρεσία σε πελάτες που χρησιμοποιούν Web Browsers.

Τέλος, η διαδικασία δημοσίευσης της υπηρεσίας, καθώς και η διαδικασία αναζήτησης της υπηρεσίας ενός εμπορικού συνεργάτη υποστηρίζονται από την τεχνολογία UDDI ή εναλλακτικά από την τεχνολογία ebXML, που διευκολύνει πιο σύνθετες συναλλαγές μεταξύ των επιχειρήσεων.

4.6. Η αγορά των Υπηρεσιών Διαδικτύου.

Οι εταιρείες IBM και Microsoft έδειξαν από νωρίς το ενδιαφέρον τους να ηγηθούν των προσπαθειών στο χώρο των Υπηρεσιών Διαδικτύου. Οι εταιρείες αυτές ήταν οι πρώτες που εργάστηκαν για τον καθορισμό μιας στοίβας τεχνολογιών για την υποστήριξη των υπηρεσιών αυτών. Επίσης, ήταν οι πρώτες εταιρείες που δημιούργησαν προϊόντα για την ανάπτυξη των Υπηρεσιών Διαδικτύου. Στο Σχήμα 4.5. δίνεται μια εικόνα της πορείας που ακολούθησε η αγορά των Υπηρεσιών Διαδικτύου τα τρία τελευταία χρόνια [Evans, 2002].



Σχήμα 4.5.: Η πορεία της αγοράς των Υπηρεσιών Διαδικτύου. [Evans, 2002]

Το Microsoft .NET (ή HailStorm) και το WebSphere της IBM, τα οποία ανακοινώθηκαν στις αρχές του 2001, ήταν τα πρώτα προϊόντα που παρείχαν υποστήριξη στα πρότυπα SOAP, WSDL και UDDI. Το προϊόν Oracle 9i Application Server της εταιρείας Oracle, τέθηκε στη διάθεση των προγραμματιστών την ίδια χρονιά και σχεδόν ταυτόχρονα με μια νέα έκδοση του WebSphere Application Server της IBM. Οι δύο application servers εκτός από υποστήριξη στα πρότυπα SOAP, WSDL και UDDI παρείχαν συμβατότητα με το πρότυπο J2EE. Η εταιρεία Sun Microsystems, αν και επικεφαλής των προσπαθειών για την υποστήριξη της νέας τεχνολογίας από το J2EE πρότυπο, καθυστέρησε αρκετά να διαθέσει στην αγορά το δικό της J2EE server. Το προϊόν Sun Open Net Environment (ONE) τελικά πρόβαλε στην αγορά το φθινόπωρο του 2001, την ίδια εποχή που η Microsoft ανακοίνωσε την αρχιτεκτονική Global XML, προτείνοντας επιπλέον προδιαγραφές, που βασίζονταν σε υπάρχοντα πρότυπα, ανάμεσα στις οποίες και την WS-security που αφορά στην ασφάλεια των υπηρεσιών διαδικτύου.

Τα παραπάνω συνθέτουν ένα επιχειρηματικό περιβάλλον που χαρακτηρίζεται από έντονο ανταγωνισμό. Η εταιρεία Microsoft έχει επιλέξει μια στάση συνεργατική, κυρίως νιοθετώντας κοινά πρότυπα, γεγονός που είναι αντίθετο με την πολιτική που ακολουθεί σε άλλες αγορές. Αυτό εντείνει σε μεγάλο βαθμό τον ανταγωνισμό. Ωστόσο, σημαντικός παράγοντας για την επικράτηση ή όχι του Microsoft .NET, είναι η συσπείρωση που θα δείξουν οι εταιρείες που υποστηρίζουν το J2EE πρότυπο. Μέχρι στιγμής, όμως, δεν φαίνεται κάτι τέτοιο. Σε αντίθεση με την εταιρεία Sun που προσπαθεί να εξασφαλίσει στους ειδικούς ανάπτυξης υπηρεσιών διαδικτύου ένα περιβάλλον ανάπτυξης κοινό για όλους, άλλες

εταιρείες, όπως η IBM, η Oracle, η Hewlett Packard και η BEA Systems, δημιουργούν υποδομές που λειτουργούν καλύτερα με τα δικά τους προϊόντα ή των συνεργατών τους [Vaughan, 2002]. Το σίγουρο αυτή τη στιγμή είναι ότι ο τομέας των υπηρεσιών διαδικτύου θα συνεχίσει να αναπτύσσεται αλματωδώς διευρύνοντας ολοένα τις δυνατότητες των επιχειρήσεων.

4.7. Συμπέρασμα.

Το γενικό συμπέρασμα που προκύπτει από το κεφάλαιο αυτό είναι η ύπαρξη μιας κοινής επιθυμίας των περισσότερων εταιρειών για ανάπτυξη των υπηρεσιών διαδικτύου, η οποία πηγάζει στις ολοένα αυξανόμενες ανάγκες που δημιουργεί το e-business. Μια πρώτη θετική διαπίστωση είναι ότι οι εταιρείες, έχοντας αντιληφθεί, ότι ανοίγει μια νέα εποχή, συμβάλλουν στη γρηγορότερη έλευση της, κυρίως με τη συμφωνία και τη συνεργασία τους πάνω σε κοινά τεχνολογικά ζητήματα. Εντούτοις, η μη διαφοροποίησή τους στη βασική δομή των υπηρεσιών, δεν επιτρέπει την κατοχύρωση ενός ανταγωνιστικού πλεονεκτήματος, που θα αποτελέσει παράγοντα για την επικράτησή τους στην αγορά. Το ζήτημα της ασφάλειας, ίσως είναι τελικά ο καθοριστικός παράγοντας που θα διαμορφώσει ευνοϊκές συνθήκες για όποιον καταφέρει να το επιλύσει γρηγορότερα. Μάλιστα, παρά το γεγονός ότι η ανάπτυξη των υπηρεσιών διαδικτύου βρίσκεται σε πρώιμο στάδιο, οι πλατφόρμες ανάπτυξης που αναφέρθηκαν στο κεφάλαιο αυτό παρέχουν αρκετές υπηρεσίες ασφάλειας. Πριν όμως παρουσιαστούν αυτές είναι απαραίτητο να προηγηθεί μια διερεύνηση πάνω στις απαιτήσεις ασφάλειας που σχετίζονται με τις υπηρεσίες διαδικτύου.

ΚΕΦΑΛΑΙΟ 5^ο : ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ

5.1. Εισαγωγή.

Στις μέρες μας, το ζήτημα της ασφάλειας των πληροφοριακών συστημάτων βρίσκεται στο επίκεντρο του ενδιαφέροντος της επιστημονικής κοινότητας, αλλά και των επιχειρήσεων, πολύ περισσότερο μάλιστα σε ότι αφορά το ηλεκτρονικό επιχειρείν. Άλλωστε, στο περιβάλλον του διαδικτύου, οι κίνδυνοι στους οποίους υποβάλλεται ένα πληροφοριακό σύστημα είναι περισσότεροι, δεδομένου ότι οι απειλές είναι πολλαπλάσιες, σε βαθμό βέβαια ανάλογο και με τη φύση του πληροφοριακού συστήματος.

Οι Υπηρεσίες Διαδικτύου καθορίζουν ένα μοντέλο αλληλεπίδρασης μεταξύ εφαρμογών που βρίσκονται σε ετερογενή πληροφοριακά συστήματα, το οποίο βασίζεται στην ανταλλαγή μηνυμάτων μέσω του διαδικτύου. Το μοντέλο αυτό χαρακτηρίζεται από ιδιαιτερότητες που το καθιστούν ευεπίφορο σε απειλές, τις οποίες δεν είναι αρκετά ευέλικτο να αντιμετωπίσει, χωρίς την κατάλληλη αξιοποίηση και επέκταση των υφιστάμενων μεθόδων και τεχνικών.

Στο κεφάλαιο αυτό αναλύονται οι βασικές απαιτήσεις ασφάλειας για τις υπηρεσίες διαδικτύου. Δίνεται έμφαση στα ιδιαίτερα χαρακτηριστικά του μοντέλου των υπηρεσιών διαδικτύου, που διαφοροποιούν τις απαιτήσεις για ασφάλεια, σε σύγκριση με το μοντέλο των απλών client-server διαδικτυακών εφαρμογών.

5.2. Τι σημαίνει Ασφάλεια Υπηρεσιών.

Μια υπηρεσία είναι ένα σύνολο από λειτουργίες που παρέχει μια οντότητα (προμηθευτής) σε μια άλλη οντότητα (πελάτης), συνήθως κατόπιν συμφωνίας (π.χ. συμβολαίου). Η συμφωνία αφορά κυρίως στον καθορισμό δικαιωμάτων και υποχρεώσεων που σχετίζονται με τις δύο οντότητες. Βάσει της συμφωνίας, για παράδειγμα, ο προμηθευτής δεσμεύεται σε συγκεκριμένα ζητήματα που αφορούν στην ποιότητα και στη διαθεσιμότητα της υπηρεσίας. Ομοίως, βάσει της συμφωνίας ο πελάτης αποδέχεται ορισμένες ευθύνες, στο πλαίσιο της απόκτησης του δικαιώματος από τον προμηθευτή, που του επιτρέπει να χρησιμοποιεί την εν λόγω υπηρεσία.

Η βάση για την παροχή υπηρεσιών είναι τα αγαθά. Τα αγαθά, στο χώρο της επιστήμης υπολογιστών, είναι δύο ειδών [Γκρίτζαλης Δ., 2001]:



- Η πληροφορία, που περιλαμβάνει τα δεδομένα (data) μαζί με τη σημασία που τους αποδίδεται.
- Οι υπολογιστικοί πόροι, που είναι οτιδήποτε χρησιμοποιείται από ένα υπολογιστικό σύστημα για να διαχειριστεί πληροφορίες. Ο όρος υπολογιστικό σύστημα αναφέρεται σε μια συλλογή υλικού, λογισμικού ή άλλου εξοπλισμού, εγκατεστημένη σε κάποια τοποθεσία, με ένα συγκεκριμένο λειτουργικό περιβάλλον, η οποία ανταποκρίνεται σε ένα συγκεκριμένο σκοπό.

Με βάση τα παραπάνω, μπορεί να δοθεί ο ορισμός της έννοιας υπηρεσία, στον χώρο της επιστήμης των υπολογιστών:

Υπηρεσία είναι ένα σύνολο από λειτουργίες, που έχουν ως βάση τους την πληροφορία, οι οποίες παρέχονται από ένα υπολογιστικό σύστημα σε ένα χρήστη, συνήθως βάσει συμφωνίας. Η συμφωνία περιλαμβάνει όρους που γνωστοποιούν στον πελάτη και στο χορηγό της υπηρεσίας τις ευθύνες που τους αντιστοιχούν στο πλαίσιο της συναλλαγής τους.

Ασφάλεια μιας υπηρεσίας σημαίνει εξασφάλιση του συνόλου των παραμέτρων που περιλαμβάνει ο παραπάνω ορισμός. Με βάση αυτή την προσέγγιση, η ασφάλεια μιας υπηρεσίας περιλαμβάνει :

- Την ασφάλεια της πληροφορίας.
- Την ασφάλεια του υπολογιστικού συστήματος.
- Την εξασφάλιση της αποδοχής και τήρησης των όρων της συμφωνίας.

Ασφάλεια της πληροφορίας είναι ο συνδυασμός της εμπιστευτικότητας, της εγκυρότητας και της διαθεσιμότητας της πληροφορίας [Γκρίτζαλης Δ., 2001]. Εμπιστευτικότητα (confidence) είναι η αποφυγή της αποκάλυψης της πληροφορίας χωρίς την άδεια του ιδιοκτήτη της. Εγκυρότητα (validity) είναι η απόλυτη ακρίβεια και πληρότητα της πληροφορίας. Περιλαμβάνει την ακεραιότητα και την αυθεντικότητα. Ακεραιότητα (integrity) είναι η αποφυγή της μη εξουσιοδοτημένης (από τον ιδιοκτήτη) τροποποίησης μιας πληροφορίας. Αντίθετα, αυθεντικότητα (authenticity) είναι η αποφυγή ατελειών και ανακριβειών κατά τη διάρκεια των εξουσιοδοτημένων τροποποιήσεων της πληροφορίας. Διαθεσιμότητα της πληροφορίας (information availability) είναι η αποφυγή προσωρινής ή μόνιμης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες.

Ασφάλεια του υπολογιστικού συστήματος είναι ο συνδυασμός της διαθεσιμότητας του συστήματος και της ασφάλειας του λογισμικού (ή της εσωτερικής πληροφορίας) του συστήματος [Γκρίτζαλης Δ., 2001]. Διαθεσιμότητα του συστήματος (system availability)

είναι η αποτροπή της προσωρινής ή μόνιμης άρνησης διάθεσης των υπολογιστικών πόρων στους εξουσιοδοτημένους χρήστες.

Η εξασφάλιση της αποδοχής των όρων της συμφωνίας αναλύεται σε δύο βασικές επιδιώξεις. Αυτές είναι: α) η εξασφάλιση της μη αποποίησης (non-repudiation) της ευθύνης του πελάτη και β) η εξασφάλιση της μη αποποίησης της ευθύνης του ιδιοκτήτη της υπηρεσίας.

Για την επαρκή εξασφάλιση όλων των παραμέτρων που συνθέτουν την έννοια της υπηρεσίας, είναι απαραίτητο να ληφθούν μια σειρά από μέτρα. Η εξασφάλιση κάθε μίας παραμέτρου συνεπάγεται και μια ξεχωριστή απαίτηση ασφάλειας. Οι απαιτήσεις ασφάλειας διατυπώνονται, αφού ληφθούν υπόψη, οι πιθανές απειλές, αλλά και οι εγγενείς αδυναμίες της υπηρεσίας που μπορεί να αποτελέσουν αιτία για να προκληθεί ζημιά σε οποιοδήποτε από τα χαρακτηριστικά που συνθέτουν την ασφάλεια της υπηρεσίας.

5.3. Τι είναι Πολιτική ασφαλείας.

Η διατύπωση απαιτήσεων είναι ένα σημαντικό βήμα για την αντιμετώπιση του ζητήματος της ασφάλειας, κυρίως γιατί φέρνει τους υπευθύνους αντιμέτωπους με το πρόβλημα και τους επιτρέπει να θέσουν συγκεκριμένους στόχους. Ωστόσο, για να επιτευχθούν οι στόχοι απαιτείται συντονισμένη προσπάθεια.

Η πολιτική ασφάλειας ουσιαστικά αποτελεί μια στρατηγική που παρέχει τις κατευθύνσεις σχετικά με τις ενέργειες που πρέπει να γίνουν, έτσι ώστε να επιτευχθούν οι στόχοι ασφαλείας που έχουν τεθεί σε έναν οργανισμό. Σύμφωνα με τον Κοκολάκη [Κοκολάκης, 2000], η πολιτική είναι ένα σύνολο έγκυρων και επίσημων δηλωτικών προτάσεων, που προσδιορίζουν το σύνολο των αποδεκτών πιθανών επιλογών, σε μελλοντικές διαδικασίες λήψεως αποφάσεων. Τα συστατικά μιας πολιτικής ασφαλείας είναι τα εξής:

- Αγαθά (assets). Τα αγαθά είναι οντότητες ενός οργανισμού που θεωρούνται πολύτιμες και χρειάζονται προστασία. Η προστασία των αγαθών είναι ο πρωταρχικός στόχος μιας πολιτικής ασφάλειας. Η επιλογή⁴¹ των μέσων προστασίας πρέπει να γίνεται με βάση την αξία των αγαθών, που δεν εκφράζεται απαραίτητα με οικονομικούς όρους, και με βάση τους κινδύνους που αντιμετωπίζουν.

⁴¹ Η Ανάλυση Επικινδυνότητας είναι για παράδειγμα μια μεθοδολογία που επιτρέπει την επιλογή μέσων προστασίας που προσφέρουν ασφάλεια αντίστοιχη με την αξία ενός πληροφοριακού συστήματος και με τους κινδύνους που αντιμετωπίζει.

- **Ρόλοι και αρμοδιότητες (roles).** Μια πολιτική ασφαλείας δεν αναφέρεται σε φυσικά πρόσωπα, αναφέρεται όμως στους ρόλους αυτών.
- **Στόχοι ασφάλειας (goal).** Αποτελούν το σημαντικότερο συστατικό μιας πολιτικής. Είναι ο σκοπός ύπαρξης της πολιτικής ασφάλειας.
- **Οδηγίες (guidelines).** Είναι κανόνες, στους οποίους πρέπει να συμμορφωθούν όλοι οι εργαζόμενοι σε έναν οργανισμό, ή διαδικασίες που πρέπει να υιοθετηθούν από τον οργανισμό. Οι κανόνες δεν πρέπει να είναι διατυπωμένοι σε αυστηρά τεχνική γλώσσα, αφού στόχος είναι να είναι κατανοητοί από το σύνολο των εργαζομένων.
- **Πεδίο εφαρμογής της πολιτικής (policy domain).** Η περιοχή στην οποία εκτείνεται η εφαρμογή της πολιτικής ασφάλειας σε έναν οργανισμό.
- **Κοσμοθεωρία (worldview).** Πρόκειται για τις θεωρήσεις, τις αρχές, τις αξίες, τα πιστεύω, τις νόρμες που λαμβάνονται υπόψη κατά τη διαχείριση απειλών και αδυναμιών, καθώς και κατά την εφαρμογή μέτρων και τεχνικών.

5.4. Πολιτικές ασφαλείας στο μοντέλο υπηρεσιών διαδικτύου.

Η πολιτική ασφαλείας που ορίζεται από έναν οργανισμό που παρέχει μια υπηρεσία διαδικτύου, αποτελεί κρίσιμο παράγοντα για την επιλογή της χρησιμοποίησης της συγκεκριμένης υπηρεσίας από ένα πελάτη. Για παράδειγμα, κάποιος ίσως να ενδιαφέρεται να μάθει πώς γίνεται η διαχείριση προσωπικών δεδομένων από μια υπηρεσία, πριν αποφασίσει να γίνει πελάτης της. Επίσης, η γνώση της πολιτικής ασφαλείας ενός χορηγού μιας υπηρεσίας μπορεί να είναι απαραίτητη και για την αλληλεπίδραση ενός πελάτη με αυτήν. Έστω ότι μια υπηρεσία A ακολουθεί μια πολιτική ασφάλειας, που καθορίζει κάποιους μηχανισμούς ασφαλείας που πρέπει να εφαρμοστούν σε ένα SOAP μήνυμα κατά την αποστολή του σε μια άλλη υπηρεσία. Η αλληλεπίδραση της υπηρεσίας A με την υπηρεσία B, είναι δυνατή μόνο αν οι συγκεκριμένοι μηχανισμοί ασφαλείας είναι συνεπείς και με την πολιτική ασφαλείας της υπηρεσίας B. Το γεγονός αυτό, απαιτεί την εύρεση ενός τρόπου, με τον οποίο ο πελάτης μιας υπηρεσίας θα μπορεί να ανακαλύπτει την πολιτική ασφαλείας του χορηγού μιας υπηρεσίας και επιπλέον να εφαρμόζει τεχνικές ασφαλείας που να είναι συνεπείς με την πολιτική ασφαλείας του χορηγού, όπως και με τη δική του.

Μια λύση στο παραπάνω πρόβλημα, είναι να συμπεριληφθεί η πολιτική ασφαλείας μιας υπηρεσίας στην περιγραφή της υπηρεσίας, ώστε να είναι διαθέσιμη με την ανακάλυψη της υπηρεσίας. Αυτό προϋποθέτει τη δημιουργία ενός XML σχήματος, που θα διαθέτει



χαρακτηριστικά εκείνα που έχει μια γλώσσα περιγραφής πολιτικών ασφαλείας. Η ανακάλυψη της πολιτικής ασφαλείας στην περίπτωση αυτή θα μπορεί να γίνεται από μια υπηρεσία καταλόγου (π.χ. UDDI). Στην περίπτωση που η πολιτική ασφαλείας της υπηρεσίας βρίσκεται σε συμφωνία με την πολιτική ασφαλείας του πελάτη, δεν υπάρχει πρόβλημα. Στην περίπτωση όμως, που υπάρχει σύγκρουση πολιτικών ασφαλείας μεταξύ δύο υπηρεσιών που ανήκουν σε διαφορετικά πεδία εφαρμογής πολιτικών ασφαλείας (policy domains), απαιτείται διαπραγμάτευση (negotiation). Για να συμβεί διαπραγμάτευση πολιτικών είναι απαραίτητο οι δύο πλευρές να έρθουν σε επικοινωνία κατά την οποία ενδέχεται να προτείνουν τις εναλλακτικές πολιτικές που έχουν (αν φυσικά έχουν).

Μια διαπραγμάτευση, χωρίς αυτό να συμβαίνει πάντα, μπορεί να έχει ως κατάληξη τη σύνταξη μιας μεταπολιτικής. Ο Κοκολάκης [Κοκολάκης, 2000] αναφέρει ότι σύμφωνα την Hosmer⁴², μια μεταπολιτική μπορεί να αποτελεί ένα σύνολο από κανόνες για το συντονισμό της εφαρμογής διαφορετικών πολιτικών ασφάλειας. Επίσης, επισημαίνει ότι ο εντοπισμός συγκρούσεων και η επίλυση τους βάσει μιας μεταπολιτικής μπορεί να γίνει με τη βοήθεια οντοτήτων λογισμικού που ονομάζονται πολιτικοί διαμεσολαβητές (Policy Agents). Απαραίτητη προϋπόθεση για αυτό, είναι η αναπαράσταση των πολιτικών και της μεταπολιτικής σε μια κοινή τυπική γλώσσα, γεγονός το οποίο επισημαίνεται και από τους Lupu και Sloman⁴³.

Με βάση τα παραπάνω, και με δεδομένη την απουσία κάποιου τρόπου επίλυσης των συγκρούσεων των πολιτικών ασφαλείας μεταξύ δύο υπηρεσιών διαδικτύου, μια πρόταση θα μπορούσε να περιλαμβάνει: α) τη διατύπωση των πολιτικών ασφαλείας και της μεταπολιτικής σε γλώσσα XML, και β) την ανάθεση του ρόλου του πολιτικού διαμεσολαβητή σε μια υπηρεσία διαδικτύου (τρίτη οντότητα).

5.5. Ανάλυση των απαιτήσεων ασφάλειας στις Υπηρεσίες Διαδικτύου.

Συνοπτικά, οι βασικές απαιτήσεις ασφάλειας των υπηρεσιών διαδικτύου, όπως προέκυψαν από την ανάλυση που προηγήθηκε στην ενότητα 5.2., περιλαμβάνουν την ανάγκη για εξασφάλιση:

1. Της εμπιστευτικότητας της πληροφορίας.
2. Της εγκυρότητας της πληροφορίας.

⁴² Hosmer H., "Metapolicies II", 15th National Computer Security Conference, Baltimore, USA, 1992.

⁴³ Lupu E. and Sloman M., "Conflicts in policy-based distributed systems management", IEEE, 1999.

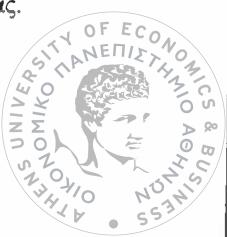
3. Της διαθεσιμότητας της πληροφορίας, των υπολογιστικών πόρων και του λογισμικού, δηλαδή την εξασφάλιση της διαθεσιμότητας της υπηρεσίας.
4. Της εμπιστευτικότητας και εγκυρότητας του λογισμικού (εσωτερικής πληροφορίας).
5. Της μη αποποίησης της ευθύνης των οντοτήτων που αλληλεπιδρούν.

Στην ενότητα αυτή αναλύονται ξεχωριστά κάθε μια από τις απαιτήσεις αυτές.

5.5.1. Εμπιστευτικότητα της πληροφορίας.

Οι υπηρεσίες διαδικτύου έχουν ως βάση τους την πληροφορία που ανταλλάσσουν μέσω μηνυμάτων οι οντότητες πελάτης της υπηρεσίας, χορηγός της υπηρεσίας και κατάλογος υπηρεσιών (βλ. ενότητα 2.5.2). Στις πληροφορίες αυτές περιλαμβάνονται εμπιστευτικά δεδομένα του πελάτη και της επιχείρησης που είναι απαραίτητα για τη διεκπεραίωση της μεταξύ τους συναλλαγής. Παραδείγματα τέτοιων δεδομένων είναι ο αριθμός της πιστωτικής κάρτας ενός πελάτη, ή οικονομικά στοιχεία που αφορούν στην επιχείρηση. Εξαιτίας της φύσης της γλώσσας XML, η πληροφορία ενός XML μηνύματος είναι σε κατανοητή μορφή για όποια μη εξουσιοδοτημένη⁴⁴ οντότητα καταφέρει να αποκτήσει πρόσβαση στο μήνυμα. Επιπλέον, η πιθανότητα αυτή η οντότητα να αποκτήσει πρόσβαση σε ένα XML μήνυμα είναι δύσκολο να αποκλειστεί. Μια τέτοια απειλή⁴⁵ ενδέχεται να παρουσιαστεί είτε κατά τη μετάδοση, είτε κατά την παραμονή ενός μηνύματος σε κάποια αποθήκη δεδομένων (π.χ. UDDI registry). Ιδιαίτερα όμως στην πρώτη περίπτωση, οι υπηρεσίες διαδικτύου εισάγουν μια πιο σύνθετη απαίτηση σε σύγκριση με απλές client-server υπηρεσίες. Η ιδιαιτερότητα των υπηρεσιών διαδικτύου οφείλεται στο γεγονός ότι μεταξύ του αποστολέα και του δέκτη των εμπιστευτικών πληροφοριών μπορεί να παρεμβάλλονται τρίτοι. Για παράδειγμα, ένας πελάτης μπορεί να καλεί μια υπηρεσία διαδικτύου που εκτελεί μια συγκεκριμένη λειτουργία και η υπηρεσία αυτή στη συνέχεια να καλεί άλλες υπηρεσίες που της προσφέρουν υποστήριξη στη λειτουργία αυτή. Η απαίτηση είναι η εξής. Πρέπει να βρεθεί τρόπος, ούτως ώστε η εμπιστευτική πληροφορία του πελάτη που καλεί μια υπηρεσία να μπορεί να αποκαλυφθεί μόνο από την υπηρεσία που τη χρειάζεται. Επίσης, η εμπιστευτικότητα της πληροφορίας πρέπει να προστατεύεται καθ' όλη τη διαδρομή της από τον πελάτη μέχρι την υπηρεσία αυτή (end-to-end confidentiality).

⁴⁴ Ποια οντότητα είναι εξουσιοδοτημένη και ποια όχι ορίζεται από την πολιτική ασφαλείας της υπηρεσίας.



5.5.2. Εγκυρότητα της πληροφορίας.

Η εγκυρότητα της πληροφορίας περιλαμβάνει την ακεραιότητα και την αυθεντικότητα. Η ακεραιότητα μιας πληροφορίας, αφορά στην περίπτωση της μη εξουσιοδοτημένη τροποποίησης. Μια πληροφορία μπορεί να αντικατασταθεί, να καταστραφεί ή να τροποποιηθεί από μη εξουσιοδοτημένα άτομα, ακόμα και αν τηρηθεί η εμπιστευτικότητα της. Αντίθετα, η αυθεντικότητα μιας πληροφορίας εξαρτάται από τον ιδιοκτήτη της και τους χρήστες που είναι εξουσιοδοτημένοι να την τροποποιούν. Ένα ερώτημα που τίθεται επομένως είναι αν υπάρχει εμπιστοσύνη στον ιδιοκτήτη και τους εξουσιοδοτημένους χρήστες. Αν υποτεθεί ότι υπάρχει εμπιστοσύνη στα πρόσωπα αυτά, μπορεί να θεωρηθεί δεδομένη η αυθεντικότητα μιας πληροφορίας, αρκεί να υπάρχει και εμπιστοσύνη στην κυριότητα της πληροφορίας. Είναι προφανές ότι στην περίπτωση των υπηρεσιών διαδικτύου τα ερωτήματα αυτά έχουν ακόμα μεγαλύτερο βάρος. Οι υπηρεσίες διαδικτύου τοπολογικά είναι ένα μοντέλο υπηρεσιών που αποτελείται από πολλές οντότητες που είναι διασκορπισμένες και επικοινωνούν με πληροφορίες που ανταλλάσσονται μεταξύ τους. Η επικοινωνία πολλές φορές γίνεται χωρίς να γνωρίζουν η μία την άλλη ή μέσω τρίτων, χωρίς πιθανόν να το γνωρίζουν. Με δεδομένη την ανάγκη για προστασία της εγκυρότητας της πληροφορίας ορισμένα βασικά ερωτήματα είναι τα εξής: α) πώς, για παράδειγμα, μια υπηρεσία ή ένας πελάτης μπορεί να εμπιστευτεί και να καλέσει μια υπηρεσία που δεν τη γνωρίζει, β) πώς μπορεί μια υπηρεσία ή ένας πελάτης να εμπιστευθεί την πληροφορία που του δίνεται για μια υπηρεσία, από ένα κατάλογο υπηρεσιών (π.χ. UDDI registry) και γ) πώς είναι δυνατό μια υπηρεσία ή ένας πελάτης που εμπιστεύεται την υπηρεσία την οποία καλεί, να έχει εμπιστοσύνη και στις υπηρεσίες που καλούνται από αυτή. Επομένως, οι απαιτήσεις που εισάγονται είναι η προστασία της ακεραιότητας της πληροφορίας αλλά και η λύση στο πρόβλημα της απόδοσης και μεταβίβασης της εμπιστοσύνης.

5.5.3. Διαθεσιμότητα Υπηρεσίας.

Προστασία της διαθεσιμότητα μιας υπηρεσίας σημαίνει εξασφάλιση της συνεχούς πρόσβαση μιας εξουσιοδοτημένης οντότητας στους υπολογιστικούς πόρους, στις διαδικασίες και στην πληροφορία. Αιτία για τη μη διαθεσιμότητα μιας υπηρεσίας μπορεί να αποτελέσει κάποια αδυναμία της υπηρεσίας, που σχετίζονται συνήθως με τεχνικούς περιορισμούς

⁴⁵ Απειλή (βλ. ενότητα 1.4.) είναι πιθανή ενέργεια ή γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή

(τεχνική αστοχία) ή κάποια απειλή που προέρχεται από ένα μη εξουσιοδοτημένο χρήστη. Στην πρώτη περίπτωση πρέπει να βρεθεί μια τεχνολογική λύση για την αντιμετώπιση των τεχνικών περιορισμών. Αντίθετα, στη δεύτερη περίπτωση το ζητούμενο είναι να μπορέσει να αντιμετωπιστεί, με τη λήψη των κατάλληλων μέτρων, το ενδεχόμενο ένας μη εξουσιοδοτημένος χρήστης να παρεμποδίσει τη συνεχή πρόσβαση του εξουσιοδοτημένου χρήστη. Φυσικά, εμπόδιο δεν θα πρέπει να αποτελέσουν ούτε και τα ίδια τα μέτρα που θα ληφθούν.

Στην περίπτωση των υπηρεσιών διαδικτύου, η διαθεσιμότητα μιας υπηρεσίας εξαρτάται και από τη διαθεσιμότητα των υπηρεσιών που την υποστηρίζουν. Αυτός είναι ένας επιπλέον λόγος, για τον οποίο μια υπηρεσία πρέπει να γνωρίζει την πολιτική ασφάλειας της άλλης. Τέλος, είναι ανάγκη να καθοριστεί ένας ασφαλής τρόπος, έτσι ώστε μια υπηρεσία διαδικτύου να είναι διαθέσιμη σε ένα πελάτη ή μια υπηρεσία, όταν η πρόσβαση γίνεται διαμέσου μιας άλλης υπηρεσίας.

5.5.4. Εμπιστευτικότητα και εγκυρότητα του λογισμικού.

Η εμπιστευτικότητα του λογισμικού μιας υπηρεσίας σχετίζεται κυρίως με τα πνευματικά δικαιώματα του δημιουργού της. Οι υπηρεσίες διαδικτύου δεν παρουσιάζουν κάποια ιδιαιτερότητα σε σύγκριση με άλλες μορφές λογισμικού ως προς τα πνευματικά δικαιώματα, ως εκ τούτου δεν κρίνεται αναγκαία η λεπτομερέστερη ανάλυση του ζητήματος. Η εγκυρότητα του λογισμικού αφορά στην αποτροπή της μη εξουσιοδοτημένης τροποποίησης και σχετίζεται με επιθέσεις που τροποποιούν τον κώδικα ενός αρχείου της εφαρμογής (π.χ. επιθέσεις με ιομορφικό λογισμικό). Στην περίπτωση αυτή υπάρχει μια σημαντική ιδιαιτερότητα των υπηρεσιών διαδικτύου.

Οι υπηρεσίες διαδικτύου είναι περισσότερο ευάλωτες στις απειλές που έχουν ως στόχο να προσβάλουν την ακεραιότητα του λογισμικού. Ο σημαντικότερος λόγος είναι ότι υπάρχει αρκετή πληροφορία διαθέσιμη στο υποκείμενο που σχεδιάζει να επιτεθεί. Το WSDL αρχείο με την περιγραφή της υπηρεσίας, στην ουσία μπορεί δώσει λεπτομερείς πληροφορίες στον επιτιθέμενο που θέλει να εισβάλει στο σύστημα. Επομένως, είναι απαραίτητη από τους διαχειριστές η συχνή πραγματοποίηση ελέγχων ασφάλειας με τη βοήθεια εργαλείων ανίχνευσης εισβολών, αναλυτών ακεραιότητας αρχείων κ.λπ.

5.5.5. Μη αποποίηση της ευθύνης.

Η μη αποποίηση της ευθύνης ενός υποκειμένου σημαίνει την αποδοχή οποιασδήποτε ενέργειας προέρχεται από το ίδιο. Σε μια συναλλαγή είναι απαραίτητο ο πελάτης να μην μπορεί να αρνηθεί μια ενέργεια για την οποία είναι υπεύθυνος, το ίδιο και ο χορηγός της υπηρεσίας. Στην περίπτωση των υπηρεσιών διαδικτύου, είναι σημαντικό μια οντότητα που αποστέλλει ένα XML μήνυμα να μπορεί να το αποδείξει, χωρίς να μπορεί να το αρνηθεί η οντότητα που το έλαβε. Αυτή η δυνατότητα αναφέρεται ως μη αποποίηση της ευθύνης του δέκτη (non-repudiation of receipt). Εξίσου, σημαντικό όμως είναι και για την οντότητα που λαμβάνει ένα XML μήνυμα να μπορεί να αποδείξει ότι το έλαβε, ακόμα και αν ο αποστολέας του το αρνείται. Η δυνατότητα αυτή αναφέρεται ως μη αποποίηση της ευθύνης του αποστολέα (non-repudiation of origin). Στις υπηρεσίες διαδικτύου είναι απαραίτητη και η εξασφάλιση της μη αποποίησης της ευθύνης της υπηρεσίας που μπορεί να προωθεί το μήνυμα ενός πελάτη (ή μιας υπηρεσίας) σε μια άλλη υπηρεσία.

5.6. Τι είναι μηχανισμός ασφαλείας.

Ένα γεγονός κατά τη διάρκεια του οποίου μια ή περισσότερες από τις απαιτήσεις ασφάλειας καταστρατηγούνται, αποτελεί παραβίαση (violation). Ένα μέσο προστασίας (safeguard), είναι ένα μέτρο σχεδιασμένο με σκοπό να εμποδίσει μια παραβίαση ή να μειώσει τις επιπτώσεις της. Κάθε μέσο προστασίας μπορεί να θεωρηθεί ότι προσφέρει μια υπηρεσία ασφάλειας. Ο τρόπος με τον οποίο ένα μέσο προστασίας λειτουργεί ονομάζεται μηχανισμός ασφαλείας [Π. κριτική, Λ., 2001].

5.7. Επίπεδα εφαρμογής μηχανισμών ασφαλείας.

Η στρωματοποιημένη αρχιτεκτονική που χρησιμοποιείται στο Internet, δηλαδή η οικογένεια πρωτοκόλλων TCP/IP, καθορίζει τέσσερα επίπεδα [Αποστολόπουλος, 1997]. Αυτά είναι:

1. Το επίπεδο πρόσβασης στο δίκτυο, που ασχολείται με τη μετάδοση των σημάτων (signals) κατά μήκος του δικτύου.
2. Το επίπεδο διαδικτύου, που ασχολείται με τη δρομολόγηση των πακέτων.
3. Το επίπεδο μεταφοράς, που ασχολείται με την παράδοση μηνυμάτων από άκρη σε άκρη.

4. Το επίπεδο εφαρμογής, που περιλαμβάνει προγράμματα και υπηρεσίες που χρησιμοποιούν το δίκτυο, όπως για παράδειγμα ηλεκτρονικό ταχυδρομείο.

Το ζήτημα της ασφάλειας στο Διαδίκτυο [Γκρίζαλης Στ., 2002 (1)] αφορά στο σχεδιασμό και την εφαρμογή μηχανισμών ασφάλειας, που μπορούν να εφαρμοστούν στα επίπεδα 2, 3, και 4 της αρχιτεκτονικής TCP/IP. (Στο επίπεδο 1 η ασφάλεια, σχετίζεται με ιδιότητες του καλωδίου και ως εκ τούτου απασχολεί κυρίως τους οργανισμούς που παρέχουν τηλεπικοινωνιακές υπηρεσίες).

Στην ενότητα αυτή, γίνεται μια σύντομη αναφορά στην αντιμετώπιση του ζητήματος της ασφάλειας σε καθένα από τα επίπεδα 2, 3 και 4.

5.6.1. Επίπεδο Διαδικτύου.

Στο επίπεδο διαδικτύου, υπάρχει το πρωτόκολλο IP, που αναλαμβάνει τη δρομολόγηση των πακέτων (που ονομάζονται datagrams) από τις πηγές στους προορισμούς τους. Οι μηχανισμοί ασφαλείας που ενσωματώνει η τελευταία έκδοση του πρωτοκόλλου IP (IPv6), παρέχουν:

- ✓ Δυνατότητα αυθεντικοποίησης της προέλευσης ενός datagram. Αυθεντικοποίηση είναι η διαδικασία με την οποία επιβεβαιώνεται η ταυτότητα μιας οντότητας από μια άλλη. Στην προκειμένη περίπτωση, ο παραλήπτης του datagram, μπορεί να επιβεβαιώσει την οντότητα του δημιουργού του.
- ✓ Δυνατότητα ανακάλυψης αν ένα datagram έχει τροποποιηθεί κατά τη μετάδοση.
- ✓ Δυνατότητα εξασφάλισης ότι μόνο οι νόμιμοι αποδέκτες ενός datagram, μπορούν να έχουν πρόσβαση στο περιεχόμενό του.
- ✓ Προαιρετική δυνατότητα για μη αποποίηση της ευθύνης του αποστολέα ενός datagram.

Εκ πρώτης όψεως, οι μηχανισμοί ασφαλείας στο επίπεδο πρωτοκόλλου διαδικτύου υπόσχονται να καλύψουν, σε κάποιο βαθμό, όλες τις απαιτήσεις ασφαλείας, με εξαίρεση τη διαθεσιμότητα μιας υπηρεσίας και τη μη αποποίηση της ευθύνης του παραλήπτη. Εντούτοις, όπως θα αναλυθεί στο επόμενο κεφάλαιο, οι μηχανισμοί αυτοί δεν είναι κατάλληλοι στην περίπτωση των υπηρεσιών διαδικτύου.

5.6.2. Επίπεδο Μεταφοράς.

Το επίπεδο μεταφοράς, ασχολείται με την παράδοση μηνυμάτων από μια πηγή σε ένα προορισμό. Στην περίπτωση των υπηρεσιών διαδικτύου η μετάδοση των SOAP μηνυμάτων

γίνεται μέσω του πρωτοκόλλου επιπέδου μεταφοράς TCP, που είναι πρωτόκολλο προσανατολισμένο σε σύνδεση. Η ασφάλεια μιας TCP σύνδεσης, απαιτεί την αυθεντικοποίηση των οντοτήτων που βρίσκονται στα δύο άκρα της σύνδεσης. Η πληροφορία αυθεντικοποίησης, δηλαδή η πληροφορία η οποία χρησιμοποιείται για να αποδειχθεί η ταυτότητα της μιας οντότητας στην άλλη οντότητα λέγεται διαπιστευτήριο (credential). Όταν ολοκληρωθεί η διαδικασία της αμοιβαίας αυθεντικοποίησης, με την επίδειξη των διαπιστευτηρίων των δύο οντοτήτων, οι δύο οντότητες είναι έτοιμες να ανταλλάξουν μηνύματα. Ένας ασφαλής μηχανισμός για την αποστολή των μηνυμάτων είναι η κρυπτογράφηση. Τα κρυπτογραφημένα μηνύματα δεν επιτρέπουν την πρόσβαση στο περιεχόμενό τους σε οντότητες που δεν γνωρίζουν το κλειδί της κρυπτογράφησης. Η κρυπτογραφία, με τη βοήθεια μονόδρομων συναρτήσεων, που ονομάζονται συναρτήσεις κατακερματισμού (hash) μπορεί να χρησιμοποιηθεί για τον έλεγχο της ακεραιότητας ενός μηνύματος. Οι μηχανισμοί αυθεντικοποίησης, κρυπτογράφησης και ελέγχου της ακεραιότητας θα περιγραφούν αναλυτικότερα στο επόμενο κεφάλαιο.

Με μια πρώτη ματιά, οι απαιτήσεις ασφάλειας των υπηρεσιών διαδικτύου που δύνανται να καλυφθούν με την εφαρμογή των παραπάνω μηχανισμών είναι βασικά οι απαιτήσεις για εγκυρότητα και εμπιστευτικότητα της πληροφορίας που μεταδίδεται από μια υπηρεσία σε μια άλλη (point-to-point). Αυτό σημαίνει, ότι παραμένει ανικανοποίητη η απαίτηση για end-to-end εξασφάλιση της πληροφορίας, το ίδιο και η απαίτηση για μη αποποίηση της ευθύνης και διαθεσιμότητα της υπηρεσίας.

5.6.3. Επίπεδο Εφαρμογής.

Στο επίπεδο εφαρμογής το *de facto* πρωτόκολλο που χρησιμοποιείται για την επικοινωνία των υπηρεσιών διαδικτύου, είναι το HTTP. Οι μηχανισμοί ασφάλειας στο επίπεδο εφαρμογής, εφαρμόζονται στο SOAP μήνυμα, που στέλνεται μέσω μιας HTTP αίτησης (ή απόκρισης). Με την ενσωμάτωση των μηχανισμών ασφάλειας στο ίδιο το μήνυμα [Hartman, 2002], δύναται να προστατευτεί η πληροφορία που περιέχει το μήνυμα, σε όλη τη διαδρομή που ακολουθεί αυτό και η οποία μπορεί να περιλαμβάνει αρκετούς ενδιάμεσους (intermediaries). Με άλλα λόγια, ικανοποιείται η απαίτηση για end-to-end εμπιστευτικότητα και ακεραιότητα.

Επιπλέον, οι τεχνολογίες του επίπεδου εφαρμογής δεν υλοποιούν μόνο μηχανισμούς που καλύπτουν επαρκώς την απαίτηση για end-to-end ασφάλειας της πληροφορίας. Η γνώση της

επιχειρησιακής λογικής, όπως θα αναφερθεί και στο επόμενο κεφάλαιο, κάνει πιο εφικτό στο επίπεδο αυτό τον έλεγχο και την ανίχνευση επιθέσεων. Οι τελευταίες, μπορεί να αφορούν σε ενέργειες που έχουν στόχο να προσβάλλουν το λογισμικό (malicious attacks) ή τη διαθεσιμότητα της υπηρεσίας (denial of service attacks).

Επομένως, στις απαιτήσεις ασφαλείας των υπηρεσιών διαδικτύου που δύνανται να καλυφθούν από τους μηχανισμούς του επίπεδο εφαρμογής, περιλαμβάνονται όλες όσες αναφέρθηκαν στην ενότητα 5.5. του κεφαλαίου. Το γεγονός αυτό όμως, δεν σημαίνει πως η αντιμετώπιση της ασφάλειας σε επίπεδο εφαρμογής είναι πάντα η βέλτιστη λύση.

5.8. Συμπέρασμα.

Οι βασικές απαιτήσεις ασφάλειας στο μοντέλο των υπηρεσιών διαδικτύου είναι α) η εξασφάλιση της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητας της πληροφορίας που ανταλλάσσεται μέσω των SOAP μηνυμάτων ή είναι αποθηκευμένη σε καταλόγους με τη μορφή WSDL εγγράφων, β) η εξασφάλιση της διαθεσιμότητας των υπηρεσιών, γ) η εξασφάλιση της εγκυρότητας και εμπιστευτικότητας του λογισμικού των υπηρεσιών, και δ) η εξασφάλιση της μη αποποίησης της ευθύνης της οντότητας πελάτη και της οντότητας χορηγού της υπηρεσίας.

Η ασφάλεια στο διαδίκτυο περιλαμβάνει μηχανισμούς των επιπέδων εφαρμογής, μεταφοράς και διαδικτύου. Οι μηχανισμοί των επιπέδων μεταφοράς και διαδικτύου δεν μπορούν σε αρκετές περιπτώσεις να παρέχουν λύσεις για την ασφάλεια των υπηρεσιών διαδικτύου, όπως το επιτυγχάνουν στις παραδοσιακές υπηρεσίες client-server. Οι ιδιαίτερότητες που υπάρχουν, ιδιαίτερα στη δομή μιας τοπολογίας από συνεργαζόμενες υπηρεσίες διαδικτύου, υποδεικνύουν την αντιμετώπιση των περισσότερων ζητημάτων ασφάλειας σε επίπεδο εφαρμογής.



ΚΕΦΑΛΑΙΟ 6^ο : ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΙΣ ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ

6.1. Εισαγωγή.

Ο τομέας της ασφάλειας των υπηρεσιών διαδικτύου είναι αναμφισβήτητα μια ερευνητική περιοχή που απασχολεί και πρόκειται να απασχολήσει ακόμα περισσότερο τα επόμενα χρόνια, ένα μεγάλο μέρος της επιστημονικής κοινότητας. Οι υπηρεσίες διαδικτύου αποτελούν ένα νέο παράδειγμα στο χώρο του διαδικτύου, που έχει επιφέρει μεγάλες αλλαγές στη φιλοσοφία του, όχι όμως στη δομή του. Το γεγονός αυτό επιτρέπει την αντιμετώπιση του ζητήματος της ασφάλειας με βάση υπάρχουσες τεχνικές και μεθόδους. Ωστόσο, δεν λείπουν οι ιδιαιτερότητες, που απαιτούν στις περισσότερες περιπτώσεις την επέκταση ή τον κατάλληλο συνδυασμό μεθόδων και τεχνικών.

Στο προηγούμενο κεφάλαιο εντοπίστηκαν οι βασικές απαιτήσεις ασφάλειας στο μοντέλο των υπηρεσιών διαδικτύου. Επίσης, αναφέρθηκαν τα τρία επίπεδα της αρχιτεκτονικής του Διαδικτύου, στα οποία μπορεί να αντιμετωπιστεί το ζήτημα της ασφάλειας. Στο παρόν κεφάλαιο αναλύονται οι βασικοί μηχανισμοί ασφάλειας κάθε επιπέδου και περιγράφονται οι κυριότερες τεχνολογίες που τους υποστηρίζουν. Επίσης, επισημαίνονται τα πλεονεκτήματα και τα μειονεκτήματα της κάθε τεχνολογίας.

6.2. Επίπεδο Διαδικτύου.

Η αντιμετώπιση του ζητήματος της ασφάλειας σε επίπεδο διαδικτύου, εμφανίζει αρκετές δυσκολίες στην περίπτωση των υπηρεσιών διαδικτύου. Όπως αναφέρθηκε στην ενότητα 5.6.1., το πρωτόκολλο IP στην τελευταία του έκδοση (IPv6), περιλαμβάνει μηχανισμούς, που παρέχουν υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και μη-αποποίησης αποστολής. Ωστόσο, αυτοί οι μηχανισμοί ασφαλείας δεν προσφέρονται από τεχνικής άποψης για την ασφάλεια των υπηρεσιών διαδικτύου και επιπλέον δεν παρέχουν επαρκή υποστήριξη για την υλοποίηση μιας πολιτικής ασφαλείας σε επίπεδο διαδικτύου.

6.2.1. Πρωτόκολλο IPSP - Μηχανισμοί ασφαλείας.

Η τελευταία έκδοση του πρωτοκόλλου IP (IPv6), ενσωματώνει δύο ισχυρούς κρυπτογραφικούς μηχανισμούς ασφαλείας, διαθέσιμους σε χρήστες που επιθυμούν υπηρεσίες



ασφαλείας. Οι μηχανισμοί αυτοί καθορίζονται από την IPv6 αρχιτεκτονική ασφαλείας και αφορούν στην αυθεντικοποίηση και στην κρυπτογράφησή δεδομένων. Επίσης, αποτελούν μέρη του IP Security Protocol (IPSP). Οι δύο μηχανισμοί ασφαλείας του IPSP είναι [Γκρίζαλης Στ., 2002 (1)]:

- Ο μηχανισμός Authentication Header (AH), που παρέχει αυθεντικοποίηση προέλευσης δεδομένων και υπηρεσίες ακεραιότητας δεδομένων χωρίς σύνδεση. Η επικεφαλίδα AH επιτρέπει στον παραλήπτη ενός IP πακέτου να επιβεβαιώνει την οντότητα του δημιουργού του και να εξετάζει αν έχει λάβει χώρα τροποποίηση του πακέτου κατά τη διάρκεια της μετάδοσης.
- Ο μηχανισμός Encapsulating Security Payload (ESP), που παρέχει υπηρεσίες εμπιστευτικότητας δεδομένων χωρίς σύνδεση. Εξασφαλίζει ότι μόνον οι νόμιμοι αποδέκτες ενός IP πακέτου έχουν τη δυνατότητα να το αναγνώσουν.

Το IPSP δύναται να χρησιμοποιηθεί για τη δημιουργία ασφαλών συνδέσεων μεταξύ συγκεκριμένων κόμβων, επιτρέποντας ακόμα και τη δημιουργία ενός ιδιωτικού εικονικού δικτύου (VPN)⁴⁶. Σε κάθε τέτοια σύνδεση η ακεραιότητα, η αυθεντικότητα και η εμπιστευτικότητα των πληροφοριών που μεταδίδονται εξασφαλίζεται μέσω των μηχανισμών AH και ESP. Επίσης, ανάλογα με την επιλογή του κρυπτογραφικού αλγορίθμου και τον τρόπο αξιοποίησης των κρυπτογραφικών κλειδιών, ο μηχανισμός AH μπορεί να παρέχει και υπηρεσίες μη-αποποίησης αποστολής (non-repudiation of origin).

6.2.2. IPSP και Υπηρεσίες Διαδικτύου.

Οι λόγοι που οι μηχανισμοί της αρχιτεκτονικής IPv6 δεν προσφέρονται στην περίπτωση των υπηρεσιών διαδικτύου είναι αρκετοί και σημαντικοί. Ορισμένοι είναι καθαρά τεχνικοί, ενώ άλλοι σχετίζονται με τις ιδιαιτερότητες των υπηρεσιών διαδικτύου. Συγκεκριμένα :

- Η αξιοποίηση των μηχανισμών ασφαλείας του IPSP απαιτεί τη χρήση και ανάπτυξη νέου TCP/IP λογισμικού, αφού η ασφάλεια που παρέχουν στηρίζεται ακριβώς στην αναβάθμιση αυτού [Γκρίζαλης Στ., 2002 (1)]. Μια τέτοια διαδικασία εκτός από δαπανηρή, δεν υποστηρίζεται από όλα τα λειτουργικά συστήματα, πράγμα που έρχεται σε αντίθεση με τη βασική φιλοσοφία των υπηρεσιών διαδικτύου, που υπόσχονται διαλειτουργικότητα και ανεξαρτησία από λειτουργικά συστήματα και πλατφόρμες.

⁴⁶ Ένα VPN αποτελεί μια λογική σύνδεση μεταξύ υπολογιστών που μπορούν ανταλλάσσουν με ασφάλεια δεδομένα μέσω ενός δημοσίου δικτύου όπως το Internet.

- Η εφαρμογή κρυπτογραφικών τεχνικών σε επίπεδο διαδικτύου καθιστά το δίκτυο πιο αργό.
- Το επίπεδο δικτύου (Internet), γενικά, δεν μπορεί να ξεχωρίσει IP πακέτα λογισμικού που ανήκουν σε διαφορετικές συνόδους και διαδικασίες εφαρμογών [Γκρίζαλις Στ.. 2002 (1)]. Αυτό έχει ως αποτέλεσμα να χρησιμοποιούνται τα ίδια κρυπτογραφικά κλειδιά και οι ίδιες πολιτικές πρόσβασης σε όλα τα IP πακέτα που προορίζονται για ένα συγκεκριμένο host. Το γεγονός αυτό δεν παρέχει στις υπηρεσίες διαδικτύου την επιθυμητή λειτουργικότητα και ασφάλεια.
- Μπορεί να υπάρχουν και περιπτώσεις συναλλαγών στις υπηρεσίες διαδικτύου που να μην απαιτούν ιδιαίτερη ασφάλεια. Επομένως, είναι περιττό να εφαρμόζονται μηχανισμοί ασφάλειας σε επίπεδο διαδικτύου. [Nagaraj, 2003]
- Τέλος, ο μηχανισμός AH δεν μπορεί να παρέχει αυθεντικοποίηση του πελάτη μιας υπηρεσίας διαδικτύου, όταν η αίτηση του προωθείται στην υπηρεσία από κάποιον ενδιάμεσο (intermediary).

6.2.3. Φίλτρα πακέτων (Packet Filters).

Μια τεχνολογική λύση που χρησιμοποιούν αρκετοί οργανισμοί για την ασφάλεια ενός πληροφοριακού συστήματος, που είναι εκτεθειμένο στο διαδίκτυο, είναι η πύλη ασφαλείας (firewall). Το firewall είναι ένα σύστημα που τοποθετείται μεταξύ ενός εσωτερικού δικτύου, που πρέπει να προστατευτεί, και του διαδικτύου. Υπάρχουν δύο τύποι firewall. Αυτοί είναι τα φίλτρα πακέτων (packet filters) και οι ασφαλείς πύλες εφαρμογών (application firewalls). Μόνο τα πρώτα λειτουργούν σε επίπεδο διαδικτύου.

Τα φίλτρα πακέτων μπορούν να λάβουν αποφάσεις σε επίπεδο δικτύου, με βάση δηλαδή τις πληροφορίες ενός IP datagram. Τα φίλτρα πακέτων, διαμορφώνονται κατάλληλα, ώστε να επιτρέπουν την κίνηση πακέτων μόνο μεταξύ έμπιστων υπολογιστών. Οποιαδήποτε άλλα πακέτα απορρίπτονται.

Τα φίλτρα πακέτων δεν αποτελούν λύση κατάλληλη για τις υπηρεσίες διαδικτύου, βασικά για τον εξής λόγο. Αυτός είναι ότι η οικοδόμηση εμπιστοσύνης στο μοντέλο των υπηρεσιών διαδικτύου είναι ένα ζήτημα που δεν έχει λυθεί ακόμα. Το ίδιο ισχύει φυσικά και για τη μεταβίβαση εμπιστοσύνης, που είναι επίσης απαραίτητη όταν μια αίτηση προωθείται από τον πελάτη στην υπηρεσία μέσω μιας ενδιάμεσης οντότητας.



6.3. Επίπεδο Μεταφοράς.

Στο επίπεδο μεταφοράς, οι τεχνολογίες που παρέχουν ασφάλεια σε μια σύνδεση, υλοποιούν υπηρεσίες, που εξασφαλίζουν: α) την αυθεντικοποίηση των οντοτήτων στα άκρα μιας σύνδεσης, β) την εμπιστευτικότητα των πληροφοριών κατά τη μεταφορά τους από το ένα άκρο της σύνδεσης στο άλλο και γ) την ακεραιότητα των πληροφοριών κατά τη μεταφορά τους από το ένα άκρο της σύνδεσης στο άλλο.

Το κλειδί στην παροχή αυτών των υπηρεσιών είναι η κρυπτογραφία. Ένα δημοφιλές πρωτόκολλο, που περιλαμβάνει μηχανισμούς ασφαλείας που χρησιμοποιούν την κρυπτογραφία για να παρέχουν τέτοιου είδους υπηρεσίες, είναι το SSL. Σύμφωνα με τον Hartman [Hartman, 2002], το πρωτόκολλο SSL σε συνδυασμό με τα πιστοποιητικά X.509 και τους κωδικούς MAC, αποτελεί μια καλή λύση για την εξασφάλιση της επικοινωνίας δύο υπηρεσιών διαδικτύου. Συγκεκριμένα, ο Hartman προτείνει:

- Το πρωτόκολλο SSL με χρήση των X.509 πιστοποιητικών, ως μηχανισμό για την αμοιβαία αυθεντικοποίηση δύο υπηρεσιών διαδικτύου.
- Την SSL κρυπτογράφηση, ως τεχνική που εξασφαλίζει επαρκώς τη μη πρόσβαση τρίτων στο περιεχόμενο των μηνυμάτων που ανταλλάσσονται οι δύο υπηρεσίες.
- Το πρωτόκολλο SSL με χρήση MACs (Message Authentication Codes), ως μηχανισμό για τον έλεγχο της ακεραιότητας των μηνυμάτων που ανταλλάσσονται οι δύο υπηρεσίες.

Τα παραπάνω συνοψίζονται στον πίνακα 6.1.

Απαιτήσεις	Μηχανισμοί	Τεχνολογίες
Εμπιστευτικότητα της πληροφορίας (point-to-point)	Αμοιβαία αυθεντικοποίηση πελάτη-υπηρεσίας.	SSL Handshake, X.509
	Κρυπτογράφηση των μηνυμάτων.	SSL Record, Encryption Algorithm
Εγκυρότητα της πληροφορίας (point-to-point)	Αμοιβαία αυθεντικοποίηση πελάτη-υπηρεσίας.	SSL Handshake, X.509
	Έλεγχος ακεραιότητας των μηνυμάτων.	SSL Record, MACs

Πίνακας 6.1.: Μηχανισμοί ασφάλειας υπηρεσιών διαδικτύου του επιπέδου μεταφοράς.

Στη συνέχεια θα παρουσιαστούν λεπτομερώς, όλες οι τεχνολογίες που αναφέρθηκαν παραπάνω. Προηγουμένως, όμως, είναι απαραίτητο να δοθεί μια σύντομη περιγραφή των δύο



βασικών μεθόδων κρυπτογράφησης, η οποία είναι απαραίτητη για την κατανόηση των μηχανισμών ασφαλείας του πρωτοκόλλου SSL.

6.3.1. Κρυπτογραφία.

Κρυπτογραφία είναι η επιστήμη που χρησιμοποιεί τα μαθηματικά για να κρυπτογραφεί (encrypt) και να αποκρυπτογραφεί (decrypt) δεδομένα. Η κρυπτογραφία επιτρέπει σε κάποιον να αποθηκεύσει τις ευαίσθητες πληροφορίες του ή να τις μεταδώσει μέσω ενός δικτύου που είναι επισφαλές (όπως το διαδίκτυο), έτσι ώστε να μην μπορούν να γίνουν κατανοητές από κανέναν, παρά μόνο από τον παραλήπτη για τον οποίο προορίζονται. Ο μαθηματικός αλγόριθμος που χρησιμοποιείται στην κρυπτογράφηση ονομάζεται cipher. Κλειδί είναι μια τιμή που χρησιμοποιεί ο κρυπτογραφικός αλγόριθμος για να παράγει ένα συγκεκριμένο κρυπτογραφημένο μήνυμα (ciphertext). Τα κλειδιά είναι συνήθως μεγάλοι σε μήκος αριθμοί.

Στην κλασική ή συμμετρική κρυπτογραφία ο αποστολέας χρησιμοποιεί ένα κλειδί για να κρυπτογραφήσει ένα έγγραφο, το οποίο κλειδί πρέπει να το γνωρίζει και ο παραλήπτης για να μπορέσει να το αποκρυπτογραφήσει. Στην περίπτωση αυτή, δηλαδή, για να επικοινωνήσουν αποστολέας και παραλήπτης «μοιράζονται» το ίδιο κλειδί. Το αδύνατο σημείο της μεθόδου αυτής είναι να υποστεί κλοπή ο ενδιάμεσος που θα χρησιμοποιηθεί για να μεταφέρει το κλειδί. Για το λόγο αυτό αναπτύχθηκαν αλγόριθμοι που στηρίζονται σε ένα ζεύγος κλειδιών, το δημόσιο και το ιδιωτικό κλειδί.

Η κρυπτογραφία δημοσίου κλειδιού στηρίζεται στη μέθοδο της δημόσιας κρυπτογράφησης (public key encryption), που ανακαλύφθηκε από τους Whitfield Diffie και Martin Hellman. Η δημόσια κρυπτογράφηση καθορίζει τη δημιουργία ενός κλειδιού κρυπτογράφησης και ενός κλειδιού αποκρυπτογράφησης. Τα ιδιάζοντα μαθηματικά αυτών των κλειδιών είναι τέτοια, ώστε το ένα κλειδί να μην μπορεί να παραχθεί από το άλλο. Επομένως, αυτός που γνωρίζει το κλειδί της κρυπτογράφησης δεν γνωρίζει το κλειδί της αποκρυπτογράφησης και συνεπώς δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Μ' αυτόν τον τρόπο, ο αποστολέας δεν χρειάζεται πλέον να ανησυχεί για την επιλογή του ενδιάμεσου που θα παραδώσει το κλειδί της κρυπτογράφησης. Στην πραγματικότητα, μπορεί άνετα να το δημοσιοποιήσει. Για αυτό το λόγο, το κλειδί της κρυπτογράφησης ονομάζεται δημόσιο κλειδί (public key), ενώ αντίθετα το κλειδί της αποκρυπτογράφησης ονομάζεται ιδιωτικό κλειδί (private key). Το δημόσιο και το ιδιωτικό κλειδί αποτελούν ένα ζεύγος κλειδιών. Το πρώτο δίδεται από το δημιουργό του ζεύγους κλειδιών, για να χρησιμοποιηθεί από άλλες οντότητες.



προκειμένου να κρυπτογραφήσουν τα δεδομένα που θέλουν να του αποστείλουν. Καμία οντότητα όμως δεν μπορεί να χρησιμοποιήσει το κλειδί για να αποκρυπτογραφήσει τα δεδομένα αυτά. Το ιδιωτικό κλειδί το γνωρίζει μόνο ο δημιουργός του ζεύγους, για να μπορεί μόνο αυτός να αποκρυπτογραφεί τις πληροφορίες που έχουν κρυπτογραφηθεί με το αντίστοιχο δημόσιο κλειδί.

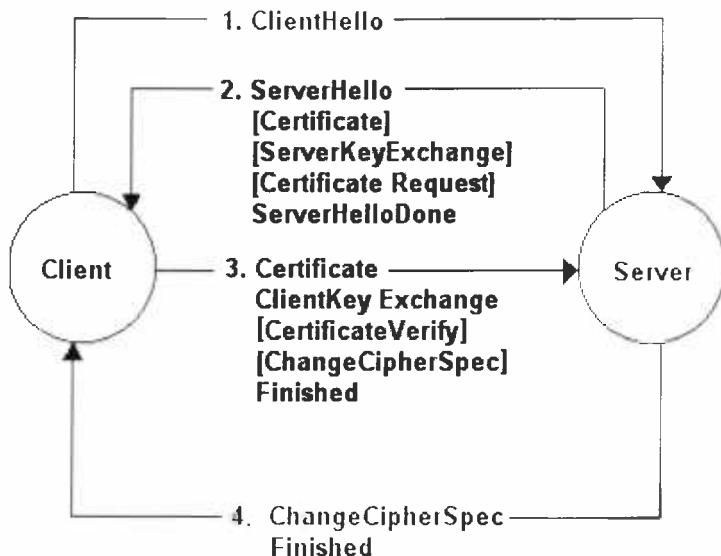
6.3.2. Πρωτόκολλο SSL - Μηχανισμοί ασφαλείας.

Το πρωτόκολλο SSL είναι πρωτόκολλο επιπέδου μεταφοράς που παρέχει ασφάλεια TCP/IP σύνδεσης, η οποία έχει τρεις βασικές ιδιότητες [Γκρίτζαλης Στ., 2002 (1)]:

- Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία, χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού.
- Επιτυγχάνεται η εμπιστευτικότητα των δεδομένων που μεταδίδονται, αφού η σύνδεση κρυπτογραφείται διαφανώς μετά από μια αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου.
- Προστατεύεται η ακεραιότητα των δεδομένων που μεταδίδονται, καθώς τα μηνύματα αυθεντικοποιούνται διαφανώς και ελέγχονται ως προς την ακεραιότητα τους κατά τη μετάδοση.

Το πρωτόκολλο SSL αποτελείται από το SSL record protocol και διάφορα πρωτόκολλα πάνω από αυτό, εκ των οποίων το σημαντικότερο είναι το SSL handshake protocol. Το SSL record protocol παρέχει υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας δεδομένων, σε μία προσανατολισμένη στη σύνδεση αξιόπιστη υπηρεσία μεταφοράς, όπως αυτή που παρέχεται από το TCP. Το SSL handshake protocol, είναι ένα πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών, το οποίο διαπραγματεύεται, αρχικοποιεί και συγχρονίζει τις παραμέτρους ασφαλείας και την αντίστοιχη κατάσταση στα δύο άκρα της σύνδεσης. Μετά την ολοκλήρωση του SSL handshake protocol, τα δεδομένα των εφαρμογών μπορούν να αποστέλλονται μέσω του SSL record protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφαλείας και κατάστασης. Το SSL handshake protocol περιλαμβάνει τέσσερα βήματα, τα οποία περιγράφονται στο σχήμα 6.1.





Σχήμα 6.1.: Το πρωτόκολλο SSL Handshake.

Τα Hello μηνύματα του πελάτη και του εξυπηρετητή χρησιμοποιούνται για τη συμφωνία στοιχείων ασφάλειας της σύνδεσης. Μετά την αποστολή του μηνύματος Hello ο εξυπηρετητής μπορεί να στείλει προαιρετικά το πιστοποιητικό του στον πελάτη για να αυθεντικοποιηθεί. Αν ο εξυπηρετητής δε διαθέτει πιστοποιητικό μπορεί να αποστείλει ένα μήνυμα ανταλλαγής κλειδιού. Αν ο εξυπηρετητής αυθεντικοποιηθεί μπορεί, προαιρετικά, να ζητήσει από τον πελάτη ένα πιστοποιητικό ανάλογα με τον αλγόριθμο κρυπτογράφησης που συμφωνήθηκε κατά τη διάρκεια της ανταλλαγής των Hello μηνυμάτων. Αφού αποστείλει αυτά τα μηνύματα, ο εξυπηρετητής περιμένει για την απάντηση του πελάτη. Αυτό σημαίνει ότι αν ο εξυπηρετητής έχει ζητήσει από τον πελάτη ένα πιστοποιητικό και ο τελευταίος το διαθέτει, τότε το αποστέλλει. Διαφορετικά στέλνει ένα μήνυμα που υποδηλώνει στον εξυπηρετητή την έλλειψη πιστοποιητικού. Στη συνέχεια ο πελάτης στέλνει το μήνυμα ανταλλαγής κλειδιού. Το περιεχόμενο του μηνύματος εξαρτάται από τον αλγόριθμο δημόσιου κλειδιού που συμφωνήθηκε κατά τη διάρκεια ανταλλαγής των Hello μηνυμάτων. Τέλος, ο πελάτης στέλνει ένα μήνυμα στον εξυπηρετητή υποδηλώνοντας τους κρυπτογραφικούς αλγόριθμους που θα χρησιμοποιήσει στη συνέχεια. Το στάδιο αυτό ολοκληρώνεται με την αποστολή ενός Finish μηνύματος, το οποίο είναι πάντα το πρώτο μήνυμα που προστατεύεται με τους τελευταία συμφωνημένους αλγορίθμους. Σε απάντηση, ο εξυπηρετητής στέλνει ένα μήνυμα στον πελάτη υποδηλώνοντας τους αλγορίθμους που θα χρησιμοποιήσει αυτός, συνοδευόμενο επίσης από ένα Finish μήνυμα.

6.3.3. Πιστοποιητικά X.509.

Ένα πιστοποιητικό είναι ένα ψηφιακό τεκμήριο το οποίο αντιστοιχίζει μοναδικά ένα δημόσιο κλειδί σε ένα χρήστη. Ένα πιστοποιητικό εκδίδεται από μια Αρχή Πιστοποίησης (Certification Authority) που είναι η κεντρική οντότητα ενός συστήματος PKI (Public Key Infrastructure), το οποίο διαχειρίζεται πιστοποιητικά. Ένα πιστοποιητικό χρησιμεύει σαν διαπιστευτήριο για την αυθεντικοποίηση ενός πελάτη, από μια υπηρεσία που χρησιμοποιεί κρυπτογραφικές τεχνικές στη μεταξύ τους επικοινωνία. Ένα πιστοποιητικό γενικά αποτελείται από τρία στοιχεία:

- Ένα δημόσιο κλειδί.
- Πληροφορίες πιστοποίησης, δηλαδή στοιχεία της ταυτότητας του χρήστη.
- Μια ή περισσότερες ψηφιακές υπογραφές⁴⁷.

Ο σκοπός της ψηφιακής υπογραφής σε ένα πιστοποιητικό είναι για να δηλώσει ότι οι πληροφορίες πιστοποίησης έχουν επιβεβαιωθεί από κάποιο άλλο άτομο ή οντότητα. Η ψηφιακή υπογραφή δεν αποδεικνύει την αυθεντικότητα ολόκληρου του πιστοποιητικού, αλλά βεβαιώνει ότι οι πληροφορίες της ταυτότητας αυτού που το έχει υπογράψει είναι σε αντιστοιχία με το δημόσιο κλειδί του πιστοποιητικού.

Το X.509 αποτελεί το πλαίσιο αυθεντικοποίησης που σχεδιάστηκε για την υποστήριξη των υπηρεσιών καταλόγου X.500⁴⁸ και περιλαμβάνεται στη σειρά προτύπων X που προτάθηκαν από τους οργανισμούς ISO και ITU. Ως πρότυπο υποστηρίζεται από πολλά πρωτοκόλλα, ανάμεσα στα οποία και το SSL.

6.3.4. Κωδικοί Αυθεντικοποίησης Μηνυμάτων (MACs).

Ένας κωδικός αυθεντικοποίησης μηνύματος (Message Authentication Code - MAC) είναι το αποτέλεσμα της εφαρμογής μιας μαθηματικής συνάρτησης, που χρησιμοποιεί ως παράμετρο ένα κρυπτογραφικό κλειδί, στα περιεχόμενα ενός μηνύματος. Το MAC είναι ένας αριθμός μήκους μερικών δυφιοσυλλαβών, που ωστόσο είναι εξαιρετικά ευαίσθητος σε μεταβολές του μορφότυπου των διφυών (bit-pattern) ενός μηνύματος. Πριν την αποστολή ενός μηνύματος, ο αποστολέας υπολογίζει το MAC του μηνύματος, αντικαθιστώντας με το μυστικό του κλειδί (συμμετρικό ή ιδιωτικό) την τιμή της παραμέτρου της συνάρτησης. Το

⁴⁷ Η ψηφιακή υπογραφή είναι μια σφραγίδα γνησιότητας, η οποία εγγυάται ότι ένα ηλεκτρονικό έγγραφο προέρχεται από ένα συγκεκριμένο αποστολέα. Ήταν περιγραφεί αναλυτικά στη συνέχεια.

⁴⁸ Το X.500 σχεδιάστηκε με σκοπό την παροχή υπηρεσιών καταλόγου παγκοσμίως και υιοθετήθηκε από πολλές εταιρίες, όπως Visa, MasterCard, Microsoft και Netscape.

MAC στέλνεται στη συνέχεια στον παραλήπτη μαζί με το μήνυμα. Ο παραλήπτης εφαρμόζει την ίδια μαθηματική συνάρτηση στο περιεχόμενο του μηνύματος αντικαθιστώντας την τιμή της παραμέτρου με το ίδιο κλειδί (στην περίπτωση της συμμετρικής κρυπτογράφησης) ή το δημόσιο κλειδί του αποστολέα (στην περίπτωση της δημόσιας κρυπτογράφησης). Αν το μήνυμα, έχει τροποποιηθεί κατά τη μετάδοση, ο αριθμός MAC που θα προκύψει από τον υπολογισμό αυτό, δεν θα ταιριάζει με τον αριθμό MAC που μεταδόθηκε από τον αποστολέα. Το πρωτόκολλο SSL στην περίπτωση αυτή ζητά την επαναμετάδοση του μηνύματος.

Οι μαθηματικές συναρτήσεις που χρησιμοποιούνται για τον υπολογισμό ενός MAC, συνήθως ονομάζονται συναρτήσεις κατακερματισμού (hash functions) ή αλγόριθμοι σύνοψης (Digest Algorithms). Το κύριο χαρακτηριστικό των συναρτήσεων κατακερματισμού είναι ότι είναι μονόδρομες. Επομένως, δεν υπάρχει αντίστροφη διαδικασία, τέτοια ώστε από το αποτέλεσμα που εξάγει μια συνάρτηση κατακερματισμού να μπορεί να προκύψει το αρχικό μήνυμα. Επίσης, οι συναρτήσεις σύνοψης εξασφαλίζουν ότι δεν μπορεί να βρεθεί άλλο μήνυμα, το οποίο να παράγει ίδια σύνοψη με αυτή που παράγει ένα δοσμένο μήνυμα.

6.3.5. SSL και Υπηρεσίες Διαδικτύου.

Το πρωτόκολλο SSL, όπως επισημαίνει ο Hartman, δύναται να χρησιμοποιηθεί για την εξασφάλιση της επικοινωνίας μεταξύ δύο υπηρεσιών διαδικτύου. Ωστόσο, δεν καλύπτει όλες τις απαιτήσεις ασφάλειας που αναφέρθηκαν στην ενότητα 5.5 της παρούσας εργασίας. Οι ελλείψεις του πρωτοκόλλου SSL, όπως επισημαίνονται από τον Hartman [Hartman, 2002] είναι :

- Μη υποστήριξη μηχανισμού για την εξασφάλιση της μη αποποίησης της ευθύνης. Μια υπηρεσία διαδικτύου δεν μπορεί να αποδείξει με τη βοήθεια του πρωτοκόλλου SSL, τη λήψη ή την αποστολή δεδομένων από ή προς μια άλλη υπηρεσία αντίστοιχα.
- Μη υποστήριξη μηχανισμού εξουσιοδότησης. Το πρωτόκολλο SSL παρέχει μόνο τη δυνατότητα αυθεντικοποίησης ενός πελάτη ή μιας υπηρεσίας, που είναι απλά ένα απαραίτητο βήμα πριν την εξουσιοδότηση. Η εξουσιοδότηση είναι η διαδικασία κατά την οποία αποφασίζεται αν η αυθεντικοποιημένη οντότητα επιτρέπεται να έχει πρόσβαση στην υπηρεσία και σε ποιους πόρους και λειτουργίες αυτής. Κατά τη διαδικασία της εξουσιοδότησης γίνεται εφαρμογή της πολιτικής ασφαλείας που αφορά στα δικαιώματα των χρηστών.



- Μη υποστήριξη μηχανισμού για παροχή ασφαλούς επικοινωνίας από άκρη σε άκρη (end-to-end). Έστω ότι κάποια δεδομένα, που στέλνει μια υπηρεσία διαδικτύου Α σε μια άλλη Β, προωθούνται από την Α στη Β, μέσω μιας υπηρεσίας διαδικτύου Γ. Τα δεδομένα αυτά στην περίπτωση που χρησιμοποιείται το πρωτόκολλο SSL πρέπει να αποκρυπτογραφηθούν και να επανακρυπτογραφηθούν για κάθε σκέλος της επικοινωνίας. Επομένως, ακόμα και αν η υπηρεσία Α είναι σίγουρη για την επικοινωνία της με την Γ, δεν είναι σίγουρη, απλά μπορεί να ευελπιστεί, ότι είναι ασφαλής και η επικοινωνία της Γ με την Β.

6.4. Επίπεδο εφαρμογής.

Όπως προκύπτει από την ανάλυση των επιπέδων διαδικτύου και μεταφοράς, οι υπάρχουσες τεχνολογίες και οι μηχανισμοί των επιπέδων αυτών, αδυνατούν να παρέχουν λύση στις απαιτήσεις των υπηρεσιών διαδικτύου για:

- εξασφάλιση της end-to-end εμπιστευτικότητας και εγκυρότητας της πληροφορίας που μεταδίδεται,
- εξασφάλιση της διαθεσιμότητας μιας υπηρεσίας,
- εξασφάλιση της εγκυρότητας του λογισμικού μιας υπηρεσίας και
- εξασφάλιση της μη αποποίησης της ευθύνης του αποστολέα και του δέκτη.

Οι μηχανισμοί ασφαλείας του επιπέδου εφαρμογής έρχονται να καλύψουν τις παραπάνω απαιτήσεις με την κατάλληλη υποστήριξη από υπάρχουσες και νέες τεχνολογίες. Στον πίνακα 6.2. απεικονίζεται μια προσπάθεια συγκέντρωσης των μηχανισμών και των τεχνολογιών που χρησιμοποιούνται στο επίπεδο εφαρμογής για την εξασφάλιση των παραπάνω απαιτήσεων.

Απαιτήσεις	Μηχανισμοί	Τεχνολογίες
Εμπιστευτικότητα της πληροφορίας (end-to-end)	Έλεγχος Πρόσβασης στην υπηρεσία ή στον κατάλογο υπηρεσιών.	<ul style="list-style-type: none"> ✓ X.509 ή Kerberos Tickets ✓ XKMS ✓ SAML ✓ XACML
	Κρυπτογράφηση των μηνυμάτων που ανταλλάσσονται.	<ul style="list-style-type: none"> ✓ XML Encryption

	Επίβλεψη (Monitoring).	✓ XML Application Firewall ✓ XML schema
Εγκυρότητα της πληροφορίας (end-to-end)	Έλεγχος Πρόσβασης στην υπηρεσία ή στον κατάλογο υπηρεσιών.	✓ X.509 ή Kerberos Tickets ✓ XKMS ✓ SAML ✓ XACML
	Έλεγχος ακεραιότητας των μηνυμάτων που ανταλλάσσονται.	✓ XML Digital Signatures ✓ Digest Algorithms
	Επίβλεψη (Monitoring).	✓ XML Application Firewall ✓ XML schema
Διαθεσιμότητα της Υπηρεσίας	Επίβλεψη (Monitoring).	✓ XML Application Firewall ✓ XML schema
	Έλεγχος Πρόσβασης στην υπηρεσία ή στον κατάλογο υπηρεσιών.	✓ X.509 ή Kerberos Tickets ✓ XKMS ✓ SAML ✓ XACML
Εγκυρότητα του λογισμικού της Υπηρεσίας	Έλεγχος Πρόσβασης στην υπηρεσία ή στον κατάλογο υπηρεσιών.	✓ X.509 ή Kerberos Tickets ✓ XKMS ✓ SAML ✓ XACML
	Επίβλεψη (Monitoring).	✓ XML Application Firewall ✓ XML schema
	Έλεγχος Ακεραιότητας Λογισμικού.	✓ Checksums
Μη αποποίηση της ευθύνης (παραλήπτη, αποστολέα, ενδιαμέσου)	Αποθήκευση και προώθηση μηνυμάτων από έμπιστο φορέα που παρέχει Υπηρεσία Μη-Αποποίησης	✓ XML Digital Signatures ✓ Time stamps

Πίνακας 6.2.: Μηχανισμοί ασφάλειας υπηρεσιών διαδικτύου επιπέδου εφαρμογής.

Οι μηχανισμοί ασφαλείας (βλ. Πίνακα 6.2.) που παρουσιάζουν ιδιαίτερο ενδιαφέρον, ως μέσα για την ικανοποίηση των απαιτήσεων ασφάλειας των υπηρεσιών διαδικτύου είναι οι εξής:

- Έλεγχος πρόσβασης. Περιλαμβάνει τις διαδικασίες Αυθεντικοποίηση και Εξουσιοδότηση. Κατά την αυθεντικοποίηση μια υπηρεσία αποδεικνύει στην υπηρεσία (συμπεριλαμβανομένης της υπηρεσίας καταλόγου) με την οποία επικοινωνεί, ότι ενεργεί εκ μέρους ενός συγκεκριμένου πελάτη ή μιας άλλης υπηρεσίας. Κατά το στάδιο της εξουσιοδότησης εφαρμόζεται η πολιτική ασφαλείας, που καθορίζει για κάθε αυθεντικοποιημένη οντότητα σε ποιους πόρους και διαδικασίες δικαιούται πρόσβαση.
- Κρυπτογράφηση. Χρησιμοποιείται για να βεβαιώσει ότι η πληροφορία ενός μηνύματος (ή μέρος αυτής), είναι αδιαφανής σε όλους εκτός από εκείνους που ορίζονται από τον αποστολέα
- Έλεγχος Ακεραιότητας μηνυμάτων. Χρησιμοποιείται για να επιβεβαιώσει ότι η πληροφορία ενός μηνύματος (ή μέρος αυτής) δεν τροποποιήθηκε από τρίτους, κατά τη μετάδοση του μηνύματος.
- Επίβλεψη (Monitoring). Είναι μια συνεχής διαδικασία ανίχνευσης, σχεδιασμένη να εξασφαλίσει την αναγνώριση περιστατικών και παραβιάσεων, όταν εμφανίζονται. Περιστατικό είναι ένα γεγονός που συνέβη ενδεχομένως εξαιτίας της υλοποίησης μιας απειλής (threat). Παραβίαση είναι ένα γεγονός, κατά τη διάρκεια του οποίου μια ή περισσότερες από τις ιδιότητες Εμπιστευτικότητα, Διαθεσιμότητα, Εγκυρότητα έχουν προσβληθεί.
- Αποθήκευση και προώθηση μηνυμάτων από έμπιστο φορέα που παρέχει υπηρεσία μη-αποποίησης. Ο μηχανισμός αυτός επιτρέπει τη διαχείριση από μια έμπιστη Τρίτη οντότητα, στοιχείων που αποδεικνύουν ότι μια συγκεκριμένη οντότητα έλαβε ή απέστειλε ένα συγκεκριμένο μήνυμα. Στην περίπτωση που υπάρχει διαφορά μεταξύ δύο οντοτήτων, που συμμετέχουν σε μια συναλλαγή, η έμπιστη τρίτη οντότητα συμπεριφέρεται ως διαιτητής και παρέχει τα στοιχεία που απαιτούνται για την επίλυση της διαφοράς. Η υπηρεσία μη-αποποίησης μπορεί να είναι υλοποιημένη ως υπηρεσία διαδικτύου.

Στις ενότητες που ακολουθούν παρουσιάζονται αναλυτικά όλες οι τεχνολογίες που χρησιμοποιούνται από τους μηχανισμούς του επιπέδου εφαρμογής.



6.4.1. Kerberos tickets.

Το Kerberos είναι μία κατανεμημένη υπηρεσία αυθεντικοποίησης. Επιτρέπει μία σε μια διεργασία (client) που εκτελείται εκ μέρους ενός χρήστη, να αποδείξει την ταυτότητα του τελευταίου, σε έναν αυθεντικοποιητή (server), χωρίς να αποστείλει δεδομένα μέσω του δικτύου, τα οποία θα δώσουν τη δυνατότητα σε έναν τρίτο να υποδυθεί (impersonate) τον χρήστη, στον αυθεντικοποιητή. Το Kerberos διατηρεί μία βάση δεδομένων που περιέχει τους πελάτες τους οποίους εξυπηρετεί και τα ιδιωτικά κλειδιά τους. Οι υπηρεσίες που απαιτούν αυθεντικοποίηση μπορούν να εγγραφούν στο Kerberos, το ίδιο και οι χρήστες που επιθυμούν να χρησιμοποιήσουν αυτές τις υπηρεσίες.

Ένα Kerberos Ticket περιέχει πληροφορίες που είναι κρυπτογραφημένες με το κλειδί του εξυπηρετητή, και μπορεί να χρησιμοποιηθεί από ένα πελάτη για να του επιτρέψει πρόσβαση στο συγκεκριμένο εξυπηρετητή. Ένα Kerberos ticket εκδίδεται από την υπηρεσία παροχής εισιτηρίων (ticket-granting service) του Kerberos για ένα συγκεκριμένο συνδυασμό εξυπηρετητή-πελάτη και περιέχει

- το όνομα του εξυπηρετητή,
- το όνομα και την IP διεύθυνση του πελάτη,
- μία χρονική σφραγίδα,
- τη διάρκειας ζωής του εισιτηρίου και
- ένα τυχαίο κλειδί συνόδου.

Τα Kerberos tickets μπορούν να χρησιμοποιηθούν ως διαπιστευτήρια ενός πελάτη (ή μιας υπηρεσίας) για την αυθεντικοποίησή του από μια υπηρεσία διαδικτύου που έχει εγγραφεί στην υπηρεσία Kerberos.

6.4.2. XML Κρυπτογραφία.

Η κρυπτογράφηση XML αποτελεί πρότυπη τεχνολογία, που χρησιμοποιείται για την αποτροπή της μη εξουσιοδοτημένης πρόσβασης σε συγκεκριμένες πληροφορίες ενός XML εγγράφου.

Το XML-ENC⁴⁹ πρότυπο προσδιορίζει μια διαδικασία κρυπτογράφησης του ψηφιακού περιεχόμενου ενός XML εγγράφου και μια XML σύνταξη για το κρυπτογραφημένο περιεχόμενο, η οποία παρέχει τις απαραίτητες πληροφορίες που επιτρέπουν στον παραλήπτη να το αποκρυπτογραφήσει. Επίσης, παρέχει τη δυνατότητα κρυπτογράφησης συγκεκριμένων



στοιχείων (ευαίσθητης πληροφορίας) ενός XML μηνύματος, επιτρέποντας την επεξεργασία της μη ευαίσθητη πληροφορίας του, κάτι που θα ήταν αδύνατο εάν η κρυπτογράφηση γινόταν στο πλήρες XML μήνυμα.

Το XML-ENC [XML ENC] εισάγει τη χρήση ιδιοτήτων (properties) στοιχείων για τον προσδιορισμό και την περιγραφή των στοιχείων που χρειάζονται προστασία, με στόχο πάντα τη διατήρηση της υπάρχουσας δομής των εγγράφων. Το κύριο στοιχείο του συντακτικού της XML κρυπτογράφησης (Σχήμα 6.2.) είναι το στοιχείο EncryptedData. Όταν ένα έγγραφο κρυπτογραφηθεί οι ετικέτες <EncryptedData> και </EncryptedData> φανερώνουν αντίστοιχα την αρχή και το τέλος των κρυπτογραφημένων πληροφοριών. Επίσης, τα πραγματικά ονόματα των ετικετών, στην περιοχή των κρυπτογραφημένων πληροφοριών του εγγράφου, αντικαθίστανται με τις ετικέτες <CipherData>, <CipherValue> και <CipherReference>.

```

<EncryptedData Id? Type?>
  <EncryptionMethod?>
    <ds:KeyInfo?>
      <EncryptedKey?>
      <AgreementMethod?>
      <ds:KeyName?>
      <ds:Retrievalethod?>
      <ds: *>
    </ds:KeyInfo?>
  <CipherData>
    <Cipher Value?>
    <CipherReference URI?>?
  </CipherData>
  <EncryptionProperties?>
</EncryptedData>

```

Σχήμα 6.2.: Δομή του συντακτικού της XML κρυπτογράφησης.

Το στοιχείο CipherValue έχει ως περιεχόμενο τα κρυπτογραφημένα δεδομένα, στην περίπτωση που αυτά εσωκλείονται στο έγγραφο. Διαφορετικά, αν γίνεται αναφορά, το στοιχείο CipherReference με την ιδιότητα URI δείχνει τα κρυπτογραφημένα δεδομένα.

Η χρήση της XML κρυπτογραφίας είναι ιδιαίτερα σημαντική στις υπηρεσίες διαδικτύου, γιατί επιτρέπει την ασφαλή μετάδοση ενός XML μηνύματος, καθ' όλη τη διαδρομή του, που μπορεί να περιλαμβάνει αρκετούς παραλήπτες, μέχρι τον τελικό του προορισμό. Η δυνατότητα της μερικής κρυπτογράφησης του XML εγγράφου, καθορίζει για κάθε παραλήπτη την πρόσβαση μόνο στα απαραίτητα δεδομένα της ευαίσθητης πληροφορίας.

⁴⁹ W3C Standard (Final vote in committee)

6.4.3. XML Ψηφιακές Υπογραφές.

Στην ενότητα 6.3.4. έγινε μια μικρή αναφορά στους αλγόριθμους σύνοψης (Digest Algorithms). Ένας αλγόριθμος σύνοψης είναι μια μονόδρομη συνάρτηση που λαμβάνει ως είσοδο ένα απλό μήνυμα (plaintext) και παράγει ως έξοδο μια μοναδική σύνοψη του μηνύματος (message digest), με συγκεκριμένο μήκος. Η εφαρμογή του ίδιου αλγορίθμου σύνοψης σε ένα μήνυμα κατά τις χρονικές στιγμές της αποστολής του και της παραλαβής, έχει ως αποτέλεσμα τη δημιουργία δύο συνόψεων του ίδιου μηνύματος, που αν αποδειχτεί ότι διαφέρουν, σημαίνει ότι το μήνυμα τροποποιήθηκε κατά τη μετάδοση του. Η ιδέα αυτή είναι βασική στην κατανόηση των ψηφιακών υπογραφών.

Μια ψηφιακή υπογραφή είναι η σύνοψη ενός μηνύματος κρυπτογραφημένη από το μυστικό κλειδί του ιδιοκτήτη της (συμμετρικό ή ιδιωτικό). Μια ψηφιακή υπογραφή επιβεβαιώνει την αυθεντικότητα και την ακεραιότητα ενός μηνύματος. Η διαδικασία της επιβεβαίωσης είναι η εξής. Όταν ο παραλήπτης ενός μηνύματος λάβει το μήνυμα (plaintext) μαζί με τη ψηφιακή υπογραφή του αποστολέα, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει την υπογραφή και να αναπαράγει τη σύνοψη του μηνύματος. Στη συνέχεια, εφαρμόζει στο μήνυμα (plaintext) τον ίδιο αλγόριθμο σύνοψης και αφού παράγει ξανά τη σύνοψη του μηνύματος, τη συγκρίνει με αυτή που παρέλαβε. Έτσι επιβεβαιώνει την αυθεντικότητα του μηνύματος, αφού γνωρίζει ότι η ψηφιακή υπογραφή εξαρτάται από το περιεχόμενό του και είναι αδύνατο κάποιος να απέσπασε την υπογραφή ενός μηνύματος και να την προσάρμοσε σε κάποιο άλλο μήνυμα.

Στις υπηρεσίες διαδικτύου ένα μήνυμα ενδέχεται να περάσει στην κατοχή αρκετών ενδιάμεσων οντοτήτων (intermediaries) που αναλαμβάνουν να το προωθήσουν στον τελικό παραλήπτη του. Στην περίπτωση αυτή, είναι απαραίτητο να βρεθεί ένας τρόπος, ώστε κάθε οντότητα που παραλαμβάνει το μήνυμα, να μπορεί να επιβεβαιώσει την αυθεντικότητα και την ακεραιότητα ενός συγκεκριμένου τμήματος της πληροφορίας του μηνύματος. Επίσης, θα πρέπει να μπορεί να τροποποιεί και να υπογράφει ψηφιακά, όποτε είναι απαραίτητο, ένα μόνο τμήμα της πληροφορίας του μηνύματος, χωρίς αυτό να είναι εμπόδιο στον έλεγχο της ακεραιότητας κάποιου άλλου τμήματος.

Όλες οι παραπάνω δυνατότητες υποστηρίζονται από τις ψηφιακές υπογραφές XML (XML Digital Signatures). Συγκεκριμένα, το πρότυπο XML-DS⁵⁰ [XMI. DS] καθορίζει μια δομή δεδομένων και βασικούς κανόνες επεξεργασίας για την προστασία, με τη χρήση της κρυπτογράφησης δημοσίου κλειδιού, της εμπιστευτικότητας:



- α) ολόκληρου του XML αρχείου,
- β) ενός στοιχείου ή μιας ομάδας στοιχείων του XML αρχείου.

Η δομή του συντακτικού μιας XML ψηφιακής υπογραφής παρουσιάζεται στο σχήμα 6.3.

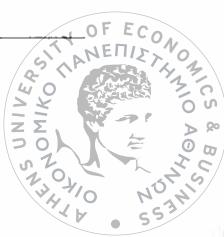
```

<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI? >
      (<Transforms>)?
      <DigestMethod>
      <DigestValue>
      </Reference>)+)
    </SignedInfo>
    <SignatureValue>
      (<KeyInfo>)?
      (<Object ID?>)*
    </Signature>
  
```

Σχήμα 6.3.: Δομή του συντακτικού της XML ψηφιακής υπογραφής.

Το στοιχείο Signature είναι η ρίζα της XML ψηφιακής υπογραφής και περιλαμβάνει αντικείμενα δεδομένων που υπογράφονται από τον ίδιο υπογράφοντα. Το στοιχείο SignedInfo περιέχει όλες τις πληροφορίες για τα αντικείμενα δεδομένων που υπογράφονται και επιπρόσθετες πληροφορίες απαραίτητες για την επικύρωση της υπογραφής. Για κάθε αντικείμενο δεδομένων που υπογράφεται υπάρχει ένα στοιχείο Reference που αναφέρεται σε αυτό. Η τιμή της σύνοψης του αντικειμένου αποθηκεύεται στο στοιχείο DigestValue, ενώ ο αλγόριθμος σύνοψης καθορίζεται στο στοιχείο DigestMethod. Στο στοιχείο CanonicalizationMethod περιέχεται ο αλγόριθμος που χρησιμοποιείται για την κανονικοποίηση του στοιχείου SignedInfo. Η κανονικοποίηση αυτή είναι απαραίτητη για να αγνοηθούν κάποια σύμβολα που μπορεί να οδηγήσουν σε λάθη κατά τη διαδικασία της επικύρωσης της υπογραφής. Η ψηφιακή υπογραφή αποθηκεύεται στο στοιχείο SignatureValue και είναι το αποτέλεσμα της κρυπτογράφησης των κανονικοποιημένων δεδομένων ολόκληρου του στοιχείου SignedInfo. Η κρυπτογράφηση γίνεται με το ιδιωτικό κλειδί του υπογράφοντα και με χρήση του αλγόριθμου κρυπτογράφησης που καθορίζεται στο στοιχείο SignatureMethod του εγγράφου.

⁵⁰ W3C Standard (Completed)



6.4.4. XML Υπηρεσίες Διαχείρισης Κλειδιών (XKMS).

Μια υπηρεσία διαχείρισης κλειδιών (Key Management Service), ασχολείται κατά κύριο λόγο, με τη σωστή, αποδοτική, επεκτάσιμη και ασφαλή διαχείριση κρυπτογραφικών κλειδιών. Ορισμένες από τις βασικές διαδικασίες που πρέπει να υποστηρίζει είναι [Παράδειγμα Στ., 2002 (2)]:

- Δημιουργία ζεύγους κλειδιών. Η δημιουργία ενός ζεύγους κλειδιών γίνεται με αίτηση εγγραφής (registration) του πελάτη στην υπηρεσία, η οποία γίνεται με συμπλήρωση των προσωπικών του στοιχείων. Περιλαμβάνει τη διαδικασία παραγωγής τυχαίων αριθμών, που είναι απαραίτητη για τη δημιουργία του ζεύγους κλειδιών.
- Αντιστοίχηση του ζεύγους κλειδιών με την αιτούσα οντότητα. Η διαδικασία αυτή αφορά στην έκδοση ενός τεκμηρίου (token), που χρησιμοποιείται για την αντιστοίχηση του ζεύγους κλειδιών με τις πληροφορίες του πελάτη (ταυτότητα και άλλες ιδιότητες).
- Διανομή ζεύγους κλειδιών στον πελάτη. Η διανομή πρέπει να πραγματοποιείται με αξιόπιστους και ασφαλείς τρόπους.
- Ενημέρωση κλειδιού. Μια KMS πρέπει να είναι ικανή να ενημερώσει ή να ανανεώσει ένα κλειδί μετά από σχετική αίτηση ή αναφορά διακύβευσής του ή κατά τη λήξη ενός πιστοποιητικού.
- Τήρηση αρχείου αντιγράφων κλειδιών. Η διαδικασία αυτή θέτει ζητήματα εμπιστοσύνης με αποτέλεσμα να είναι επιλογή του χρήστη αν επιλέξει να τη χρησιμοποιήσει.
- Ανάκτηση δημοσίου κλειδιού από κατάλογο δημόσιων κλειδιών. Γίνεται έπειτα από αίτηση και γίνεται χωρίς αυθεντικοποίηση του αιτούντα, αφού τα δημόσια κλειδιά είναι πάντα διαθέσιμα σε κάθε αίτηση. Μια αίτηση απορρίπτεται μόνο στην περίπτωση διακύβευσης ενός κλειδιού και στην περίπτωση λήξης ή ανάκλησης του πιστοποιητικού του.
- Ανάκαμψη κλειδιού σε περίπτωση απώλειας ή διακύβευσης της ασφάλειάς του. Η διαδικασία αυτή επιτρέπει την ανάκτηση ενός μυστικού κλειδιού σε ειδικές περιπτώσεις, έπειτα από αυθεντικοποιημένη αίτηση.
- Διαδικασίες που αναλαμβάνονται σε περίπτωση διακύβευσης της ασφάλειας του κλειδιού. Περιλαμβάνει μηχανισμούς αποδοχής, επιβεβαίωσης και αναφοράς διακύβευσης κλειδιών.
- Έλεγχος αιτήσεων για διαδικασίες που αφορούν την πρόσβαση στα κλειδιά. Περιλαμβάνει την αυθεντικοποίηση και εξουσιοδότηση του αιτούντα.



Το πρότυπο XKMS ορίζει ορισμένες προδιαγραφές για XML υπηρεσίες διαχείρισης κλειδιών (XML Key Management Services) που μπορούν να χρησιμοποιηθούν από υπηρεσίες διαδικτύου. Το XKMS καθορίζει ένα τρόπο με τον οποίο μια υπηρεσία διαδικτύου μπορεί να καταχωρίσει, να ανακαλέσει, να εντοπίσει, και να ενημερώσει πληροφορίες δημοσίου κλειδιού στην XKMS υπηρεσία, κατορθώνοντας έτσι να υποστηρίξει ευκολότερα τη χρήση της XML κρυπτογράφησης και των XML ψηφιακών υπογραφών. Ο τρόπος αυτός είναι η ανταλλαγή XML μηνυμάτων και απαλλάσσει τις υπηρεσίες διαδικτύου από την ανάγκη να υποστηρίζουν πρωτόκολλα εξειδικευμένα στη διαχείριση κλειδιών. Ένας οργανισμός που παρέχει μια υπηρεσία διαδικτύου, μπορεί να απαιτήσει από ένα πελάτη να εγγραφεί σε μια XKMS υπηρεσία, προκειμένου να χρησιμοποιήσει την υπηρεσία του [Nagaraj. 2003].

Το πρότυπο XKMS [XKMS] ορίζει τις εξής τρεις προδιαγραφές:

- XML Key Registration Service Specification (XKRSS).
- XML Key Information Service Specification (XKISS).
- Protocol Bindings Specification.

Οι προδιαγραφές αυτές: α) καθορίζουν τα μηνύματα (αίτηση-απόκριση) που ανταλλάσσονται με την XKMS υπηρεσία, β) υποστηρίζουν τις διαδικασίες καταχώρισης και διαχείρισης της πληροφορίας που σχετίζεται με τα δημόσια κλειδιά, και γ) εξασφαλίζουν ότι ικανοποιούνται δεδομένες απαιτήσεις ασφάλειας.

Η προδιαγραφή XKRSS υποστηρίζει τη διαδικασία εγγραφής στην υπηρεσία. Η αιτούσα οντότητα αποστέλλει στην υπηρεσία μια αίτηση εγγραφής (RegisterRequest) που έχει ως βασικό στοιχείο το <KeyInfo>, που περιέχει πληροφορίες οι οποίες αφορούν στο ζεύγος κλειδιών που έχει δημιουργήσει. Η αίτηση εγγραφής καθορίζει μέσω του στοιχείου <RespondWith> το περιεχόμενο του μηνύματος απόκρισης της υπηρεσίας⁵¹. Το μήνυμα απόκρισης της υπηρεσίας (RegisterResponse) αφορά στο αποτέλεσμα της διαδικασίας εγγραφής και περιλαμβάνει ένα στοιχείο <KeyBinding>, που παρέχει την αντιστοίχιση μεταξύ του ζεύγους κλειδιών και της αιτούσας οντότητα. Η «binding» πληροφορία (π.χ. πιστοποιητικό X.509) ισχύει για συγκεκριμένο χρονικό διάστημα, μετά την παρέλευση του οποίου μπορεί είτε να επανεκδοθεί (reissued) είτε να αποσυρθεί (revoked). Η τήρηση αντιγράφου ασφαλείας του ιδιωτικού κλειδιού είναι προαιρετική.

Η προδιαγραφή XKISS επιτρέπει σε ένα πελάτη να εντοπίσει (locate) ή να επικυρώσει (validate) τις πληροφορίες που σχετίζονται με ένα <KeyInfo> στοιχείο. Μια αίτηση προς την

⁵¹ Για παράδειγμα ένας πελάτης μπορεί να επιθυμεί την έκδοση ενός X.509 πιστοποιητικού.

υπηρεσία πρέπει να καθορίζει τον τύπο της σχετιζόμενης με το κλειδί πληροφορίας που ζητά να της επιστραφεί.

Τέλος, η προδιαγραφή Protocol Bindings ορίζει μηχανισμούς για την εξασφάλιση των μηνυμάτων που ανταλλάσσονται μεταξύ της υπηρεσίας διαδικτύου και της υπηρεσίας XKMS. Συγκεκριμένα, εκτός από την XML κρυπτογράφηση και την XML ψηφιακή υπογραφή, στις προτεινόμενες λύσεις οι περιλαμβάνονται και οι μηχανισμοί του πρωτοκόλλου SSL, που παρέχουν point-to-point εμπιστευτικότητα και ακεραιότητα.

6.4.5. Γλώσσα Σήμανσης Διαβεβαιώσεων Ασφάλειας (SAML).

Η γλώσσα SAML⁵² (Security Assertion Markup Language) καθορίζει ένα πρότυπο συντακτικό XML για την ανταλλαγή διαβεβαιώσεων ασφαλείας (security assertions) μεταξύ των υπηρεσιών διαδικτύου, συμπεριλαμβανομένων διαβεβαιώσεων που αφορούν στους μηχανισμούς αυθεντικοποίησης και εξουσιοδότησης [SAML]. Η ανταλλαγή των διαβεβαιώσεων αυτών έχει ως στόχο:

- Τη δημιουργία μοναδικού σημείου πρόσβασης (single sign-on) για τους μηχανισμούς αυθεντικοποίησης και εξουσιοδότησης.
- Τη διαχείριση των μηχανισμών αυθεντικοποίησης και εξουσιοδότησης από τρίτες οντότητες.

Μια SAML διαβεβαίωση αντιστοιχεί σε μια και μοναδική οντότητα. Μια SAML διαβεβαίωση αυθεντικοποίησης ή εξουσιοδότησης, παρέχει την πληροφορία ότι μια οντότητα αυθεντικοποίηθηκε ή εξουσιοδοτήθηκε, αντίστοιχα, με συγκεκριμένο τρόπο, σε μια συγκεκριμένη χρονική στιγμή. Η SAML καθορίζει μοναδικά αναγνωριστικά (URNs) για την περιγραφή των διαφορετικών μηχανισμών αυθεντικοποίησης και των διαφορετικών ενεργειών εξουσιοδότησης. Για παράδειγμα, επιτρέπει την περιγραφή όλων των τεχνικών αυθεντικοποίησης, που μπορεί να περιλαμβάνουν αυθεντικοποίηση με χρήση συνθηματικού, αυθεντικοποίηση με χρήση τεκμηρίου (π.χ. hardware token), ή ακόμα και αυθεντικοποίηση με χρήση κάποιας βιομετρικής μεθόδου. Το συντακτικό της γλώσσας SAML επιτρέπει τον καθορισμό του είδους του διαπιστευτηρίου (credential) που περιλαμβάνεται στο SOAP μήνυμα.

Η γλώσσα SAML καθορίζει ένα πρωτόκολλο αίτησης-απόκρισης για τη μεταβίβαση των διαβεβαιώσεων. Μια υπηρεσία διαδικτύου μπορεί να ζητήσει με τη μορφή αίτησης και να

⁵² OASIS Open Standard



λάβει σαν απόκριση, από μια υπηρεσία με την οποία συνεργάζεται, μια SAML διαβεβαίωση που μπορεί να αυθεντικοποιήσει ή να εξουσιοδοτήσει ένα συγκεκριμένο χρήστη της. Το μόνο που χρειάζεται είναι και οι δύο υπηρεσίες να υποστηρίζουν το πρότυπο SAML. Στην περίπτωση μάλιστα που μια SAML διαβεβαίωση προωθείται σε μια σειρά από συνεργαζόμενες υπηρεσίες διαδικτύου, μπορεί να χρησιμοποιηθεί για την υποστήριξη ενός μοναδικού σημείου πρόσβασης για όλες τις υπηρεσίες αυτές. Αυτό πολύ απλά σημαίνει, ότι χρήστες που έχουν αυθεντικοποιηθεί από μια υπηρεσία, δεν χρειάζεται να κάνουν login ξανά σε καμία από τις συνεργαζόμενες υπηρεσίες.

Τις περισσότερες φορές, για την αποφυγή κινδύνων, οι προδιαγραφές της γλώσσας SAML καθορίζουν ένα μέγιστο χρονικό διάστημα ως διάρκεια ζωής μιας διαβεβαίωσης. Επίσης, συχνά επιτρέπουν την εφαρμογή των διαβεβαιώσεων μόνο σε συγκεκριμένες κατηγορίες χρηστών. Τέλος, οι προδιαγραφές της γλώσσας SAML καθορίζουν και τη χρήση ψηφιακών υπογραφών για την εξασφάλιση των διαβεβαιώσεων.

6.4.6. Εκτεταμένη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης (XACML).

Παρά το γεγονός ότι η γλώσσα SAML παρέχει ένα μηχανισμό για τη μεταβίβαση διαβεβαιώσεων αυθεντικοποίησης και εξουσιοδότησης μέσω SOAP μηνυμάτων, είναι απαραίτητο ένα συντακτικό που να μπορεί να περιγράψει τους κανόνες που απαιτεί η λήψη μιας απόφασης εξουσιοδότησης. Ένα συντακτικό XML που δημιουργήθηκε για αυτόν ακριβώς το λόγο αποτελεί η γλώσσα Extensible Access Control Markup Language⁵³.

Η γλώσσα XACML [XACML] είναι βασισμένη στο μοντέλο του πίνακα ελέγχου προσπέλασης (ACM) και καθορίζει τους κανόνες εξουσιοδότησης για κάθε στοιχείο ενός εγγράφου XML ή για ένα ολόκληρο XML έγγραφο. Κάθε κανόνας σχετίζεται με ένα υποκείμενο (οντότητα που αιτείται), ένα δικαίωμα (ανάγνωση, τροποποίηση κ.λπ.), ένα αντικείμενο (το στοιχείο του εγγράφου), και μια συνθήκη (π.χ. ημέρα της εβδομάδας που επιτρέπεται η πρόσβαση).

Το πρότυπο XACML καθορίζει:

- Ένα XML συντακτικό για την αναπαράσταση κανόνων εξουσιοδότησης.
- Ένα XML συντακτικό για την αναπαράσταση ενός συνόλου από διαφορετικές συνθήκες που μπορούν να χρησιμοποιηθούν για τη δημιουργία κανόνων.
- Ένα τρόπο με τον οποίο μπορούν να συνδυαστούν και να αποτιμηθούν οι κανόνες.

⁵³ OASIS Standard (Committee review).



- Τα μέσα για τη δημιουργία μιας έκθεσης της πολιτικής ασφαλείας.

6.4.7. Υπηρεσία Μη αποποίησης.

Μια υπηρεσία μη-αποποίησης (non-repudiation service) περιλαμβάνει διαδικασίες που αφορούν στη δημιουργία, αποθήκευση, ανάκτηση και μετάφραση στοιχείων, τα οποία αποδεικνύουν ότι μια συγκεκριμένη οντότητα επεξεργάστηκε ένα συγκεκριμένο κείμενο ή δεδομένα [Γκρίτζαλης Στ., 2002 (2)].

Στην περίπτωση των υπηρεσιών διαδικτύου, μια υπηρεσία μη αποποίησης είναι απαραίτητη, έτσι ώστε να μπορεί να αποδειχτεί βάσει στοιχείων, ότι μια υπηρεσία διαδικτύου απέστειλε ή παρέλαβε ένα συγκεκριμένο μήνυμα σε μια άλλη ή από μια άλλη, αντίστοιχα. Επιθυμητό είναι στην περίπτωση των υπηρεσιών διαδικτύου, ο έμπιστος φορέας που θα παρέχει την υπηρεσία μη-αποποίησης να την έχει υλοποιήσει με βάση το μοντέλο ανάπτυξης Web Services εφαρμογών, έτσι ώστε να επικοινωνεί με τους πελάτες της μέσω SOAP μηνυμάτων. Μια υπηρεσία μη αποποίησης πρέπει να έχει ως αρμοδιότητα να λαμβάνει και στη συνέχεια να προωθεί τα μηνύματα που ανταλλάσσονται μεταξύ δύο υπηρεσιών, παρέχοντας υπηρεσίες ψηφιακής υπογραφής και χρονοσήμανσης.

Η υπηρεσία ψηφιακής υπογραφής ουσιαστικά εξασφαλίζει την αυθεντικότητα και την ακεραιότητα ενός μηνύματος, χρησιμοποιώντας την τεχνολογία της XML ψηφιακής υπογραφής. Η υπηρεσία χρονοσήμανσης (timestamping service), απλά αναλαμβάνει την προσθήκη ημερομηνίας και ώρας σε ένα μήνυμα, έτσι ώστε να μπορεί να αποδειχθεί ότι η μεταφορά ενός μηνύματος έλαβε χώρα σε μια συγκεκριμένη χρονική στιγμή.

6.4.8. XML Application Firewalls.

Μια ασφαλής πύλη εφαρμογών (application firewall), σε αντίθεση με ένα φίλτρο πακέτων (packet filter), κατανοεί την πληροφορία που διέρχεται από αυτή, ως ροή δεδομένων (data stream) και όχι ως κίνηση πακέτων. Μια ασφαλής πύλη εφαρμογών έχει πρόσβαση στα περιεχόμενα ενός πακέτου του επιπέδου εφαρμογής και μπορεί να λαμβάνει έξυπνες αποφάσεις για τα πακέτα, με βάση το περιεχόμενό τους.

Εντούτοις, στην περίπτωση των υπηρεσιών διαδικτύου, ένα τυπικό application firewall δεν μπορεί να πάρει ασφαλείς αποφάσεις, εξετάζοντας απλά το περιεχόμενο των HTTP αιτήσεων που φτάνουν σε μια υπηρεσία. Η δυσκολία εντοπίζεται στο γεγονός ότι το

πρωτόκολλο SOAP επιτρέπει τη διέλευση δεδομένων που μπορούν να εκτελεστούν, τα οποία τυγχάνουν από το firewall την ίδια αντιμετώπιση με τα τυπικά HTTP μηνύματα. Αυτό, αποτελεί σημείο ευπάθειας για την υπηρεσία.

Παρά το γεγονός ότι οι επικεφαλίδες HTTP μπορούν να επεκταθούν, προκειμένου να παρέχουν αναγνώριση σε SOAP μηνύματα, το πρόβλημα παραμένει, αφού το πρωτόκολλο SOAP δεν ορίζει προδιαγραφές σχετικές με ασφάλεια. Σύμφωνα με τον Damiani [Damiani et al., 2001] μια SOAP υπηρεσία μπορεί να χρησιμοποιεί μηχανισμούς αυθεντικοποίησης HTTP αιτήσεων, ωστόσο αυτό δε δύναται να της προσφέρει επαρκή ασφάλεια. Ο λόγος είναι ότι οι προδιαγραφές ασφαλείας του προτύπου HTTP έχουν δημιουργηθεί για να υποστηρίζουν διαδικασίες ανάκτησης απλών εγγράφων και δεν προσφέρονται για την απομακρυσμένη κλήση διαδικασιών.

Στην περίπτωση των υπηρεσιών διαδικτύου, είναι απαραίτητος ο έλεγχος της XML κίνησης με βάση το περιεχόμενο των αιτήσεων. Αυτό προϋποθέτει, εκτός από τη δυνατότητα πρόσβασης του firewall στο περιεχόμενο ενός SOAP μηνύματος, τη γνώση της επιχειρησιακής λογικής της υπηρεσίας.

Τα XML Application firewalls, είναι νέα προϊόντα που υποστηρίζεται ότι παρέχουν σε μια υπηρεσία διαδικτύου επαρκή ασφάλεια ενάντια σε παραβιάσεις, επιτρέποντας τη λήψη σύνθετων αποφάσεων ασφαλείας. Συγκεκριμένα, ένα XML Application Firewall [Westbridge, 2002] υποστηρίζει:

- Πρόσβαση στην επικεφαλίδα, το σχήμα και το περιεχόμενο των SOAP μηνυμάτων, που αποστέλλονται μέσω μιας HTTP αίτησης. Επίσης, διενεργεί ελέγχους, κάνοντας ανάλυση του XML κώδικα, ανιχνεύοντας με αυτόν τον τρόπο τα εισερχόμενα και εξερχόμενα μηνύματα που δεν ακολουθούν τους κανόνες που πρέπει να ακολουθεί ένα καλά δομημένο XML έγγραφο.
- Αυθεντικοποίηση της οντότητας, για λογαριασμό της οποίας καλείται η υπηρεσία, και αναγνώριση του επίπεδου δικαιωμάτων πρόσβασης που έχει η οντότητα αυτή. Στις μεθόδους που χρησιμοποιεί για το σκοπό αυτό περιλαμβάνονται ο έλεγχος πιστοποιητικών και ο έλεγχος SAML εισιτηρίων.

6.5. Συμπέρασμα.

Η αντιμετώπιση του ζητήματος της ασφάλειας από τους οργανισμούς, περιλαμβάνει την εφαρμογή μηχανισμών σε διαφορετικά επίπεδα, ανάλογα με τις απαιτήσεις που έχουν



προσδιορίσει και τις δυνατότητες που τους παρέχει η υπάρχουσα τεχνολογία. Στην περίπτωση ενός οργανισμού που παρέχει μια υπηρεσία διαδικτύου, η ανάγκη για εξασφάλιση της επικοινωνίας με τον τελικό χρήστη, καθώς και η ανάγκη εφαρμογής πολιτικών ασφάλειας για τον τελικό χρήστη, καθιστά δύσκολη την εφαρμογή μηχανισμών ασφαλείας σε χαμηλό επίπεδο. Για το λόγο αυτό, η αντιμετώπιση των απαιτήσεων ασφαλείας λαμβάνει χώρα κυρίως στο επίπεδο εφαρμογής.

Τα πρότυπα που ξεχωρίζουν στο επίπεδο εφαρμογής είναι τα πρότυπα XML ENC, XML DS, XKMS, SAML και XACML. Τα πρότυπα XML ENC και XML DS επεκτείνουν τις δυνατότητες των τεχνολογιών κρυπτογράφησης και ψηφιακής υπογραφής, επιτρέποντας τη δυνατότητα εφαρμογής τους στο ίδιο έγγραφο από διαφορετικές οντότητες. Το πρότυπο XKMS καθορίζει ένα τρόπο κλήσης διαδικασιών διαχείρισης δημοσίου κλειδιού, μέσω XML μηνυμάτων. Τέλος, τα πρότυπα SAML και XACML υποστηρίζουν από κοινού τη διαδικασία εξουσιοδότησης του τελικού χρήστη σε μια υπηρεσία διαδικτύου.



ΚΕΦΑΛΑΙΟ 7^ο : ΜΟΝΤΕΛΟ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΙΣ ΥΠΗΡΕΣΙΕΣ ΔΙΑΔΙΚΤΥΟΥ

7.1. Εισαγωγή.

Στο προηγούμενο κεφάλαιο, έγινε αναφορά στους μηχανισμούς που μπορεί να υλοποιήσει ένας οργανισμός, προκειμένου να ικανοποιήσει τις βασικές απαιτήσεις ασφάλειας για την παροχή και χρήση υπηρεσιών διαδικτύου. Επίσης, αναφέρθηκαν οι τεχνολογίες που μπορούν να χρησιμοποιηθούν προς αυτή την κατεύθυνση. Το ερώτημα, όμως, που παρέμεινε αναπάντητο είναι με ποιο τρόπο ένας οργανισμός θα επιλέξει τις κατάλληλες λύσεις και πώς θα τις προσαρμόσει στις απαιτήσεις του.

Στο κεφάλαιο αυτό περιγράφεται ένα μοντέλο ασφαλείας για το περιβάλλον των υπηρεσιών διαδικτύου, πάνω στο οποίο συνεργάζονται αυτή τη στιγμή οι εταιρείες IBM και Microsoft. Στόχος του μοντέλου είναι να αποτελέσει στο μέλλον ένα πρότυπο για τους οργανισμούς, που θα τους επιτρέπει να σχεδιάσουν, και εν συνεχείᾳ να υλοποιήσουν την αρχιτεκτονική ασφάλειας που προτείνει, προσαρμόζοντάς την στους στόχους ασφάλειας που έχουν θέσει. Για να το πετύχει αυτό, το μοντέλο ενσωματώνει, υποστηρίζει και ενοποιεί δημοφιλή μοντέλα, μηχανισμούς και τεχνολογίες ασφάλειας.

7.2. Στόχοι του προτεινόμενου μοντέλου ασφαλείας.

Η ικανοποίηση των απαιτήσεων ασφάλειας στο περιβάλλον των υπηρεσιών διαδικτύου, απαιτεί τη λήψη μέτρων σε τεχνικό, αλλά και σε οργανωσιακό επίπεδο. Επίσης, απαιτεί τη συντονισμένη προσπάθεια των προμηθευτών του δικτυακού εξοπλισμού, των προμηθευτών των πλατφόρμων ανάπτυξης, των ομάδων ανάπτυξης εφαρμογών και των πελατών των υπηρεσιών. Το μοντέλο ασφάλειας για τις υπηρεσίες διαδικτύου, το οποίο προτείνουν οι εταιρείες IBM και Microsoft έχει ως στόχο να καθορίσει ένα γενικό πλαίσιο ασφάλειας που θα περιλαμβάνει προδιαγραφές, οι οποίες θα αφορούν σε τεχνικά και οργανωσιακά ζητήματα, και θα απευθύνεται σε κάθε μια από τις παραπάνω ομάδες.

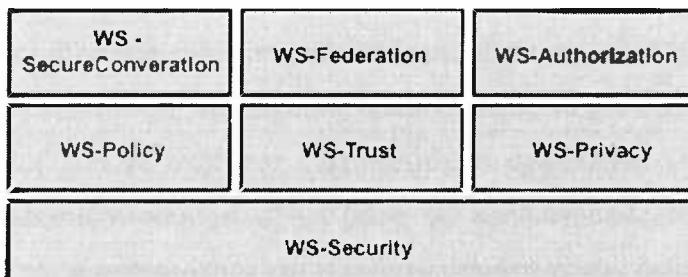
Από τους βασικούς στόχους του μοντέλου θα είναι και η δημιουργία πρότυπων διαδικασιών και προδιαγραφών για τη σύνταξη των πολιτικών ασφαλείας. Ζητούμενο είναι το μοντέλο να παρέχει ευελιξία, επιτυγχάνοντας την προσαρμογή του γενικού πλαισίου ασφάλειας στις απαιτήσεις του πελάτη ή του χορηγού της υπηρεσίας.



Τέλος, πρόθεση των δύο εταιρειών είναι το μοντέλο ασφάλειας να μπορεί να χρησιμοποιηθεί τόσο για την παροχή ασφάλειας σε υπάρχουσες εφαρμογές, όσο και για την ανάπτυξη ασφαλών εφαρμογών.

7.3. Περιγραφή του μοντέλου ασφαλείας.

Το προτεινόμενο μοντέλο των εταιρειών IBM και Microsoft, αποτελεί μια στρατηγική ασφαλείας που περιλαμβάνει στρατηγικούς στόχους, οι οποίοι ακολουθούν μια ιεραρχία. Στο σχήμα 7.1. απεικονίζονται οι στρατηγικοί στόχοι (συστατικά στοιχεία) του μοντέλου. [IBM-MS, 2002]



Σχήμα 7.1.: Συστατικά στοιχεία του μοντέλου ασφάλειας των IBM και Microsoft.

Κάθε συστατικό στοιχείο του μοντέλου ασφαλείας καθορίζει ένα σύνολο από προδιαγραφές, οι οποίες στηρίζονται στις προδιαγραφές των συστατικών στοιχείων του μοντέλου που βρίσκονται χαμηλότερα από αυτό στην ιεραρχία. Το σύνολο προδιαγραφών WS-Security, όπως φαίνεται στο σχήμα 7.1., βρίσκεται στο χαμηλότερο επίπεδο στην ιεραρχία, γι' αυτό και στηρίζεται μόνο στις προδιαγραφές του προτύπου SOAP.

Αναλυτικά, τα συστατικά στοιχεία του μοντέλου ασφάλειας είναι τα εξής:

- **WS-Security.** Είναι το βασικό συστατικό του μοντέλου ασφαλείας και αφορά στην ασφάλεια των SOAP μηνυμάτων. Το WS-Security έχει υλοποιηθεί και πρόκειται να αποτελέσει τη βάση για τις υπόλοιπες προδιαγραφές ασφαλείας. Καθορίζει με ποιο τρόπο επισυνάπτονται σε ένα SOAP μήνυμα οι επικεφαλίδες κρυπτογράφησης και ψηφιακής υπογραφής. Επίσης, περιγράφει με ποιο τρόπο επισυνάπτεται ένα τεκμήριο ασφαλείας (π.χ. πιστοποιητικό X.509 ή εισιτήριο του Kerberos) σε ένα μήνυμα. Το WS-Security είναι το μόνο συστατικό στοιχείο του μοντέλου που είναι έτοιμο στην πρώτη του έκδοση.
- **WS-Policy.** Πρόκειται να υποστηρίζει την περιγραφή των δυνατοτήτων και των περιορισμών, που καθορίζει μια πολιτική ασφαλείας για τις υπηρεσίες διαδικτύου (endpoint).

policy). Με βάση τις προδιαγραφές του WS-Policy μια υπηρεσία θα μπορεί να δηλώσει τους κρυπτογραφικούς αλγόριθμους που υποστηρίζει, τα διαπιστευτήρια που απαιτεί από τον πελάτη, τους κανόνες τήρησης της ιδιωτικότητας που εφαρμόζει κ.ά.. Το WS-Policy επίσης προτίθεται να ορίσει ένα XML σχήμα που θα υποστηρίζει την περιγραφή όχι μόνο μιας πολιτικής ασφαλείας, αλλά μιας οποιαδήποτε πολιτικής για την υπηρεσία, χωρίς περιορισμούς στους τύπους των δυνατοτήτων και των περιορισμών που μπορεί να περιγράψει. Βασικός στόχος, επίσης, του WS-Policy είναι να καθορίσει και ένα μηχανισμό που θα επιτρέπει την επισύναψη της πολιτικής σε ένα SOAP μήνυμα.

- **WS-Trust.** Προτίθεται να υποστηρίξει ένα τρόπο για την οικοδόμηση σχέσεων εμπιστοσύνης μεταξύ δύο οντοτήτων που αλληλεπιδρούν, ακόμα και στην περίπτωση που η αλληλεπίδραση γίνεται μέσω τρίτων. Στόχος του WS-Trust είναι η δυνατότητα δημιουργίας σχέσεων άμεσης εμπιστοσύνης (direct trust) μεταξύ δύο οντοτήτων, που να μπορούν να χρησιμοποιηθούν στη συνέχεια σαν βάση για τη δημιουργία σχέσεων έμμεσης εμπιστοσύνης (brokered trust). Στη περίπτωση της έμμεσης εμπιστοσύνης το ρόλο του μεσίτη (broker) θα αναλάβουν υπηρεσίες που θα εκδίδουν διαπιστευτήρια ασφάλειας. Οι υπηρεσίες έκδοσης διαπιστευτηρίων θα είναι υλοποιημένες με βάση τις προδιαγραφές του WS-Security, έτσι ώστε να εξασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα των διαπιστευτηρίων κατά τη μετάδοση τους στους πελάτες. Τέλος, το μοντέλο εμπιστοσύνης WS-Trust θα καθορίζει με ποιο τρόπο θα μπορούν να χρησιμοποιηθούν οι ήδη υπάρχοντες μηχανισμοί εμπιστοσύνης, έτσι ώστε να βρίσκονται σε συμφωνία μαζί του.

- **WS-Privacy.** Οι οργανισμοί που αναπτύσσουν και διαχειρίζονται υπηρεσίες διαδικτύου, συχνά είναι απαραίτητο να δηλώνουν την πολιτική που ακολουθούν για την προστασία της ιδιωτικότητας. Το ίδιο ισχύει και για τους πελάτες που πρέπει στις αιτήσεις που στέλνουν σε μια υπηρεσία να καθορίζουν τις προτιμήσεις τους σε ότι αφορά στην τήρηση της ιδιωτικότητας. Το WS-Privacy, όταν ολοκληρωθεί, αναμένεται να παρέχει ένα σύνολο προδιαγραφών που θα επιτρέπουν την ενσωμάτωση σε μια WS-Policy περιγραφή, μιας γλώσσας περιγραφής δηλώσεων για τη διαχείριση ιδιωτικών πληροφοριών. Επίσης, αναμένεται να εξασφαλίσει ένα τρόπο καθορισμού των απαιτήσεων τήρησης της ιδιωτικότητας που αφορούν σε ένα μήνυμα, με βάση τις προδιαγραφές του WS-Security. Τέλος, ένας ακόμα στόχος του WS-Privacy θα είναι να καθορίσει κάποιο μηχανισμό αποτίμησης των πρακτικών ενός οργανισμού και των προτιμήσεων ενός πελάτη, που σχετίζονται με την τήρηση της ιδιωτικότητας.

- **WS-SecureConversation.** Το WS-SecureConversation πρόκειται να παρέχει τις προδιαγραφές για την υποστήριξη: α) της διαδικασίας αυθεντικοποίησης ενός πελάτη από την

υπηρεσία διαδικτύου, β) της διαδικασίας αυθεντικοποίησης της υπηρεσίας από τον αιτούντα και γ) της ασφαλούς μετάδοσης μηνυμάτων μεταξύ της υπηρεσίας και του αιτούντα. Βάση για τη δημιουργία του WS-SecureConversation θα είναι οι μηχανισμοί του WS-Security και του WS-Trust, οι οποίοι λειτουργούν σε επίπεδο εφαρμογής. Εντούτοις, όπως αναφέρεται στην περιγραφή του μοντέλου ασφαλείας, πρόκειται να υπάρξει υποστήριξη και σε μηχανισμούς του επιπέδου μεταφοράς. Έτσι σε επιλεγμένες συνδέσεις, θα υποστηρίζεται παράλληλα και η χρησιμοποίηση μηχανισμών και τεχνολογιών του επιπέδου μεταφοράς (όπως είναι για παράδειγμα το πρωτόκολλο SSL).

- **WS-Federation.** Το WS-Federation θα στηριχτεί στις προδιαγραφές των WS-Security, WS-Policy, WS-Trust και WS-SecureConversation προκειμένου να υποστηρίξει federated trust σενάρια. Στα σενάρια αυτά ένας πελάτης που έχει δικαίωμα πρόσβασης σε μια υπηρεσία A θα μπορεί να αποκτά με συγκεκριμένους τρόπους δικαίωμα πρόσβασης σε μια άλλη υπηρεσία B, αρκεί η B να είναι πρόθυμη να αποδεχτεί μια ομοσπονδιακή σύνδεση ασφάλειας (security federation) με την A.
- **WS-Authorization.** Οι προδιαγραφές του WS-Authorization θα υποδεικνύουν με ποιο τρόπο πρέπει να δηλώνονται οι ισχυρισμοί (claims) που περιλαμβάνει ένα διαπιστευτήριο και πώς οι ισχυρισμοί αυτοί θα ερμηνεύονται στη συνέχεια από την υπηρεσία. Οι WS-Authorization προδιαγραφές θα είναι ευέλικτες και επεκτάσιμες σε ότι αφορά τη μορφή και τη γλώσσα εξουσιοδότησης, στοχεύοντας στην κάλυψη ενός μεγάλου αριθμού από σενάρια που θα εξασφαλίζει μακροπρόθεσμα τη βιωσιμότητα του πλαισίου ασφάλειας.

7.4. Ανάλυση του μοντέλου ασφαλείας.

Στο προηγούμενο κεφάλαιο έγινε αναφορά στους μηχανισμούς ασφαλείας που δύνανται να καλύψουν τις βασικές απαιτήσεις ασφάλειας που σχετίζονται με τις υπηρεσίες διαδικτύου. Στον πίνακα 7.1. παρουσιάζονται συνοπτικά οι μηχανισμοί που υποστηρίζονται από το μοντέλο ασφαλείας που προτείνει η IBM και η Microsoft.

Απαιτήσεις Ασφάλειας	Μηχανισμοί	Υποστήριξη από
Εμπιστευτικότητα της πληροφορίας	Αμοιβαία αυθεντικοποίηση πελάτη-υπηρεσίας	Transport Protocol (π.χ. SSL)
	Κρυπτογράφηση των μηνυμάτων που ανταλλάσσονται.	Transport Protocol (π.χ. SSL)

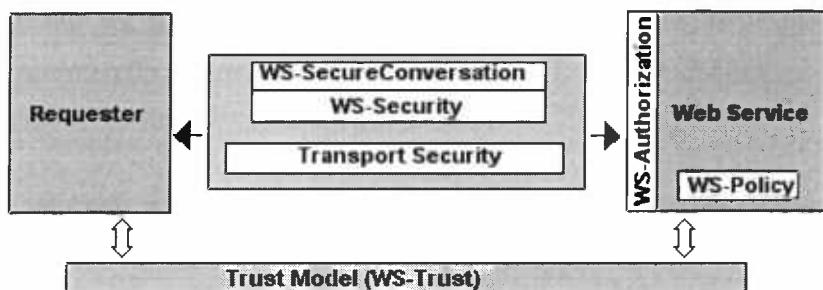
	Επίπεδο Εφαρμογής	Έλεγχος Πρόσβασης στην υπηρεσία ή στον κατάλογο υπηρεσιών Κρυπτογράφηση των μηνυμάτων που ανταλλάσσονται. Ανίχνευση	X.509 ή Kerberos Tickets WS-SecureConversation WS-Secure WS-Trust WS-Policy WS-Authorization WS-Conversation WS-Security WS-Policy WS-Privacy
Εγκυρότητα της πληροφορίας	Επίπεδο Μεταφοράς	Αμοιβαία αυθεντικοποίηση πελάτη-υπηρεσίας.	Transport Protocol (π.χ. SSL)
		Έλεγχος ακεραιότητας των μηνυμάτων που ανταλλάσσονται.	Transport Protocol (π.χ. SSL)
	Επίπεδο Εφαρμογής	Έλεγχος Πρόσβασης στην υπηρεσία ή στον κατάλογο υπηρεσιών. Έλεγχος ακεραιότητας των μηνυμάτων που ανταλλάσσονται. Ανίχνευση	X.509 ή Kerberos Tickets WS-SecureConversation WS-Secure WS-Trust WS-Policy WS-Authorization WS-Security WS-Policy WS-Privacy
Διαθεσιμότητα της Υπηρεσίας		Έλεγχος Πρόσβασης στην υπηρεσία ή στον κατάλογο υπηρεσιών. Ανίχνευση	X.509 ή Kerberos Tickets WS-SecureConversation WS-Secure WS-Trust WS-Policy WS-Authorization WS-Policy WS-Privacy
Εγκυρότητα του λογισμικού της Υπηρεσίας		Έλεγχος Πρόσβασης στην υπηρεσία ή στον κατάλογο υπηρεσιών. Ανίχνευση	X.509 ή Kerberos Tickets WS-SecureConversation WS-Secure WS-Trust WS-Policy WS-Authorization WS-Policy WS-Privacy
Μη αποποίηση της ευθύνης (παραλήπτη, αποστολέα, ενδιαμέσου)	Αποθήκευση και προώθηση μηνυμάτων από έμπιστο φορέα που παρέχει Υπηρεσία Μη-Αποποίησης		WS-Security

Πίνακας 7.1.: Μηχανισμοί ασφάλειας.

Εκ πρώτης άποψης, το μοντέλο επιτυγχάνει να ενοποιήσει τους μηχανισμούς και τις βασικές τεχνολογίες που αναφέρθηκαν στο κεφάλαιο 6, περιλαμβάνοντας μηχανισμούς που μπορούν να υλοποιηθούν στα επίπεδα μεταφοράς και εφαρμογής. Στη συνέχεια εξετάζονται περισσότερο αναλυτικά οι παραπάνω μηχανισμοί.

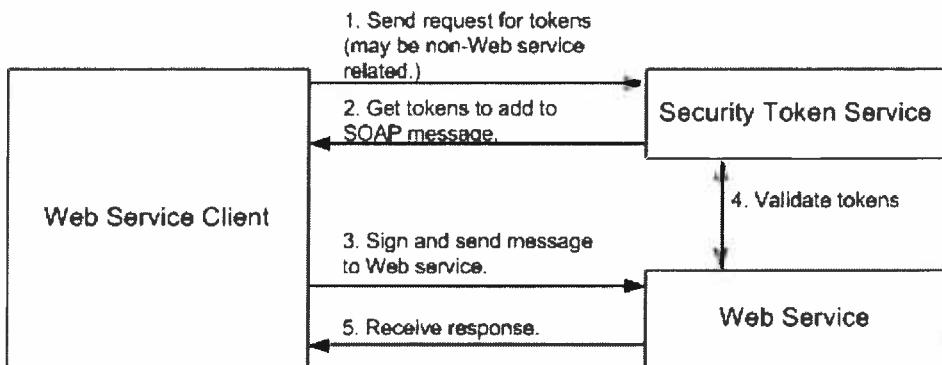
7.4.1. Αυθεντικοποίηση πελάτη-υπηρεσίας και Έλεγχος πρόσβασης.

Σύμφωνα με το μοντέλο ασφάλειας των IBM και Microsoft, το WS-SecureConversation πρόκειται να παρέχει ένα σύνολο προδιαγραφών που θα υποστηρίζουν την αυθεντικοποίηση του πελάτη και της υπηρεσίας (σχήμα 7.2.). Το WS-SecureConversation έχει σχεδιαστεί για να λειτουργήσει σε επίπεδο εφαρμογής, με βάση τις προδιαγραφές του WS-Security, ωστόσο το μοντέλο ασφάλειας θα παρέχει και τη δυνατότητα αξιοποίησης των μηχανισμών αυθεντικοποίησης των πρωτοκόλλων του επίπεδου μεταφοράς. Για παράδειγμα, σε συγκεκριμένες συνδέσεις, ένας απλός τρόπος αυθεντικοποίησης του πελάτη θα είναι η αποστολή ενός unsigned token (username) ή ενός signed token ενός πελάτη, μέσω του Secure Socket Layer. Τα είδη των signed tokens που υποστηρίζει το WS-Security είναι τα X.509 certificates και τα Kerberos tickets.



Σχήμα 7.2.: Έλεγχος Πρόσβασης στο μοντέλο ασφάλειας των IBM και Microsoft

Στην περίπτωση που μια υπηρεσία εμπιστεύεται άμεσα το διαπιστευτήριο ενός πελάτη, η αυθεντικοποίηση θα πραγματοποιείται χωρίς άλλη προϋπόθεση. Διαφορετικά, θα είναι απαραίτητη η ύπαρξη μιας έμπιστης οντότητας που θα εκδίδει διαπιστευτήρια στους πελάτες που θα θέλουν να αυθεντικοποιηθούν από μια υπηρεσία (σχήμα 7.3.). Το μοντέλο WS-Trust θα υποστηρίζει τις υπηρεσίες που εκδίδουν διαπιστευτήρια με χρήση δημόσιων κρυπτογραφικών κλειδιών. Ως προς το τελευταίο θα μοιάζει με το PKI trust model, χωρίς αυτό να σημαίνει ότι θα νιοθετηθεί το PKI σαν μοντέλο εμπιστοσύνης.



Σχήμα 7.3.: Έκδοση Διαπιστευτηρίων στο μοντέλο ασφάλειας των IBM και Microsoft.

Ο μηχανισμός εξουσιοδότησης ενός πελάτη θα στηρίζεται στο σύνολο προδιαγραφών WS-authorization. Με βάση τις προδιαγραφές αυτές η υπηρεσία θα μπορεί να διαχειρίζεται τα δεδομένα εξουσιοδότησης και τις πολιτικές εξουσιοδότησης, οι οποίες θα ακολουθούν τις WS-Policy προδιαγραφές.

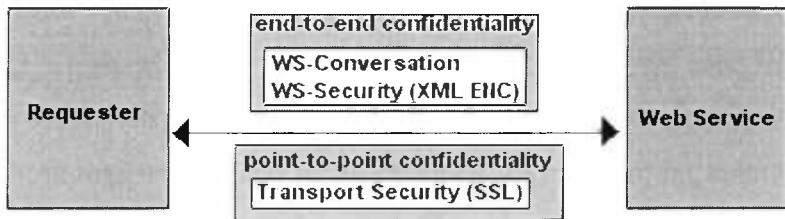
Επομένως, σε ότι αφορά τον έλεγχο πρόσβασης το μοντέλο ασφαλείας γενικά καλύπτει τις απαιτήσεις που είχαν τεθεί στο προηγούμενο κεφάλαιο, αν και δεν παρέχει επαρκή πληροφόρηση για τις διαδικασίες που θα υποστηρίζει η υπηρεσία έκδοσης διαπιστευτηρίων. Επίσης, δεν αναφέρεται αν θα υποστηρίζεται η πρόσβαση από ένα σημείο (single sign-on) και γενικά αν θα είναι δυνατή η μεταβίβαση διαβεβαιώσεων ασφάλειας. Ίσως, κάτι τέτοιο να υποστηριχτεί μέσω του WS-federation, όμως προς το παρόν δεν έχει επισημανθεί οτιδήποτε. Πάντως, ακόμα και αν η απάντηση στο προηγούμενο ερώτημα είναι θετική, τίθεται το ερώτημα αν το μοντέλο θα υποστηρίζει τα πρότυπα SAML και XACML.

7.4.2. Κρυπτογράφηση μηνυμάτων.

Ένας από τους στόχους του WS-SecureConversation, όπως προκύπτει από την περιγραφή του, θα είναι να παρέχει τις προδιαγραφές για την υλοποίηση ενός μηχανισμού κρυπτογράφησης μηνυμάτων σε επίπεδο εφαρμογής. Το WS-SecureConversation έχει σχεδιαστεί στην κορυφή του WS-Security, το οποίο ως γνωστόν υποστηρίζει την XML κρυπτογράφηση, επομένως μπορεί να παρέχει εξασφάλιση της end-to-end εμπιστευτικότητας των μηνυμάτων.

Το μοντέλο ασφάλειας υποστηρίζει, ωστόσο, και μηχανισμούς κρυπτογράφησης του επιπέδου μεταφοράς, με τη διαφορά ότι τους εφαρμόζει μόνο στην περίπτωση που η

επικοινωνία του πελάτη με την υπηρεσία γίνεται σε ένα βήμα (hop). Και οι δύο περιπτώσεις απεικονίζονται στο σχήμα 7.4.



Σχήμα 7.4.: Κρυπτογράφηση μηνυμάτων στο μοντέλο ασφάλειας των IBM και Microsoft.

Συνεπώς, σε ότι αφορά την κρυπτογράφηση των μηνυμάτων, το μοντέλο πληροί τις απαιτήσεις που είχαν τεθεί στο κεφάλαιο 6. Στο ζήτημα αυτό δεν υπάρχουν ερωτήματα χωρίς απάντηση, από τη στιγμή που και η πρώτη έκδοση του WS-Security είναι διαθέσιμη.

7.4.3. Έλεγχος ακεραιότητας των μηνυμάτων.

Ο μηχανισμός ελέγχου της ακεραιότητας των μηνυμάτων στηρίζεται στο σύνολο προδιαγραφών WS-Security. Το τελευταίο υποστηρίζει την τεχνολογία των XML ψηφιακών υπογραφών, επιτρέποντας έτσι τον υπολογισμό μιας σύνοψης ξεχωριστά για κάθε τμήμα του XML μηνύματος και κατόπιν την υπογραφή αυτού. Φυσικά, υπάρχει και η δυνατότητα εφαρμογής των ίδιων τεχνικών για ολόκληρο το XML μήνυμα, είτε μέσω της XML ψηφιακής υπογραφής, είτε και μέσω των μηχανισμών του πρωτοκόλλου SSL. Το μοντέλο υποστηρίζει και τα δύο. Η διαφορά βέβαια είναι ότι με την εφαρμογή των τεχνικών σε τμήματα του μηνύματος που αφορούν σε ένα συγκεκριμένο αποστολέα, εξασφαλίζεται η end-to-end ακεραιότητα του μηνύματος. Οι μηχανισμοί του SSL και σε αυτή την περίπτωση μπορούν να χρησιμοποιηθούν σε μια point-to-point σύνδεση.

Επομένως, το μοντέλο σε ότι αφορά τον έλεγχο ακεραιότητας των μηνυμάτων καλύπτει τις ζητούμενες απαιτήσεις. Η μοναδική αδυναμία του μηχανισμού αφορά μόνο στην περίπτωση απώλειας του μυστικού κλειδιού, κάτι που ισχύει και για την κρυπτογράφηση των μηνυμάτων.

7.4.4. Υπηρεσία μη αποποίησης.

Για την εξασφάλιση της μη αποποίησης της ευθύνης από τον πελάτη, την υπηρεσία ή την ενδιάμεση οντότητα που προωθεί ένα μήνυμα, στο προηγούμενο κεφάλαιο είχε επισημανθεί η ανάγκη ύπαρξης μιας υπηρεσίας μη αποποίησης. Η υπηρεσία αυτή θα είναι ουσιαστικά μια υπηρεσία διαδικτύου που θα έχει τον ρόλο του μεσάζοντα σε κάθε αποστολή ενός μηνύματος, αναλαμβάνοντας: α) να προωθεί τα μηνύματα στον παραλήπτη τους, αφού πρώτα τους τοποθετήσει μια σφραγίδα χρόνου και τα υπογράψει ψηφιακά, και β) να αποθηκεύει τα μηνύματα για την παροχή αποδείξεων σε περιπτώσεις αποποίησης της ευθύνης.

Το σύνολο προδιαγραφών WS-Security δύναται να υποστηρίξει μια υπηρεσία μη-αποποίησης, από τη στιγμή που καθορίζει πώς μπορεί να επισυναφθεί μια ψηφιακή υπογραφή σε ένα XML μήνυμα. Οι ίδιες προδιαγραφές, άλλωστε, καθορίζουν με ποιο τρόπο μπορεί να επισυναφθεί οποιοδήποτε token σε ένα XML μήνυμα, επομένως μπορούν να υποστηρίξουν και την επισύναψη μιας σφραγίδας χρόνου σε αυτό.

Επομένως, το προτεινόμενο μοντέλο ασφαλείας παρέχει την υποστήριξη που χρειάζεται για τη λειτουργία μιας υπηρεσίας μη αποποίησης. Ωστόσο, πρέπει να επισημανθεί ότι απαραίτητη προϋπόθεση για τη χρησιμοποίηση μιας υπηρεσίας μη αποποίησης είναι η εμπιστοσύνη του αποστολέα και του παραλήπτη του μηνύματος στον φορέα της υπηρεσίας αυτής. Για την εξασφάλιση της επικοινωνίας ενός πελάτη με την υπηρεσία μη αποποίησης, εξακολουθεί να ισχύει ότι αναφέρθηκε στην περίπτωση επικοινωνίας ενός πελάτη με μια υπηρεσία διαδικτύου.

7.4.5. Ανίχνευση.

Η περιγραφή του μοντέλο ασφάλειας που προτείνουν οι εταιρείες IBM και Microsoft δεν αναφέρεται στην υποστήριξη που παρέχεται σε μηχανισμούς ανίχνευσης, εντούτοις το μοντέλο δύναται να παρέχει υποστήριξη σε εργαλεία ανίχνευσης. Τα εργαλεία αυτά καταγράφουν γεγονότα που λαμβάνουν χώρα σε ένα σύστημα, τα οποία αναλύονταν στη συνέχεια, προκειμένου να ανιχνεύσουν ένα περιστατικό ή μια παραβίαση. Σε ότι αφορά το δεύτερο, η WS-Policy περιγραφή, μπορεί να αποτελέσει τη βάση για την αναγνώριση ενεργειών που δεν είναι επιτρεπτές. Εντούτοις, το μοντέλο ασφάλειας θα πρέπει να υποστηρίζει επίσης: α) μηχανισμούς προστασίας της εγκυρότητας των αρχείων καταγραφής, και β) μηχανισμούς προστασίας της εμπιστευτικότητα των καταγραφών, όπως επιβάλει η ανάγκη για προστασία της ιδιωτικότητας των χρηστών. Ο έλεγχος πρόσβασης, όπως υποστηρίζεται από το μοντέλο (βλ. ενότητα 7.4.1), δύναται να εξασφαλίσει ότι οι ενέργειες

που καταγράφονται για ένα πελάτη της υπηρεσίας συνδέονται όντως με αυτόν τον πελάτη και επιπλέον μπορεί να εμποδίσει την πρόσβαση των πελατών στα αρχεία καταγραφής των ενεργειών. Τέλος, οι WS-Privacy προδιαγραφές μπορούν να υποστηρίζουν την ενσωμάτωση στην περιγραφή WS-Policy, δηλώσεων που αφορούν στη διαχείριση των αρχείων καταγραφής.

Επομένως, το μοντέλο μπορεί να υποστηρίξει επαρκώς τα εργαλεία ανίχνευσης προσβολών.

7.5. Αξιολόγηση του μοντέλου ασφάλειας – Συμπέρασμα.

Με βάση την ανάλυση που προηγήθηκε, η βασική διαπίστωση είναι ότι το μοντέλο ασφαλείας που προτείνουν οι εταιρείες IBM και Microsoft, όπως έχει σχεδιαστεί, δύναται να αποτελέσει ένα γενικό πλαίσιο ασφάλειας που θα ικανοποιεί τις κύριες απαιτήσεις ασφάλειας των υπηρεσιών διαδικτύου. Διαθέτει με άλλα λόγια τα χαρακτηριστικά εκείνα που το καθιστούν πλήρες μοντέλο, εφόσον βέβαια ο στόχος του είναι η κάλυψη των απαιτήσεων ασφάλειας που αναφέρονται στην παρούσα εργασία. Προς το παρόν βέβαια, υπάρχουν πολλές εκκρεμότητες μέχρι την ολοκλήρωση του συνόλου των προδιαγραφών.

Ασφαλώς στο μέλλον, με την ανάπτυξη των υπηρεσιών διαδικτύου, το μοντέλο θα πρέπει να μπορεί να επεκταθεί προκειμένου να καλύψει και νέες απαιτήσεις ασφάλειας, που οπωσδήποτε θα υπάρξουν. Προς το παρόν, απαραίτητη προϋπόθεση για την επιτυχία του μοντέλου, είναι η υποστήριξη του από τους πελάτες και τους χορηγούς των υπηρεσιών διαδικτύου, και ασφαλώς και η συνεργασία με τους οργανισμούς ανάπτυξης προτύπων.



ΚΕΦΑΛΑΙΟ 8^ο : ΥΛΟΠΟΙΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

8.1. Εισαγωγή.

Στο προηγούμενο κεφάλαιο έγινε αναφορά σε ένα υπό κατασκευή μοντέλο ασφάλειας για τις υπηρεσίες διαδικτύου, που είναι πρωτοβουλία των εταιρειών IBM και Microsoft. Το μοντέλο αυτό έχει ως στόχο να καθορίσει ένα γενικό πλαίσιο ασφάλειας το οποίο μπορεί να χρησιμοποιηθεί για την ανάπτυξη ασφαλών υπηρεσιών ή για τη μετατροπή υφιστάμενων υπηρεσιών σε ασφαλείς.

Στο κεφάλαιο αυτό εξετάζεται ποιες από τις προδιαγραφές του μοντέλου ασφαλείας υποστηρίζονται, και σε ποιο βαθμό, από τις δύο πλατφόρμες ανάπτυξης εφαρμογών που μελετήθηκαν στο κεφάλαιο 4. Γίνεται αναφορά στις υπηρεσίες ασφάλειας που παρέχουν οι πλατφόρμες Microsoft .NET και Java 2 Enterprise Edition για την υποστήριξη των μηχανισμών ασφαλείας των υπηρεσιών διαδικτύου και επισημαίνονται οι ελλείψεις τους.

8.2. Ασφάλεια στο .NET.

Το Microsoft .NET περιλαμβάνει ένα σύνολο από εργαλεία λογισμικού και υπηρεσίες, που βασίζονται στα πρότυπα ασφάλειας και υλοποιούν τους μηχανισμούς ασφάλειας για τις υπηρεσίες διαδικτύου, που αναφέρθηκαν στα προηγούμενα κεφάλαια. Στον πίνακα 8.1. δίνεται μια συνοπτική εικόνα του τρόπου με τον οποίο η πλατφόρμα .NET παρέχει τους μηχανισμούς που εξασφαλίζουν επαρκώς τις απαιτήσεις για εμπιστευτικότητα και ακεραιότητα της πληροφορίας, διαθεσιμότητα της υπηρεσίας, εγκυρότητα του λογισμικού και μη αποποίηση της ευθύνης.

Απαιτήσεις Ασφάλειας	Μηχανισμοί	Υλοποίηση	
Εμπιστευτικότητα της πληροφορίας	Επίπεδο Μεταφοράς	Αυθεντικοποίηση Πελάτη-Υπηρεσίας	<input checked="" type="checkbox"/> SSL (IIS) <input checked="" type="checkbox"/> Username or X.509
	Κρυπτογράφηση Μηνυμάτων	<input checked="" type="checkbox"/> SSL (IIS) <input checked="" type="checkbox"/> Message Authentication Code	
	Επίπεδο Εφαρμογής	Αυθεντικοποίηση	<input checked="" type="checkbox"/> Digest, NTLM, Kerberos (IIS) <input checked="" type="checkbox"/> .NET Passport (Passport SDK) <input checked="" type="checkbox"/> SOAP-based (WSDK)
		Εξουσιοδότηση	Role-based <input checked="" type="checkbox"/> Admin. tools, Config. settings <input checked="" type="checkbox"/> Programmatic (components)
		Κρυπτογράφηση Μηνυμάτων	<input checked="" type="checkbox"/> Encryption (Crypto API) <input checked="" type="checkbox"/> XML encryption (WSDK)

Εγκυρότητα της πληροφορίας	Επίπεδο Μεταφοράς	Αυθεντικοποίηση Πελάτη-Υπηρεσίας	✓ SSL (IIS) ✓ Username or X.509
		Κρυπτογράφηση Μηνυμάτων	✓ SSL (IIS) ✓ Message Authentication Code
	Επίπεδο Εφαρμογής	Αυθεντικοποίηση	✓ Digest, NTLM, Kerberos (IIS) ✓ .NET Passport (Passport SDK) ✓ SOAP-based (WSDK)
		Εξουσιοδότηση	Role-based ✓ Admin. tools, Config. settings ✓ Programmatic (components)
		Έλεγχος ακεραιότητας μηνυμάτων	✓ Hash Function-Dig. Signature (Crypto API) ✓ XML Dig. Signatures (WSDK)
	Διαθεσιμότητα της Υπηρεσίας	Αυθεντικοποίηση	✓ Digest, NTLM, Kerberos (IIS) ✓ .NET Passport (Passport SDK) ✓ SOAP-based (WSDK)
		Εξουσιοδότηση	Role-based ✓ Admin. tools, Config. settings ✓ Programmatic (components)
		Έλεγχος του κώδικα που εκτελείται	✓ Code Access Security (CLR) ✓ Verification Process (CLR)
	Εγκυρότητα του λογισμικού της Υπηρεσίας	Αυθεντικοποίηση	✓ Digest, NTLM, Kerberos (IIS) ✓ .NET Passport (Passport SDK) ✓ SOAP-based (WSDK)
		Εξουσιοδότηση	Role-based ✓ Admin. tools, Config. settings ✓ Programmatic (components)
		Έλεγχος του κώδικα που εκτελείται	✓ Code Access Security (CLR) ✓ Verification Process (CLR)
Μη αποποίηση της ευθύνης	Ψηφιακή υπογραφή και καταγραφή συναλλαγών	✓ Digital Signatures (Crypto API) ✓ XML Digital Signatures (WSDK) ✓ Third Party	

Πίνακας 8.1.: Υλοποίηση των μηχανισμών ασφάλειας στην πλατφόρμα .NET.

Οι παραπάνω μηχανισμοί ασφάλειας που αφορούν στις υπηρεσίες διαδικτύου και ο τρόπος με τον οποίο υλοποιούνται στην πλατφόρμα Microsoft .NET αναλύονται στη συνέχεια.

8.2.1. Αυθεντικοποίηση.

Το Microsoft .NET υποστηρίζει αρκετές μεθόδους αυθεντικοποίησης. Αυτές είναι οι μέθοδοι αυθεντικοποίησης που παρέχει το ίδιο το λειτουργικό σύστημα των Microsoft Windows, η μέθοδος αυθεντικοποίησης διαμέσου μιας τρίτης οντότητας (.NET Passport) και

η μέθοδος που στηρίζεται στην ενσωμάτωση πληροφορίας αυθεντικοποίησης σε ένα SOAP μήνυμα [.NET SEC].

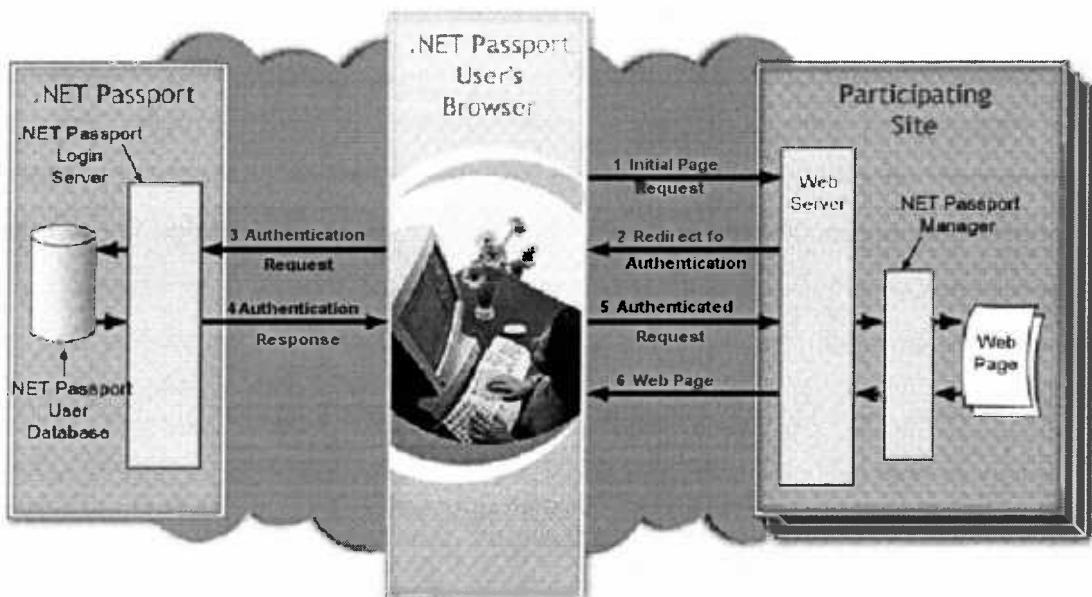
Σε επίπεδο μεταφοράς, δύναται να χρησιμοποιηθεί για την αμοιβαία αυθεντικοποίηση πελάτη και υπηρεσίας το πρωτόκολλο SSL, το οποίο υποστηρίζεται από τον Microsoft Internet Information Server (περιλαμβάνεται στο λειτουργικό σύστημα Windows 2000). Το πρωτόκολλο αυτό, όπως έχει αναφερθεί και στα προηγούμενα κεφάλαια, μπορεί να χρησιμοποιηθεί όταν η επικοινωνία πελάτη και υπηρεσίας γίνεται χωρίς τη μεσολάβηση ενδιάμεσων οντοτήτων (point-to-point σύνδεση).

Σε επίπεδο εφαρμογής, τα Windows 2000 και τα Windows NT υποστηρίζουν την αυθεντικοποίηση του πελάτη με χρήση των πρωτοκόλλων Kerberos και NTLM αντίστοιχα. Ωστόσο, το πρωτόκολλο NTLM της Microsoft είναι κατάλληλο για ένα Intranet περιβάλλον, και επιπλέον περιορίζει τον πελάτη στη χρήση συγκεκριμένου λειτουργικού συστήματος και συγκεκριμένου browser. Το Kerberos είναι ένα πρωτόκολλο που αναπτύχθηκε από το MIT και έχει υλοποιηθεί σε αρκετές πλατφόρμες. Σε αντίθεση με το NTLM, υποστηρίζει τη δυνατότητα αυθεντικοποίησης της υπηρεσίας και αντιπροσωπείας της ταυτότητας (identity delegation) του χρήστη, επιτρέποντας server-to-server σενάρια. Μολονότι οι περισσότεροι οργανισμοί χρησιμοποιούν το Kerberos στο εσωτερικό τους δίκτυο και δεν επιτρέπουν σε πελάτες να μπορούν να κάνουν αιτήσεις μέσω του διαδικτύου για την έκδοση εισιτηρίου, το οποίο θα τους επιτρέψει να χρησιμοποιήσουν μια υπηρεσία, το Kerberos μπορεί, αν αξιοποιηθεί κατάλληλα, να αποτελέσει μια λύση για την αυθεντικοποίηση υπηρεσιών διαδικτύου.

Η αυθεντικοποίηση με χρήση digest, είναι ιδιαίτερα απλή μέθοδος, που εφαρμόζει τον αλγόριθμο MD5 της εταιρείας RSA στο συνθηματικό του πελάτη πριν την αποστολή του στην υπηρεσία. Δημιουργήθηκε για το Internet και υποστηρίζεται στον server της υπηρεσίας από το λειτουργικό σύστημα Windows 2000. Ωστόσο, δεν αποτελεί ιδιαίτερα ασφαλή λύση, αφού δεν εμποδίζει κάποιο τρίτο που θα κατορθώσει να υπεξαιρέσει ένα μήνυμα που περιέχει την πληροφορία αυθεντικοποίησης, να επαναλάβει την αποστολή του (replay attack), προκαλώντας ακόμα και άρνηση της υπηρεσίας (denial of service). Επίσης δεν υποστηρίζει την αντιπροσωπεία ενός χρήστη από τον server (delegation).

Το .NET Passport (βλ. ενότητα 4.4.4.) είναι μια κεντρικοποιημένη form-based υπηρεσία αυθεντικοποίησης που παρέχει μοναδικό σημείο πρόσβασης για πολλαπλά domains. Η χρήση του Passport από μια υπηρεσία απαιτεί την εγγραφή και την εγκατάσταση του Passport SDK στον server. Μια υπηρεσία που έχει εγγραφεί στο .NET Passport, δεν χρειάζεται να διατηρεί

πληροφορίες αυθεντικοποίησης για τους πελάτες της, οι οποίοι αυθεντικοποιούνται για λογαριασμό της υπηρεσίας από το .NET Passport (σχήμα 8.1.).



Σχήμα 8.1. : .NET Passport Authentication. [Skoularidou et al., 2002]

Το μειονέκτημα του Passport είναι ότι δεν αυθεντικοποιεί πελάτες οι οποίοι είναι εφαρμογές που καλούν την υπηρεσία μέσω του κώδικα ενός προγράμματος. Εντούτοις, όπως έχει ανακοινώσει η Microsoft, μέσα στο έτος 2003 η υπηρεσία .NET Passport θα παρέχεται ως υπηρεσία διαδικτύου, υποστηρίζοντας δηλαδή το πρωτόκολλο SOAP. Έτσι θα μπορεί να καλείται από XML υπηρεσίες διαδικτύου, στις οποίες θα παρέχει υπηρεσίες αυθεντικοποίησης των πελατών τους.

Αντίθετα, το εργαλείο WSDK (Web Services Development Kit), που αποτελεί υλοποίηση των WS-Security προδιαγραφών είναι ήδη έτοιμο. Το WSDK επιτρέπει την επισύναψη ενός πιστοποιητικού X.509 σε ένα SOAP μήνυμα, δίνοντας με αυτό τον τρόπο τη δυνατότητα σε ένα πελάτη να αυθεντικοποιηθεί από μια υπηρεσία διαδικτύου.

8.2.2. Εξουσιοδότηση.

Το Microsoft .NET υποστηρίζει τη βασισμένη σε ρόλους (role-based) εξουσιοδότηση του χρήστη να καλεί ένα στοιχείο (component) μιας υπηρεσίας [.NET SEC]. Η διαδικασία στηρίζεται στην αναγνώριση ρόλων, που σχετίζονται με κατηγορίες χρηστών του συστήματος, και ορίζονται από την πολιτική ασφαλείας της υπηρεσίας (.NET Framework).

Policy). Με τον τρόπο αυτό, αντί να καθορίζεται η πρόσβαση σε ένα στοιχείο για κάθε ένα χρήστη, καθορίζεται για κάθε ρόλο. Ένας ρόλος αντιστοιχείται με ένα συγκεκριμένο σύνολο από δικαιώματα πρόσβασης και προνόμια. Μια εξουσιοδότηση δίνεται σε ένα χρήστη προκειμένου να υιοθετήσει ένα ρόλο [Samarati et al., 2001]. Η εξουσιοδότηση ελέγχεται από τους διαχειριστές του συστήματος (system administrators), ή τους δημιουργούς των στοιχείων (component creators). Στην πρώτη περίπτωση, ο καθορισμός των δικαιωμάτων και των προνομίων ενός ρόλου συνήθως γίνεται με τη βοήθεια εργαλείων διαχείρισης του συστήματος (administrative tools) και επιλογών διαμόρφωσης (configuration settings). Στη δεύτερη περίπτωση, ο ίδιος ο δημιουργός του στοιχείου καθορίζει προγραμματιστικά ποιο τμήμα του κώδικα θα εκτελεστεί ανάλογα με τον ρόλο που έχει δοθεί σε ένα χρήστη (βλ. σχήμα 8.2.).

```
If User.IsInRole("Broker")
    ' Permit requested function
Else
    ' Bounce back to login
End If
```

Σχήμα 8.2.: Programmatic Authorization.

8.2.3. Κρυπτογράφηση μηνυμάτων.

Το Microsoft .NET με την επιλογή των κατάλληλων ρυθμίσεων του IIS Server υποστηρίζει το πρωτόκολλο SSL, επιτρέποντας την κρυπτογράφηση μιας συνόδου. Επίσης, το .NET Framework παρέχει μια διεπαφή (CryptoAPI) που αποτελεί μέρος του λειτουργικού συστήματος των Windows και προσφέρει δυνατότητες κρυπτογράφησης. Το CryptoAPI υποστηρίζει τους αλγόριθμους δημοσίας κρυπτογράφησης RSA και DSA, τους συμμετρικούς αλγόριθμους DES, TripleDES και RC2, και τους αλγόριθμους σύνοψης MD5 και SHA1. Επίσης, υποστηρίζει τα πρότυπα PKCS #7 και PKCS #10, που περιγράφουν ένα συντακτικό μεταφοράς για αιτήσεις πιστοποιητικών και ένα γενικό συντακτικό για δεδομένα στα οποία έχει εφαρμοσθεί κάποιος κρυπτογραφικός αλγόριθμος (π.χ. ψηφιακές υπογραφές) αντίστοιχα. Το CryptoAPI παρέχει τη δυνατότητα στους developers του .NET να ενσωματώσουν κρυπτογραφικές λειτουργίες στις εφαρμογές τους, ωστόσο δεν παρέχει υποστήριξη σε τεχνολογίες όπως XML κρυπτογραφία και XML ψηφιακή υπογραφή. Οι δυνατότητες αυτές παρέχονται μέσω του εργαλείου WSDK, το οποίο αποτελεί υλοποίηση του WS-Security από την Microsoft. Η XML κρυπτογράφηση επιτρέπει την κρυπτογράφηση ολόκληρου ή μέρους

του SOAP μηνύματος, εξασφαλίζοντας την end-to-end εμπιστευτικότητα των πληροφοριών που περιέχει, κατά τη μετάδοση του.

8.2.4. Έλεγχος ακεραιότητας των μηνυμάτων.

Στο Microsoft .NET ο έλεγχος ακεραιότητας των μηνυμάτων, στην περίπτωση που έχει επιλεγεί το πρωτόκολλο μεταφοράς SSL για την επικοινωνία του πελάτη με την υπηρεσία, υποστηρίζεται από το ίδιο το πρωτόκολλο, με χρήση των Message Authentication Codes (βλ. ενότητα 6.3.4.).

Σε επίπεδο εφαρμογής το .NET υποστηρίζει μέσω του CryptoAPI την εφαρμογή μιας συνάρτησης σύνοψης για κάθε SOAP μήνυμα που αποστέλλεται και εν συνεχείᾳ την ψηφιακή υπογραφή της σύνοψης, επιτρέποντας τον έλεγχο της ακεραιότητάς του στον παραλήπτη. Το μοναδικό μειονέκτημα της μεθόδου αυτής είναι ότι αν ένα μήνυμα φτάσει σε ένα παραλήπτη που δεν είναι ο τελικός προορισμός του, προκειμένου να προωθηθεί στον τελικό του παραλήπτη θα πρέπει να αλλάξουν κάποια από τα δεδομένα που περιλαμβάνονται στην επικεφαλίδα του μηνύματος. Αυτό θα έχει ως αποτέλεσμα να μην επιβεβαιωθεί η ακεραιότητα του μηνύματος στον παραλήπτη. Το εργαλείο WSDK επιτρέπει την εφαρμογή ενός αλγορίθμου σύνοψης σε τμήμα του SOAP εγγράφου και εν συνεχείᾳ την υπογραφή μόνο του συγκεκριμένου τμήματος με χρήση της XML ψηφιακής υπογραφής.

8.2.5. Έλεγχος του κώδικα που εκτελείται.

Στην ενότητα 3.4.1. έγινε αναφορά στο περιβάλλον χρόνου εκτέλεσης κοινής γλώσσας (CLR) του .NET Framework. Το CLR είναι η λειτουργική μονάδα που ευθύνεται για τη διαχείριση της μεταγλώττισης και εκτέλεσης του κώδικα. Η μεταγλώττιση του κώδικα δημιουργεί έναν ενδιάμεσο κώδικα, που ονομάζεται MSIL (Microsoft Intermediate Language) και βρίσκεται σε υψηλότερο επίπεδο από τον κώδικα μηχανής. Ο MSIL κώδικας περιλαμβάνει metadata (δηλαδή στοιχεία με πληροφορίες για τη χρήση τους) που χρησιμοποιεί το CLR για να εντοπίσει και να «φορτώσει» τις κλάσεις, να τοποθετήσει αντικείμενα στη μνήμη, να ελέγξει την ασφάλεια και να πραγματοποιήσει μια σειρά από πρόσθετες λειτουργίες. Ο έλεγχος της ασφάλειας του κώδικα που πρόκειται να εκτελεστεί είναι από τις βασικές λειτουργίες του CLR [.NET SEC].



Κατά τον χρόνο εκτέλεσης, ένα τμήμα κώδικα απαιτεί τα δικαιώματα (permissions) που καθορίζονται στα metadata, για να αποκτήσει πρόσβαση σε κάποιο πόρο. Όταν συμβεί αυτό, το CLR εκτελεί μια διαδικασία που είναι γνωστή ως “stack walk” προκειμένου να ελέγξει ότι όχι μόνο το συγκεκριμένο τμήμα κώδικα, αλλά όλα τα τμήματα κώδικα της call-chain στοιβας δεν έχουν παραβιάσει τα επιτρεπτά τους δικαιώματα. Σε περίπτωση που κάποιο τμήμα κώδικα αποτύχει σε αυτόν τον έλεγχο, παράγεται ένα security exception.

Το τελευταίο στάδιο στον έλεγχο της ασφάλειας του κώδικα που εκτελείται, είναι η διαδικασία της επαλήθευσης (verification process). Η διαδικασία αυτή εμποδίζει την εμφάνιση συνηθισμένων τύπων σφαλμάτων, που οφείλονται σε προγραμματιστικά λάθη, τα οποία συχνά είναι πηγή αδυναμιών για τις εφαρμογές.

8.2.6. Ψηφιακή υπογραφή και καταγραφή συναλλαγών.

Το Microsoft .NET παρέχει μέσω της CryptoAPI διεπαφής τη δυνατότητα στους developers να αξιοποιήσουν την τεχνολογία των ψηφιακών υπογραφών στις εφαρμογές τους. Το WSDK, παρέχει την ίδια δυνατότητα υποστηρίζοντας και τις XML ψηφιακές υπογραφές. Μια υπηρεσία μπορεί να χρησιμοποιήσει σαν μηχανισμό για την εξασφάλιση της μη αποποίησης της ευθύνης του πελάτη τη ψηφιακή υπογραφή ενός μηνύματος από τον ίδιο τον πελάτη και εν συνεχεία την αποθήκευσή του σε ένα tamper-proof αρχείο καταγραφών (audit trail). Εντούτοις, με τον τρόπο αυτό μπορεί να εξασφαλιστεί μόνο η μη αποποίηση της ευθύνης του αποστολέα. Για τη μη αποποίηση της ευθύνης του παραλήπτη είναι απαραίτητη η ύπαρξη μιας έμπιστης τρίτης οντότητας που θα παρέχει υπηρεσίες μη αποποίησης. Η οντότητα αυτή θα αποθηκεύει και θα προωθεί τα μηνύματα από τον αποστολέα στον παραλήπτη τους, υπογράφοντας τα ψηφιακά και τοποθετώντας τους σφραγίδες χρόνου.

8.3. Ασφάλεια στο J2EE.

Το Java 2 Enterprise Edition αποτελεί πρότυπο σε αντίθεση με το Microsoft .NET που είναι προϊόν. Αυτό σημαίνει ότι ο τρόπος με τον οποίο υλοποιούνται οι υπηρεσίες ασφάλειας που παρέχουν οι J2EE πλατφόρμες στις υπηρεσίες διαδικτύου, είναι σε αρκετές περιπτώσεις απόφαση των προμηθευτών, αλλά και των υπεύθυνων ανάπτυξης.

Στον πίνακα 8.2. δίνεται απλά μια γενική εικόνα του τρόπου με τον οποίο υλοποιούνται στις J2EE πλατφόρμες οι μηχανισμοί που παρέχουν εξασφάλιση των απαιτήσεων για



εμπιστευτικότητα και ακεραιότητα της πληροφορίας, διαθεσιμότητα της υπηρεσίας, εγκυρότητα του λογισμικού και μη αποποίηση της ευθύνης.

Απαιτήσεις Ασφάλειας	Μηχανισμοί	Υλοποίηση	
Εμπιστευτικότητα της πληροφορίας	Επίπεδο Μεταφοράς	Αυθεντικοποίηση Πελάτη-Υπηρεσίας	
		Κρυπτογράφηση Μηνυμάτων	
	Επίπεδο Εφαρμογής	Αυθεντικοποίηση	
		Εξουσιοδότηση	
		Κρυπτογράφηση Μηνυμάτων	
Εγκυρότητα της πληροφορίας	Επίπεδο Μεταφοράς	Αυθεντικοποίηση Πελάτη-Υπηρεσίας	
		Έλεγχος ακεραιότητας μηνυμάτων	
	Επίπεδο Εφαρμογής	Αυθεντικοποίηση	
		Εξουσιοδότηση	
		Έλεγχος ακεραιότητας μηνυμάτων	
Διαθεσιμότητα της Υπηρεσίας	Αυθεντικοποίηση	Αυθεντικοποίηση	
		Εξουσιοδότηση	
		Έλεγχος του κώδικα που εκτελείται	
	Εγκυρότητα του λογισμικού της Υπηρεσίας	Αυθεντικοποίηση	
		Εξουσιοδότηση	
		Έλεγχος του κώδικα που εκτελείται	
Μη αποποίηση της ευθύνης	Ψηφιακή υπογραφή και καταγραφή συναλλαγών	✓ SSL (JSSE) ✓ Username or X.509 ✓ SSL (JSSE) ✓ Encryption Algorithm ✓ HTTP ✓ Form-based login ✓ SOAP-based authentication Role-based ✓ Declarative (deployment tool) ✓ Programmatic ✓ Encryption (JCE) ✓ XML encryption (JSR 106) ✓ SSL (JSSE) ✓ Username or X.509 ✓ SSL (JSSE) ✓ Hash function ✓ HTTP ✓ Form-based login ✓ SOAP-based authentication Role-based ✓ Declarative (deployment tool) ✓ Programmatic ✓ Hash Function-Dig. Signature (JCA) ✓ XML Dig. Sign. (JSR 105) ✓ HTTP ✓ Form-based login ✓ SOAP-based authentication Role-based (Programmatic) ✓ Code Access Security (JVM) ✓ Code Verification (JVM) ✓ HTTP ✓ Form-based login ✓ SOAP-based authentication Role-based ✓ Declarative (deployment tool) ✓ Programmatic ✓ Code Access Security (JVM) ✓ Code Verification (JVM) ✓ Digital Signatures (JCA) ✓ XML Dig. Sign. (JSR 105) ✓ Third Party	✓ SSL (JSSE) ✓ Username or X.509 ✓ SSL (JSSE) ✓ Encryption Algorithm ✓ HTTP ✓ Form-based login ✓ SOAP-based authentication Role-based ✓ Declarative (deployment tool) ✓ Programmatic ✓ Encryption (JCE) ✓ XML encryption (JSR 106) ✓ SSL (JSSE) ✓ Username or X.509 ✓ SSL (JSSE) ✓ Hash function ✓ HTTP ✓ Form-based login ✓ SOAP-based authentication Role-based (Programmatic) ✓ Code Access Security (JVM) ✓ Code Verification (JVM) ✓ HTTP ✓ Form-based login ✓ SOAP-based authentication Role-based ✓ Declarative (deployment tool) ✓ Programmatic ✓ Hash Function-Dig. Signature (JCA) ✓ XML Dig. Sign. (JSR 105) ✓ HTTP ✓ Form-based login ✓ SOAP-based authentication Role-based (Programmatic) ✓ Code Access Security (JVM) ✓ Code Verification (JVM) ✓ HTTP ✓ Form-based login ✓ SOAP-based authentication Role-based ✓ Declarative (deployment tool) ✓ Programmatic ✓ Code Access Security (JVM) ✓ Code Verification (JVM) ✓ Digital Signatures (JCA) ✓ XML Dig. Sign. (JSR 105) ✓ Third Party

Πίνακας 8.2.: Υλοποίηση των μηχανισμών ασφάλειας στις J2EE πλατφόρμες ανάπτυξης.

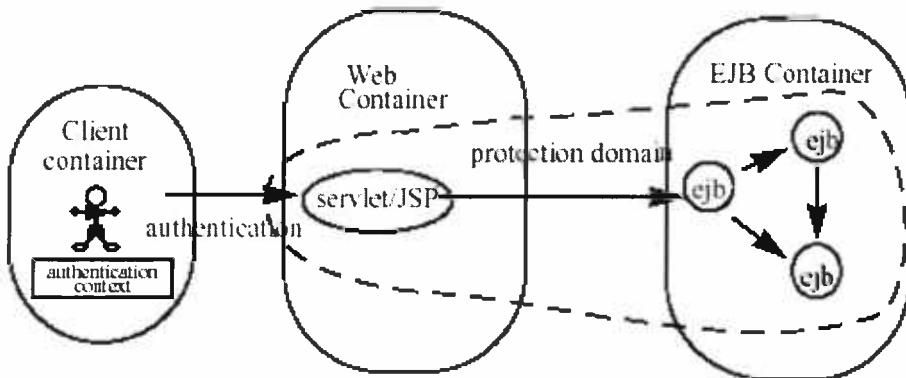


Οι παραπάνω μηχανισμοί ασφάλειας αναλύονται ξεχωριστά στη συνέχεια.

8.3.1. Αυθεντικοποίηση.

Η αυθεντικοποίηση στο J2EE είναι στενά συνδεδεμένη με την έννοια του protection domain [J2EE SEC]. Η αλληλεπίδραση δύο οντοτήτων που ανήκουν στο ίδιο protection domain, δεν προϋποθέτει την αυθεντικοποίηση της οντότητας που καλεί. Στην περίπτωση αυτή ο ισχυρισμός μιας ταυτότητας από την οντότητα που καλεί βασίζεται στην εμπιστοσύνη, και όχι στην αυθεντικοποίηση. Τα όρια ενός protection domain καθορίζονται για τα στοιχεία (components) από το container που τα φιλοξενεί. Ένα container έχει την ευθύνη να παρέχει σε κάθε στοιχείο που φιλοξενεί μια αυθεντική αναπαράσταση (διαπιστευτήριο) της ταυτότητας του στοιχείου που το καλεί (inbound calls), καθώς και να αποδεικνύει την ταυτότητα του στοιχείου που φιλοξενεί όταν αυτό πραγματοποιεί μια κλήση σε κάποιο άλλο στοιχείο (outbound calls), όταν τα στοιχεία ανήκουν σε διαφορετικά protection domains.

Στην περίπτωση που ένας πελάτης θέλει να χρησιμοποιήσει μια υπηρεσία, είναι απαραίτητο να προσκομισθεί ένα διαπιστευτήριο από το Client container στο Web container⁵⁴ της υπηρεσίας (σχήμα 8.3).



Σχήμα 8.3.: Αυθεντικοποίηση στο J2EE. [J2EE SEC]

Τα J2EE Web containers υποστηρίζουν σε επίπεδο μεταφοράς το πρωτόκολλο SSL για αμοιβαία αυθεντικοποίηση πελάτη-υπηρεσίας με χρήση X.509 πιστοποιητικών, μέσω της διεπαφής Java Secure Socket Extension (JSSE API).

⁵⁴ Στο Web container περιέχονται οι JSP σελίδες και τα Java Servlets (βλ. ενότητα 3.5)

Σε επίπεδο εφαρμογής, τα J2EE Web Containers υποστηρίζουν την αυθεντικοποίηση με μετάδοση συνθηματικού μέσω του πρωτοκόλλου HTTP, καθώς και το form-based login στην υπηρεσία. Ωστόσο και στις δύο περιπτώσεις δεν εξασφαλίζεται η εμπιστευτικότητα του συνθηματικού, με αποτέλεσμα και οι δυο μέθοδοι να μην αποτελούν την καλύτερη επιλογή. Τέλος, η SOAP-based αυθεντικοποίηση σαν δυνατότητα δεν έχει ενσωματωθεί στην πλατφόρμα J2EE, ωστόσο είναι έτοιμο από την IBM ένα σύνολο εργαλείων που αποτελεί υλοποίηση του WS-Security. Με το εργαλείο WSTK (Web Services Toolkit), το οποίο λειτουργεί ανεξαρτήτως λειτουργικού συστήματος με μόνη προϋπόθεση την υποστήριξη του SDK 1.3.1, είναι δυνατή η επισύναψη ενός πιστοποιητικού σε ένα SOAP μήνυμα. Με αυτόν τον τρόπο είναι δυνατή η αυθεντικοποίηση του πελάτη στην υπηρεσία.

8.3.2. Εξουσιοδότηση.

Οι προδιαγραφές του J2EE προτύπου καθορίζουν οργανωσιακούς ρόλους που είναι απαραίτητοι για την ανάθεση αρμοδιοτήτων σε φυσικά πρόσωπα, που ισχύουν καθ' όλη τη διάρκεια του κύκλου ζωής των εφαρμογών. Οι τρεις ρόλοι, που εμπλέκονται στη διαδικασία της εξουσιοδότησης, είναι ο ρόλος του Application Assembler, ο ρόλος του Deployer και ο ρόλος του Component Provider. Ο Application Assembler είναι υπεύθυνος για τον καθορισμό των δικαιωμάτων που συνδέονται με τις μεθόδους ενός αντικειμένου (method permissions) και τον καθορισμό προνομίων που αφορούν σε συγκεκριμένους ρόλους. Τα δικαιώματα μιας μεθόδου και τα προνόμια που έχει κάθε ρόλος, τα οποία αφορούν σε ένα αντικείμενο (EJB), δηλώνονται σε ένα XML αρχείο που ονομάζεται Deployment Descriptor. Η εξουσιοδότηση είναι ουσιαστικά η διαδικασία υιοθέτησης ενός ρόλου από ένα χρήστη, που νωρίτερα έχει αυθεντικοποιηθεί.

Η εξουσιοδότηση στις J2EE πλατφόρμες γίνεται είτε με δηλωτικό (declarative) είτε με προγραμματιστικό (programmatic) τρόπο [J2EE SEC]. Η δηλωτική εξουσιοδότηση, ονομάζεται και εξωτερική πολιτική ελέγχου πρόσβασης, είναι περισσότερο ευέλικτη και πραγματοποιείται από τον Deployer με χρήση εργαλείων (ονομάζονται declarative ή configuration tools). Η εξουσιοδότηση με προγραμματιστικό τρόπο, ονομάζεται και εσωτερική πολιτική ελέγχου πρόσβασης και είναι ενσωματωμένη στον κώδικα από τον Component Provider που τον έχει συντάξει. Το πρόβλημα στη δεύτερη περίπτωση είναι συνήθως ότι η πολιτική ελέγχου πρόσβασης είναι κατανοητή μόνο στους υπευθύνους ανάπτυξης.



8.3.3. Κρυπτογράφηση μηνυμάτων.

Οι J2EE πλατφόρμες υποστηρίζουν μέσω της JSSE διεπαφής το πρωτόκολλο επιπέδου μεταφοράς SSL για την κρυπτογράφηση της επικοινωνίας του πελάτη με την υπηρεσία. Υπηρεσίες κρυπτογράφησης σε επίπεδο εφαρμογής παρέχονται μέσω της διεπαφής Java Cryptography Extension. Το JCE API επιτρέπει τη δημιουργία και την ανταλλαγή κρυπτογραφικών κλειδιών, καθώς και την κρυπτογράφηση δεδομένων. Οι αλγόριθμοι που υποστηρίζει για την κρυπτογράφηση το JCE είναι: DES, RC4 (συμμετρικοί) και RSA, ElGamal (ασύμμετροι).

Η XML κρυπτογραφία πρόκειται να υποστηριχθεί σύντομα από το J2EE, με την υλοποίηση της προδιαγραφής JSR #106, η οποία και καθορίζει ένα σύνολο από διεπαφές για το σκοπό αυτό (XML Encryption Java APIs). Προς το παρόν μόνο η IBM έχει υλοποιήσει το σύνολο εργαλείων WSTK που επιτρέπει τη χρήση της XML κρυπτογραφίας σε J2EE εφαρμογές, καλύπτοντας έτσι την απαίτηση για end-to-end εμπιστευτικότητα των μηνυμάτων.

8.3.4. Έλεγχος ακεραιότητας των μηνυμάτων.

Εκτός από την υποστήριξη του πρωτοκόλλου SSL που επιτρέπει τον έλεγχο της ακεραιότητας των μηνυμάτων που ανταλλάσσονται σε μια σύνοδο με χρήση MACs, το J2EE υποστηρίζει και μηχανισμούς ελέγχου της ακεραιότητας των μηνυμάτων σε επίπεδο εφαρμογής. Η διεπαφή Java Cryptography Architecture υποστηρίζει τη δημιουργία και χρήση πιστοποιητικών, τη δημιουργία σύνοψης και κωδικών αυθεντικοποίησης για τα δεδομένα, καθώς και τη ψηφιακή υπογραφή των δεδομένων που ανταλλάσσονται. Οι αλγόριθμοι που υποστηρίζει το JCA είναι οι HMAC και hash MAC για τη δημιουργία κωδικών αυθεντικοποίησης μηνυμάτων (MACs), ο αλγόριθμος MD5 για τη δημιουργία σύνοψης των δεδομένων και οι αλγόριθμοι DSA και RSA (μαζί με τον MD5) για τη δημιουργία της ψηφιακής υπογραφής.

Με την υλοποίηση της προδιαγραφής JSR #105 το J2EE πρόκειται να παρέχει και τη δυνατότητα χρησιμοποίησης XML ψηφιακών υπογραφών, υποστηρίζοντας έτσι τον έλεγχο της ακεραιότητας ενός μηνύματος στην περίπτωση που η διαδρομή του από τον αποστολέα μέχρι την υπηρεσία περιλαμβάνει ενδιάμεσες οντότητες, που πιθανόν να τροποποιούν κάποια τμήματα του. Προς το παρόν, είναι διαθέσιμο μόνο το σύνολο εργαλείων WSTK της IBM.



8.3.5. Έλεγχος του κώδικα που εκτελείται.

Όπως είναι γνωστό, η Java επιτρέπει τη μεταφορά εκτελέσιμου περιεχομένου και την εκτέλεσή του σε οποιαδήποτε αρχιτεκτονική και λειτουργικό σύστημα έχει υλοποιηθεί η ιδεατή μηχανή Java (JVM). Οι περισσότεροι εξυπηρετητές υποστηρίζουν την μεταφορά και εκτέλεση προγραμμάτων Java μέσα από το διαδίκτυο με τη χρήση της ετικέτας applet της HTML. Τέτοια προγράμματα περιέχουν μη έμπιστο (untrusted) κώδικα. Για την προστασία του συστήματος ο μη έμπιστος κώδικας στο J2EE ελέγχεται ως προς την ορθότητά του και εκτελείται σε ένα περιβάλλον περιορισμένων δυνατοτήτων, το σκάμμα (sandbox). Το σκάμμα διασφαλίζει ότι ο μη έμπιστος κώδικας εκτελείται μόνο σε συγκεκριμένη περιοχή της Java πλατφόρμας και έχει πρόσβαση μόνο σε ένα περιορισμένο σύνολο πόρων. Υλοποιείται από την JVM και τον ελεγκτή κλάσεων (class verifier) αυτής, τους φορτωτές κλάσεων (class loaders) και την οντότητα Security Manager [Mulcahy, 2002].

Ο δυναμικός τρόπος με τον οποίο η JVM δεσμεύει τις διάφορες περιοχές μνήμης καθιστά σχεδόν αδύνατο για έναν εν δυνάμει επιτιθέμενο να αποφασίσει σε ποιες περιοχές μνήμης να προσπαθήσει να παρεμβάλει κακόβουλες (malicious) εντολές. Επίσης, ο έλεγχος των ορίων στους πίνακες από την JVM αποτρέπει κάθε πρόσβαση χωρίς αναφορά στην μνήμη. Ο ελεγκτής κλάσεων (class verifier) καλείται να εξασφαλίσει ότι ο κώδικας, ο οποίος μπορεί να έχει δημιουργηθεί από ένα μεταγλωττιστή της Java ή από έναν εχθρικό (hostile) μεταγλωττιστή, πληροί ορισμένους κανόνες. Οι μόνες κλάσεις που δεν ελέγχονται είναι οι βασικές κλάσεις (base class). Όλες οι άλλες κλάσεις, συμπεριλαμβανομένων και εκείνων που φορτώνονται από το classpath της εφαρμογής θεωρούνται μη έμπιστες και ελέγχονται.

Οι φορτωτές κλάσεων έχουν ευθύνη να εντοπίσουν τις κλάσεις που έχουν ζητηθεί από το JVM για τη φόρτωση τους στο περιβάλλον χρόνου εκτέλεσης. Επίσης, μέρος της ευθύνης τους είναι να εμποδίσουν την αντικατάσταση του έμπιστου κώδικα, που αποτελεί τις βασικές κλάσεις, από μη εξουσιοδοτημένα ή μη έμπιστα τμήματα κώδικα. Η απόπειρα αντικατάστασης μιας βασικής κλάσης από μια κωδικοποιημένη με κακόβουλη πρόθεση κλάση είναι γνωστή ως class spoofing.

Τέλος, η οντότητα Security Manager διενεργεί ελέγχους κατά το χρόνο εκτέλεσης σε ενέργειες που μπορεί να είναι μη ασφαλείς (βάση κάποιας υπόθεσης). Ο Security manager περιλαμβάνει για κάθε ενέργεια που υποθετικά θεωρείται μη ασφαλής, μια μέθοδο που καθορίζει αν η ενέργεια επιτρέπεται ή όχι από το σκάμμα. Με τον τρόπο αυτό δεν εκτελείται καμία ενέργεια που να μην επιτρέπεται από την πολιτική ασφαλείας.



8.3.6. Ψηφιακή υπογραφή και καταγραφή συναλλαγών.

Οι J2EE πλατφόρμες παρέχουν μέσω της JCA διεπαφής τη δυνατότητα στους developers να χρησιμοποιήσουν υπηρεσίες ψηφιακών υπογραφών στις εφαρμογές τους. Το JCA βέβαια δεν υποστηρίζει τις XML ψηφιακές υπογραφές, ωστόσο σύντομα πρόκειται να υλοποιηθούν οι προδιαγραφές που ορίζει το JSR #105.

Οι ψηφιακές υπογραφές είναι η βασική τεχνολογία που υποστηρίζει την παροχή υπηρεσιών μη αποποίησης. Η ψηφιακή υπογραφή ενός μηνύματος από τον ίδιο τον πελάτη και εν συνεχείᾳ την αποθήκευση του σε ένα tamper-proof αρχείο καταγραφών (audit trail) μπορεί να χρησιμοποιηθεί, όπως αναφέρθηκε και στην περίπτωση του .NET, ως μηχανισμός για την εξασφάλιση της μη αποποίησης της ευθύνης του πελάτη μιας υπηρεσίας. Σε κάθε περίπτωση ωστόσο, η μη αποποίηση της ευθύνης και του πελάτη και της υπηρεσίας, μπορεί να επιτευχθεί μόνο με τη διαμεσολάβηση μιας έμπιστης τρίτης οντότητας που θα παρέχει υπηρεσίες μη αποποίησης.

8.4. Σύγκριση των δύο πλατφόρμων.

Οι πλατφόρμες .NET και J2EE παρέχουν παρόμοιες υπηρεσίες ασφάλειας, χωρίς ωστόσο να ακολουθούν την ίδια φιλοσοφία. Στο Microsoft .NET η αυθεντικοποίηση και η εξουσιοδότηση είναι υπηρεσίες που παρέχονται μέσω των λειτουργικών συστημάτων Microsoft Windows. Επίσης, υπάρχει εξάρτηση από τις αποθήκες αναγνωριστικών (identification stores) που παρέχει η ίδια η Microsoft, όπως είναι το .NET Passport και τα Windows domains. Αντίθετα, το J2EE δεν προσδιορίζει ποιες μέθοδοι ή ποιες αποθήκες αναγνωριστικών πρέπει να χρησιμοποιηθούν για την υλοποίηση του ελέγχου πρόσβασης, αφήνοντας αυτές τις αποφάσεις στους προμηθευτές και τους υπεύθυνους της ανάπτυξης των εφαρμογών. Για παράδειγμα, η Sun παρέχει την υπηρεσία JAAS (Java Authentication and Authorization Service), εντούτοις η χρήση της στο J2EE είναι προαιρετική. Το ίδιο ισχύει και για το Project Liberty, το οποίο είναι μια υπηρεσία που επιτρέπει την αυθεντικοποίηση και την εξουσιοδότηση ενός πελάτη παρέχοντας μοναδικό σημείο πρόσβασης (single sign on) και έχει μέλη της την Sun και άλλες εταιρείες όπως την AOL, τη Vodafone, την American Express, την HP και την RSA.

Κοινό στοιχείο και στις δύο πλατφόρμες ανάπτυξης, είναι ότι χρησιμοποιούν παρόμοιες μεθόδους για τη διαχείριση της πρόσβασης των χρηστών και του κώδικα στα στοιχεία



(components). Και στις δύο πλατφόρμες οι έννοιες δικαιώμα (permission) και ρόλος είναι οι δύο έννοιες κλειδιά, και η βάση της role-based πολιτικής ελέγχου πρόσβασης. Μια διαφορά, βέβαια είναι ότι στο J2EE χρησιμοποιείται επίσης η έννοια των οργανωσιακών ρόλων για την ανάθεση ευθυνών σε φυσικά πρόσωπα (καθορίζοντας έτσι και μια ιεραρχία), πράγμα που δεν καθορίζεται σαφώς στο .NET.

Σε ότι αφορά τα πρωτόκολλα ασφαλείας του επιπέδου μεταφοράς και οι δύο πλατφόρμες υποστηρίζουν τους μηχανισμούς του Secure Socket Layer για την αυθεντικοποίηση πελάτη-υπηρεσίας και για την προστασία των δεδομένων που μεταδίδονται. Σε επίπεδο εφαρμογής, οι SOAP-based μηχανισμοί ασφάλειας δεν έχουν υλοποιηθεί για το J2EE (είναι έτοιμες απλά οι προδιαγραφές τους), ενώ αντίθετα είναι έτοιμοι για το .NET, έστω και αν δεν έχουν δοκιμαστεί αρκετά.

Τέλος, στον τομέα του ελέγχου του κώδικα, οι λειτουργίες επαλήθευσης του κώδικα στη JVM μηχανή είναι αρκετά ώριμες και έχουν αποφευχθεί τα λάθη που είχαν γίνει στο παρελθόν. Το μοντέλο του CLR αντίθετα, αν και είναι σε πολλά σημεία παρόμοιο, είναι μη δοκιμασμένο.

8.5. Συμπέρασμα.

Οι πλατφόρμες ανάπτυξης .NET και J2EE παρέχουν υπηρεσίες ασφάλειας που μπορούν να αξιοποιηθούν από τους υπεύθυνους ανάπτυξης και διαχείρισης των υπηρεσιών διαδικτύου, εντούτοις υπάρχουν ακόμα σημαντικές ελλείψεις. Η αντιμετώπιση του ζητήματος της ασφάλειας, παρά το γεγονός ότι φαίνεται να είναι επιτακτική ανάγκη για την ανάπτυξη των υπηρεσιών διαδικτύου, εισάγει νέες απαιτήσεις για διαλειτουργικότητα. Η πλατφόρμα .NET εισάγει στους χρήστες των υπηρεσιών περιορισμούς που σχετίζονται με την υποστήριξη συγκεκριμένου λειτουργικού συστήματος, ακόμα και συγκεκριμένου browser. Οι πλατφόρμες J2EE δεν εισάγουν τέτοιους περιορισμούς, ωστόσο βρίσκονται ένα βήμα πιο πίσω στην υλοποίηση των SOAP-based μηχανισμών ασφάλειας. Επίσης, παρά το γεγονός ότι η κρυπτογραφία είναι το κλειδί στην υλοποίηση των περισσότερων μηχανισμών ασφάλειας, το πρόβλημα της διαχείρισης των κλειδιών παραμένει. Είναι οπωσδήποτε ιδιαίτερα σημαντικό, και για τις δύο πλατφόρμες, να υλοποιηθούν υπηρεσίες διαχείρισης κλειδιών με βάση το XKMS πρότυπο, ώστε να μπορούν να χρησιμοποιηθούν από τις υπηρεσίες διαδικτύου. Τέλος, είναι απαραίτητη και η δημιουργία SOAP υπηρεσιών αυθεντικοποίησης και εξουσιοδότησης



με βάση τα πρότυπα SAML και XACML, οι οποίες θα μπορούν να παρέχονται από τρίτες οντότητες.



ΚΕΦΑΛΑΙΟ 9^ο: ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΑΝΟΙΚΤΑ ΘΕΜΑΤΑ

9.1. Σύνοψη.

Τα ζητήματα που αφορούν στην ασφάλεια των υπηρεσιών διαδικτύου έχουν συγκεντρώσει το ενδιαφέρον ενός μεγάλου μέρους της επιστημονικής κοινότητας, των επιχειρήσεων, καθώς και των εταιρειών που παρέχουν υποδομή για την ανάπτυξη εφαρμογών στο διαδίκτυο. Η έρευνα που έχει πραγματοποιηθεί μέχρι σήμερα έχει προσφέρει ένα σημαντικό σύνολο θεωρητικής και πρακτικής γνώσης, που αφορά στην αξιοποίηση υφιστάμενων τεχνολογιών, αλλά και στην ανάπτυξη αρκετών νέων.

Η παρούσα εργασία αποτελεί μια προσπάθεια να διερευνηθεί το ζήτημα της ασφάλειας στις υπηρεσίες διαδικτύου, να περιγραφεί και να αξιολογηθεί η παρούσα κατάσταση, και να εντοπιστούν τα ζητήματα που θα απασχολήσουν πιθανότατα στο μέλλον τους ερευνητές.

Στα προηγούμενα κεφάλαια, παρουσιάστηκαν οι υπηρεσίες διαδικτύου, έγινε αναφορά στην αιτία που οδήγησε στην εμφάνιση τους, περιγράφηκαν οι τεχνολογίες και τα πρότυπα που τις υποστηρίζουν και εξετάστηκαν τα μοντέλα ανάπτυξης που υπάρχουν. Στη συνέχεια, αναφέρθηκαν οι ιδιότητες που ορίζουν την έννοια της ασφάλειας των υπηρεσιών και εντοπίστηκαν και αναλύθηκαν οι απαιτήσεις ασφάλειας που σχετίζονται με το περιβάλλον των υπηρεσιών διαδικτύου και τις ιδιαιτερότητες που το χαρακτηρίζουν.

Με βάση τις απαιτήσεις ασφάλειας διαμορφώθηκε ένα πλαίσιο ασφαλείας για την καταγραφή και αξιολόγηση των μηχανισμών, και κατ' επέκταση των πρωτοκόλλων και των πρότυπων ασφαλείας, που υπάρχουν ή είναι υπό κατασκευή και δύνανται να χρησιμοποιηθούν. Για κάθε τεχνολογία εξετάστηκαν τα πλεονεκτήματα και τα μειονεκτήματα, που την καθιστούν αποτελεσματική ή όχι στην κάλυψη των συγκεκριμένων απαιτήσεων.

Στη συνέχεια αφού υπογραμμίστηκε η ανάγκη ύπαρξης ενός μοντέλου που θα μπορέσει να ενοποιήσει τις υπάρχουσες λύσεις για την ασφάλεια των υπηρεσιών διαδικτύου, έχοντας βασικό στόχο τον καθορισμό μιας στρατηγικής για την ασφάλεια, ακολούθησε η περιγραφή και η κριτική ενός μοντέλου ασφαλείας για τις υπηρεσίες διαδικτύου, το οποίο βρίσκεται υπό ανάπτυξη και αποτελεί πρόταση των εταιρειών IBM και Microsoft.

Τέλος, καταγράφηκαν και αξιολογήθηκαν, με βάση το πλαίσιο των απαιτήσεων ασφαλείας, οι υπηρεσίες ασφάλειας που παρέχονται στους χορηγούς και στους πελάτες των



υπηρεσιών διαδικτύου από τις πλατφόρμες ανάπτυξης Microsoft .NET και Java 2 Enterprise Edition.

9.2. Συμπεράσματα.

Τα βασικά συμπεράσματα που προκύπτουν από την παρούσα εργασία και αφορούν στην ασφάλεια των υπηρεσιών διαδικτύου είναι τα παρακάτω:

- Για την αντιμετώπιση του ζητήματος της ασφάλειας σε έναν οργανισμό που παρέχει κάποια υπηρεσία διαδικτύου, είναι απαραίτητη η ύπαρξη μιας πολιτικής ασφαλείας, που θα είναι διαθέσιμη και στον πελάτη. Στο μοντέλο των υπηρεσιών διαδικτύου αυτό προϋποθέτει τη δημιουργία ενός XML σχήματος, με τα χαρακτηριστικά μιας γλώσσας περιγραφής πολιτικών ασφαλείας, για τη σύνταξη μιας πολιτικής σε γλώσσα XML. Με την ενσωμάτωση της στο WSDL έγγραφο, η πολιτική ασφαλείας θα μπορεί να ανακαλύπτεται από μια υπηρεσία καταλόγου, μαζί με την περιγραφή μιας υπηρεσίας.
- Η σύγκρουση των πολιτικών ασφαλείας δύο υπηρεσιών που ανήκουν σε διαφορετικά πεδία εφαρμογής πολιτικών ασφαλείας (policy domains), επιλύεται μέσω της διαπραγμάτευσης (negotiation). Στη διαδικασία της διαπραγμάτευσης οι δύο πλευρές έρχονται σε επικοινωνία και συνήθως προτείνουν κάποιες εναλλακτικές πολιτικές ασφαλείας. Με δεδομένη την απουσία κάποιου τρόπου επίλυσης των συγκρούσεων των πολιτικών ασφαλείας μεταξύ δύο υπηρεσιών διαδικτύου, μια πρόταση θα μπορούσε να περιλαμβάνει: α) τη διατύπωση των πολιτικών ασφαλείας και κάποιας μεταπολιτικής σε γλώσσα XML, και β) την ανάθεση του ρόλου του πολιτικού διαμεσολαβητή σε μια υπηρεσία διαδικτύου.
- Οι βασικές απαιτήσεις ασφάλειας στο μοντέλο των υπηρεσιών διαδικτύου είναι α) η εξασφάλιση της εμπιστευτικότητας, της αυθεντικότητας και της ακεραιότητα της πληροφορίας που ανταλλάσσεται μέσω των SOAP μηνυμάτων ή είναι αποθηκευμένη σε καταλόγους με τη μορφή WSDL εγγράφων, β) η εξασφάλιση της διαθεσιμότητας των υπηρεσιών, γ) η εξασφάλιση της εγκυρότητας και εμπιστευτικότητας του λογισμικού των υπηρεσιών, και δ) η εξασφάλιση της μη αποποίησης της ευθύνης της οντότητας πελάτη και της οντότητας χορηγού της υπηρεσίας.
- Οι μηχανισμοί ασφάλειας που στηρίζονται σε υπάρχουσες τεχνολογίες των επιπέδων μεταφοράς και διαδικτύου δεν μπορούν σε αρκετές περιπτώσεις να παρέχουν λύσεις για την ασφάλεια των υπηρεσιών διαδικτύου, όπως το επιτυγχάνουν στις παραδοσιακές

- υπηρεσίες client-server. Οι τεχνολογίες ασφαλείας σε επίπεδο διαδικτύου δεν προσφέρονται από τεχνικής άποψης και επιπλέον δεν παρέχουν επαρκή υποστήριξη για την υλοποίηση μιας πολιτικής ασφαλείας σε επίπεδο διαδικτύου. Οι τεχνολογίες ασφαλείας σε επίπεδο μεταφοράς παρέχουν ασφάλεια σε μια σύνδεση, εξασφαλίζοντας: α) την αυθεντικοποίηση των οντοτήτων στα άκρα μιας σύνδεσης, β) την εμπιστευτικότητα των πληροφοριών κατά τη μεταφορά τους από το ένα άκρο της σύνδεσης στο άλλο, και γ) την ακεραιότητα των πληροφοριών κατά τη μεταφορά τους από το ένα άκρο της σύνδεσης στο άλλο. Ωστόσο, δεν επιτυγχάνεται η εξασφάλιση της μη αποποίησης της ευθύνης, δεν υποστηρίζονται μηχανισμοί εξουσιοδότησης και κυρίως δεν εξασφαλίζεται η επικοινωνία πελάτη-υπηρεσίας από άκρη σε άκρη (end-to-end).
- Οι ιδιαιτερότητες που υπάρχουν, κυρίως στη δομή μιας τοπολογίας από συνεργαζόμενες υπηρεσίες διαδικτύου, υποδεικνύουν την αντιμετώπιση των περισσότερων ζητημάτων ασφάλειας σε επίπεδο εφαρμογής. Σε επίπεδο εφαρμογής υποστηρίζονται οι μηχανισμοί: α) αυθεντικοποίησης του πελάτη και της υπηρεσίας, β) εξουσιοδότησης του πελάτη, γ) κρυπτογράφησης των XML μηνυμάτων, δ) ελέγχου ακεραιότητας των XML μηνυμάτων στον παραλήπτη, ε) ανίχνευσης περιστατικών και παραβιάσεων, και στ) αποθήκευσης και προώθησης των μηνυμάτων από υπηρεσίες μη αποποίησης.
 - Οι μηχανισμοί ασφάλειας του επιπέδου εφαρμογής, στηρίζονται στα πρότυπα XML ENC, XML DS, XKMS, SAML και XACML. Τα πρότυπα XML ENC και XML DS επεκτείνουν τις δυνατότητες των τεχνολογιών κρυπτογράφησης και ψηφιακής υπογραφής, επιτρέποντας την εφαρμογή των μηχανισμών κρυπτογράφησης και ψηφιακής υπογραφής: α) σε ολόκληρο το XML μήνυμα, β) σε τμήμα του XML μηνύματος, που περιλαμβάνει πληροφορία, η οποία σχετίζεται με κάποια συγκεκριμένη οντότητα που προωθεί το μήνυμα και απευθύνεται σε παραλήπτες που ορίζονται από αυτή. Το πρότυπο XKMS καθορίζει ένα τρόπο κλήσης διαδικασιών διαχείρισης δημοσίου κλειδιού, μέσω XML μηνυμάτων. Τέλος, τα πρότυπα SAML και XACML υποστηρίζουν από κοινού τη διαδικασία εξουσιοδότησης του τελικού χρήστη σε μια υπηρεσία διαδικτύου, με βάση την πολιτική ασφαλείας, επιτρέποντας επίσης και την ανταλλαγή διαβεβαιώσεων ασφαλείας μεταξύ των υπηρεσιών.
 - Το μοντέλο ασφαλείας που προτείνουν οι εταιρείες IBM και Microsoft, όπως έχει σχεδιαστεί, δύναται να αποτελέσει ένα γενικό πλαίσιο ασφάλειας που θα ικανοποιεί τις κύριες απαιτήσεις ασφάλειας των υπηρεσιών διαδικτύου. Ωστόσο, πολλές προδιαγραφές βρίσκονται ακόμα σε αρχικό στάδιο ανάπτυξης. Το σημαντικότερο είναι ότι δεν έχει καθοριστεί το μοντέλο εμπιστοσύνης, που πρόκειται να υιοθετηθεί και κυρίως ο τρόπος

με τον οποίο θα αντιμετωπιστούν ορισμένα ζητήματα που αποτέλεσαν τις αδυναμίες μοντέλων όπως το PKI. Επίσης, δεν έχει διασαφηνιστεί αν το μοντέλο θα υποστηρίζει μοναδικό σημείο πρόσβασης για πολλές υπηρεσίες.

- Η αντιμετώπιση του ζητήματος της ασφάλειας, εισάγει νέες απαιτήσεις για διαλειτουργικότητα. Οι πλατφόρμες ανάπτυξης .NET και J2EE παρέχουν υπηρεσίες ασφάλειας που μπορούν να αξιοποιηθούν από τους υπεύθυνους ανάπτυξης και διαχείρισης των υπηρεσιών διαδικτύου, εντούτοις υπάρχουν ακόμα ελλείψεις. Το .NET εισάγει αρκετούς περιορισμούς στους χρήστες από άποψη διαλειτουργικότητας, ενώ οι πλατφόρμες J2EE βρίσκονται πίσω στην υλοποίηση των SOAP-based μηχανισμών ασφάλειας. Επίσης, είναι απαραίτητο και για τις δύο πλατφόρμες, να υλοποιηθούν υπηρεσίες διαχείρισης κλειδιών με βάση το XKMS πρότυπο και να δημιουργηθούν SOAP υπηρεσίες αυθεντικοποίησης και εξουσιοδότησης με βάση τα πρότυπα SAML και XACML.

9.3. Συμβολή της εργασίας - Ανοικτά θέματα.

Όπως αναφέρθηκε στην ενότητα 1.8. η κύρια συνεισφορά της παρούσας διατριβής συνίσταται:

- Στη διαμόρφωση ενός πλαισίου, που περιλαμβάνει τις απαιτήσεις ασφάλειας, για την περιγραφή και την αξιολόγηση των μηχανισμών, των τεχνολογιών και των μοντέλων ασφαλείας.
- Στην περιγραφή ανοικτών ερευνητικών ζητημάτων που προκύπτουν.

Ο πρώτος τομέας συνεισφοράς της εργασίας αναδείχτηκε μέσα από τα προηγούμενα κεφάλαια, επομένως αυτό που απομένει στον επίλογο της παρούσας εργασίας είναι να περιγραφούν τα ανοικτά ερευνητικά ζητήματα.

Γενικά, η παρούσα εργασία μπορεί να αποτελέσει αφετηρία για περαιτέρω έρευνα στο μέλλον. Ορισμένα από τα ανοικτά θέματα που αφορούν στην ασφάλεια των υπηρεσιών διαδικτύου και παρουσιάζουν ιδιαίτερο ενδιαφέρον είναι τα παρακάτω.

9.3.1. Διαχείριση πολιτικών ασφαλείας στο περιβάλλον των υπηρεσιών διαδικτύου.

Σε ότι αφορά τις υπηρεσίες διαδικτύου, η διαχείριση των πολιτικών ασφαλείας αποτελεί ζήτημα που έχει ιδιαίτερη σημασία σε δύο περιπτώσεις. Η πρώτη περίπτωση περιλαμβάνει



εκείνα τα σενάρια στα οποία δύο ανεξάρτητοι οργανισμοί έχουν υλοποιήσει υπηρεσίες διαδικτύου, οι οποίες αλληλεπιδρούν ανταλλάσσοντας πληροφορίες και διασυνδέοντας τα πληροφοριακά τους συστήματα. Η δεύτερη περίπτωση αφορά στα σενάρια εκείνα στα οποία ένας ιδεατός οργανισμός διατηρεί υπηρεσίες διαδικτύου που ανήκουν σε ανεξάρτητες διοικητικές οντότητες, λειτουργούν σε αυτόνομα πληροφοριακά συστήματα, αλλά καλούνται να συνεργαστούν αποτελεσματικά μεταξύ τους. Στις παραπάνω περιπτώσεις, επειδή τα συνεργαζόμενα πληροφοριακά συστήματα έχουν τη δική τους πολιτική ασφαλείας, η αποτελεσματικότητα της συνεργασίας τους εξαρτάται σημαντικά από το βαθμό συμβατότητας των πολιτικών τους [Κοκολάκης, 2000].

Γενικά, τα προβλήματα συνεργασίας που προκύπτουν από ασυμβατότητες και συγκρούσεις πολιτικών ασφαλείας, αποτελούν προβλήματα διαλειτουργικότητας και απαιτούν την αποτελεσματική διαχείριση των πολιτικών ασφαλείας. Η ανάπτυξη ενός εργαλείου που θα αυτοματοποιεί πλήρως τη διαδικασία διαχείρισης των πολιτικών ασφαλείας σύμφωνα με τον Κοκολάκη δεν θα πρέπει να θεωρείται εφικτή, αφού η ερμηνεία και η κατανόηση των πολιτικών απαιτεί τη συμβολή της ανθρώπινης νοημοσύνης και η σύγκλιση των πολιτικών απαιτεί μια πολιτική διαπραγμάτευσης. Το μόνο που μπορεί να επιτευχθεί είναι η ανάπτυξη ενός εργαλείου που θα υποστηρίζει το ανθρώπινο δυναμικό ενός πληροφοριακού συστήματος στη διαχείριση των πολιτικών.

Για την αντιμετώπιση των προβλημάτων διαλειτουργικότητας που προκύπτουν από την υιοθέτηση πολλαπλών πολιτικών ασφαλείας, ο Κοκολάκης προτείνει α) ένα μεθοδολογικό πλαίσιο, το οποίο ονομάζει Σύστημα Ανάπτυξης Μεταπολιτικών (Σ.Α.Μ.) και β) ένα Σύστημα Διαχείρισης Πολιτικών Ασφαλείας (Σ.Δ.Π.Α.), το οποίο μπορεί να υποστηρίξει το ανθρώπινο δυναμικό των πληροφοριακών συστημάτων στην εφαρμογή του Σ.Α.Μ. [Κοκολάκης, 2000].

Με τη μεταφορά των παραπάνω προτάσεων στο περιβάλλον των υπηρεσιών διαδικτύου, προκύπτει ένα ανοικτό ερευνητικό ζήτημα που αφορά στην κατασκευή ενός Συστήματος Διαχείρισης Πολιτικών Ασφαλείας για τις υπηρεσίες αυτές, που θα έχει σαν στόχο:

1. Την καταγραφή των πολιτικών και των μεταπολιτικών ασφαλείας με τη βοήθεια ενός XML σχήματος που θα επιτρέπει τη σύγκριση και την επεξεργασία τους.
2. Την υποστήριξη της διαχείρισης των πολιτικών και των μεταπολιτικών.
3. Την υποστήριξη της προσπάθειας αντιμετώπισης των προβλημάτων που προκύπτουν από την ασυμβατότητα των πολιτικών ασφαλείας.

Η πρόκληση της κατασκευής ενός τέτοιου συστήματος είναι μεγάλη. Ιδιαίτερα σε ότι αφορά τον τελευταίο στόχο του, το έργο ενός ΣΔΠΑ φαντάζει ιδιαίτερα σύνθετο,

αναλογιστεί κανείς ότι στο μοντέλο των υπηρεσιών διαδικτύου η ανακάλυψη και η δέσμευση μιας υπηρεσίας από μια άλλη μπορεί να γίνει με δυναμικό τρόπο.

9.3.2. Αναζήτηση μοντέλου εμπιστοσύνης για τις υπηρεσίες διαχείρισης κλειδιών.

Η ασφαλής μετάδοση μηνυμάτων μεταξύ ενός πελάτη και μιας υπηρεσίας διαδικτύου, όπως έγινε φανερό στα προηγούμενα κεφάλαια, στηρίζεται σε μεγάλο βαθμό στην XML κρυπτογραφία και τις XML ψηφιακές υπογραφές. Για την αξιοποίηση των τεχνολογιών αυτών υπογραμμίστηκε στην παρούσα εργασία⁵⁵ η ανάγκη για σωστή, αποδοτική, επεκτάσιμη και ασφαλή διαχείριση των κρυπτογραφικών κλειδιών.

Οι XML υπηρεσίες διαχείρισης κλειδιών είναι υπηρεσίες διαδικτύου που υποστηρίζουν τη δημιουργία ζεύγους κλειδιών και τη διατήρηση ενός καταλόγου δημοσίων κλειδιών. Περιλαμβάνουν διαδικασίες ενημέρωσης και ανάκτησης και των κλειδιών, διαδικασίες ανάκαμψης των κλειδιών σε περιπτώσεις απώλειας ή διακύβευσης της ασφάλειάς τους, καθώς και διαδικασίες που αναλαμβάνονται σε περίπτωση διακύβευσης της ασφάλειας του κλειδιού και αφορούν σε μηχανισμούς αποδοχής, επιβεβαίωσης και αναφοράς της διακύβευσης.

Το πρότυπο XKMS καθορίζει τη μορφή που πρέπει να έχουν τα XML μηνύματα, μέσω των οποίων μια υπηρεσία διαδικτύου μπορεί να καταχωρίσει, να ανακαλέσει, να εντοπίσει, και να ενημερώσει πληροφορίες δημοσίου κλειδιού σε μια XML υπηρεσία διαχείρισης κλειδιών και εξασφαλίζει ότι ικανοποιούνται συγκεκριμένες απαιτήσεις ασφάλειας. Επίσης, καθορίζει προδιαγραφές που υποστηρίζουν τις διαδικασίες καταχώρισης και διαχείρισης της πληροφορίας που σχετίζεται με τα δημόσια κλειδιά. Στην πράξη ωστόσο, οι δυνατότητες αυτές δεν είναι αρκετές. Με δεδομένη την παγκόσμια εμβέλεια των υπηρεσιών διαδικτύου και τη δυνατότητα για δυναμική δέσμευση τους, είναι ρητή η ανάγκη ύπαρξης υπηρεσιών διαχείρισης κλειδιών, που να συνεργάζονται μεταξύ τους. Το γεγονός αυτό προϋποθέτει την ύπαρξη ενός μοντέλου εμπιστοσύνης, στο οποίο θα στηρίζεται η συνεργασία. Συνεπώς, σε ότι αφορά τον τρόπο με τον οποίο θα είναι δυνατή η ύπαρξη εμπιστοσύνης μεταξύ των οντοτήτων που θα παρέχουν τις XKMS υπηρεσίες η απουσία ενός μοντέλου, αποτελεί σημαντική έλλειψη.

Το γεγονός αυτό καθιστά την διερεύνηση του κατάλληλου μοντέλου εμπιστοσύνης, που θα υποστηρίζει τις XKMS υπηρεσίες, ένα σημαντικό ανοικτό ερευνητικό ζήτημα. Στο

⁵⁵ βλ. ενότητα 6.4.4



πλαίσιο αυτού του ζητήματος θα πρέπει να γίνει διερεύνηση των μοντέλων εμπιστοσύνης που υπάρχουν (ιεραρχικό, μοντέλο προσανατολισμένου γράφου, μοντέλο που στηρίζεται στη χρήση αντίστροφων πιστοποιητικών κ.τ.λ.), να ακολουθήσει η συγκριτική ανάλυση τους και να αξιολογηθούν τα στοιχεία εκείνα που τα καθιστούν κατάλληλα ή μη για την υποστήριξη των XKMS υπηρεσιών. Στην περίπτωση που θα αποδειχτεί ότι κανένα από τα μοντέλα που υπάρχουν δεν επαρκεί, σκοπός της έρευνας θα πρέπει να είναι η ανάπτυξη κάτι καινούργιου.

9.3.3. Παρακολούθηση των συμφωνιών που κλείνονται σε επίπεδο υπηρεσίας.

Μια συμφωνία σε επίπεδο υπηρεσίας (SLA-Service Level Agreement) είναι ένα συμβόλαιο μεταξύ του χορηγού μιας υπηρεσίας και ενός πελάτη, που εγγυάται κάποια χαρακτηριστικά της συναλλαγής που είναι ποσοτικά μετρήσιμα. Η παρακολούθηση (monitoring) μιας συμφωνίας θα πρέπει να παρέχει προστασία από επιπτώσεις ενεργειών μη-συμμόρφωσης (non-compliance). Επίσης, θα πρέπει να καθορίζει την εκτέλεση ενεργειών και την ενημέρωση του χρήστη και της υπηρεσίας σε κάθε περίπτωση μη-συμμόρφωσης.

Ένα ζήτημα με έντονο ερευνητικό ενδιαφέρον αφορά στην υλοποίηση ενός συστήματος για την παρακολούθηση των συμφωνιών μεταξύ ενός πελάτη και μιας υπηρεσίας διαδικτύου. Η υλοποίηση ενός τέτοιου συστήματος μπορεί να περιλαμβάνει:

- α) την ανάπτυξη και παροχή, από μια έμπιστη τρίτη οντότητα, μιας υπηρεσίας που θα υποστηρίζει τις διαδικασίες της παρακολούθησης της συμφωνίας (Contract Monitoring), της ενημέρωσης των δύο πλευρών (Contract Notifying) και της επιβολής των συμφωνηθέντων (Contract Enforcing).
- β) την κατασκευή ενός XML σχήματος για την περιγραφή μιας συμφωνίας.
- γ) τη διατήρηση μιας βάσης δεδομένων (Contract Database) για τη φύλαξη των συμφωνιών που έχουν πραγματοποιηθεί και έχουν υπογραφεί από τις οντότητες που εμπλέκονται. Μολονότι φαίνεται φυσικό ο χορηγός μιας υπηρεσίας να διατηρεί τη βάση με τις συμφωνίες που έχει κλείσει με τους πελάτες του, το προτιμότερο είναι οι συμφωνίες που κλείνονται να τίθενται υπό την κατοχή της έμπιστης τρίτης οντότητας που θα παίξει τον ρόλο του επόπτη της συμφωνίας.

Τα παραπάνω γίνονται πιο κατανοητά στο παράδειγμα που ακολουθεί. Έστω ότι βάσει του συμβολαίου μεταξύ ενός πελάτη και μιας υπηρεσίας καθορίζεται για ένα ποσοτικά μετρήσιμο χαρακτηριστικό της μεταξύ τους συναλλαγής, μια μέγιστη τιμή που μπορεί να ζητηθεί από τον πελάτη. Καθήκον της υπηρεσίας Contract Monitoring είναι να καταγράψει

γεγονότα συγκρίνοντας την μέγιστη τιμή του συγκεκριμένου χαρακτηριστικού με την τιμή που ζητά ο πελάτης σε κάθε του συναλλαγή. Η υπηρεσία Contract Enforcing θα πρέπει να χρησιμοποιεί ως είσοδο τα γεγονότα που καταγράφονται από την υπηρεσία Contract Monitoring για να εκτελεί τις απαραίτητες ενέργειες στις περιπτώσεις μη-συμμόρφωσης του πελάτη με το συμβόλαιο. Ομοίως η υπηρεσία Contract Notifying θα πρέπει σε κάθε περίπτωση μη-συμμόρφωσης να στέλνει ειδοποίησεις τόσο στον πελάτη, όσο και στον χορηγό της υπηρεσίας.

9.3.4. Παροχή υπηρεσιών ασφάλειας από καταλόγους των υπηρεσιών διαδικτύου.

Ένας κατάλογος υπηρεσιών διαδικτύου (π.χ. UDDI) επιτρέπει τη δυναμική αναζήτηση υπηρεσιών διαδικτύου από ένα πελάτη με βάση ορισμένα κριτήρια. Η παροχή υπηρεσιών ασφάλειας από ένα κατάλογο υπηρεσιών είναι μια ιδέα που παρουσιάζει εξαιρετικό ενδιαφέρον. Πρώτα από όλα ένας κατάλογος υπηρεσιών είναι απαραίτητο να μπορεί να εξασφαλίζει την αυθεντικότητα μιας υπηρεσίας στον πελάτη. Ακόμα, είναι χρήσιμο να μπορεί να υποστηρίξει την αυθεντικοποίηση ενός πελάτη από μία υπηρεσία. Επίσης, ένας κατάλογος υπηρεσιών μπορεί να επεκταθεί για να παρέχει χρήσιμες πληροφορίες σχετικές με την ασφάλεια στον πελάτη μιας υπηρεσίας. Τέλος, μπορεί να χρησιμοποιηθεί και για την σύναψη συμφωνιών σε επίπεδο υπηρεσίας. Συγκεκριμένα :

- Σε ότι αφορά στην εξασφάλιση της αυθεντικότητας μιας υπηρεσίας, ένας κατάλογος υπηρεσιών θα πρέπει να υποστηρίζει μια σειρά ελέγχων που θα αφορούν στην πιστοποίηση της ταυτότητας μιας υπηρεσίας. Αυτό σημαίνει, ότι θα πρέπει να εξασφαλίζεται ότι ο δείκτης που δείχνει στην περιγραφή μιας υπηρεσίας παρέχει πρόσβαση στην πραγματική υπηρεσία στην οποία αντιστοιχούν οι πληροφορίες που αναφέρονται στον κατάλογο. Επίσης, θα πρέπει να εφαρμόζεται έλεγχος πρόσβασης πριν επιτραπεί οποιαδήποτε τροποποίηση των καταχωρήσεων του καταλόγου.
- Σε ότι αφορά στην υποστήριξη της αυθεντικοποίηση ενός πελάτη, ένας κατάλογος υπηρεσιών μπορεί να επεκταθεί προκειμένου να εκδίδει διαπιστευτήρια για την αυθεντικοποίηση ενός πελάτη από μια υπηρεσία ή ακόμα και να αυθεντικοποιεί ένα πελάτη για λογαριασμό μιας υπηρεσίας, εφόσον έχει εξουσιοδοτηθεί για αυτό από την υπηρεσία. Μια καλή ιδέα είναι να χρησιμοποιηθεί επίσης ένας κατάλογος υπηρεσιών για την έκδοση ενός διαπιστευτηρίου που θα επιτρέπει την πρόσβαση σε πολλές υπηρεσίες ή



για την αυθεντικοποίηση ενός πελάτη επιτρέποντας τον έλεγχο πρόσβασης τους σε πολλές υπηρεσίες από ένα κοινό σημείο (single sign-on).

- Σε ότι αφορά στην παροχή πληροφοριών σχετικών με την ασφάλεια, ένας κατάλογος υπηρεσιών μπορεί να επεκταθεί έτσι ώστε να μπορεί για παράδειγμα να συγκρίνει την πολιτική ασφαλείας του πελάτη με την πολιτική ασφαλείας της υπηρεσίας, εφόσον είναι διαθέσιμες σε XML απεικόνιση, και να παρέχει πληροφορίες στον πελάτη. Επίσης, μπορεί να παρέχει πληροφορίες σε ένα πελάτη για τα πρωτόκολλα ασφαλείας ή τους αλγόριθμους κρυπτογράφησης που υποστηρίζονται από μία υπηρεσία. Επίσης, πολύ χρήσιμο θα ήταν ένας κατάλογος υπηρεσιών να μπορεί να εκτελεί και αναζητήσεις θέτοντας ως κριτήριο τέτοιου είδους πληροφορίες
- Σε ότι αφορά τέλος στις συμφωνίες σε επίπεδο υπηρεσίας, ένας κατάλογος υπηρεσιών μπορεί να υποστηρίξει ορισμένες από τις λειτουργίες που αναφέρθηκαν στην προηγούμενη ενότητα. Για παράδειγμα ένας κατάλογος υπηρεσιών μπορεί να υποστηρίξει την διαδικασία σύνταξης μιας συμφωνίας με βάση κάποιο XML σχήμα ή μπορεί να διατηρεί μια βάση δεδομένων με τις συμφωνίες που κλείνονται μεταξύ ενός πελάτη και μιας υπηρεσίας. Τέλος, ιδιαίτερα χρήσιμο θα ήταν ένας κατάλογος υπηρεσιών να μπορεί να παρέχει γενικές πληροφορίες σε ένα δυνητικό πελάτη, με βάση τις πληροφορίες των συμφωνιών που έχουν συναφθεί μεταξύ άλλων πελατών και της υπηρεσίας, ή ακόμα και να εκτελεί αναζητήσεις με βάση τις πληροφορίες αυτές.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ**Στην αγγλική γλώσσα.**

- [Armstrong et al., 2002] Armstrong Eric, Bodoff Stephanie, Carson Debbie, Fisher Maydene, Green Dale, Haase Kim, “The Java Web Services Tutorial”, Chapter 13, Sun Microsystems, Inc., March 2002.
- [Bosworth, 2001] Bosworth Adam, “Developing Web Services”, IEEE, 2001.
- [Clabby, 2002] Joe Clabby, “Web Services Explained: Solutions and Applications for the Real World”, Prentice Hall, May 2002.
- [Curbera et al., 2001] Francisco Curbera, William A. Nagy, Sanjiva Weerawarana, “Web Services: Why and How”, IBM T.J. Watson Research Center, August 2001.
- [Curbera et al., 2002] Curbera Francisco, Duftler Matthew, Khalaf Rania, Nagy William, Mukhi Nirmal, Weerawarana Sanjiva, “Unraveling the Web Services Web”, IEEE, April 2002.
- [Damiani, 2001] Damiani E., Capitani S., Paraboschi S., Samarati P., “Fine Grained Access Control for SOAP E-Services”, ACM, May 2001.
- [Evans, 2002] Nick Evans, “Dissecting the Web Services Value Chain”, Fawcette Technical Publications, 2001.
- [Gisolfi, 2001] Gisolfi, D., “Web Services Architect Part 1: An Introduction to Dynamic e-Business”, IBM, April 2001.
- [Glass, 2000] Graham Glass, “The Web services (r)evolution”, The Mind Electric, November 2001.
- [Goldfarb et al., 2000] Goldfarb Charles, Prescod Paul, “The XML Handbook”, second edition, Prentice Hall, January 2000.
- [Gunzer, 2002] Hartwig Gunzer, “Introduction to Web Services”, Borland, March 2002.
- [Hartman, 2002] Hartman Hans, “Web Services Are Catching On. Is Security Catching Up?”, June 2002.
- [HP, 2001] Hewlett-Packard Company, “Web services concepts: A technical overview”, White Paper, 2001.
- [IBM-MS, 2002] IBM Corporation, Microsoft Corporation, “Security in a Web Services World: A proposed Architecture and Roadmap”, Whitepaper (Version 1.0), April 2002.



- [Iona, 2002] IONA Technologies PLC, “Orbix E2A XMLBus Edition: Technology Overview”, White Paper, April 2002.
- [J2EE SEC] Sun Microsystems, “Developing Enterprise Applications with J2EE: Security (ch.9)”, pp. 221-245, December 1999.
- [Kao, 2001] Kao James, “Developer's Guide to Building XM-based Web Services with the Java 2 Platform, Enterprise Edition”, The Middleware Company, June 2001.
- [Kazutoshi et al., 2002] Kazutoshi Yokoyama, Eiji Yoshida, Shigeyuki Matsuda, “Requirements for Open Service Collaboration among Web Services”, IEEE, 2002.
- [Khare et al., 1997] Khare Rohit, Rifkin Adam, “XML: A door to Automated Web Applications”, IEEE 1997.
- [Kreger, 2001] Heather Kreger, “Web Services Conceptual Architecture (1.0)”, IBM Software Group, May 2001.
- [Layman et al., 2001] Layman Andrew, Montgomery John, “XML, Web Services, and .NET Framework”, Microsoft, January 2001.
- [Maddox et al., 2002] Maddox A. Roberts T., “Distributed Web Application Development: A Comparison of .Net and J2EE”, Department of Electrical and Electronic Engineering, Manukau Institute of Technology, Auckland, 2002.
- [Mariucci, 2000] Mariucci Marcello, “Enterprise Application Server Development Environments” University of Stuttgart, October 2000.
- [MS .NET] Microsoft .NET Web Site (<http://www.microsoft.com/net>)
- [Mulcahy, 2002] Mulcahy G., “J2EE and .NET security”, February 2002.
- [Nagaraj, 2003] Nagaraj S. V., “Aspects of Web Services Security”, IFIP/SEC 2003.
- [.NET SEC] Foundstone, Inc., Core Security Technologies, “Security in the Microsoft .NET Framework”.
- [Power, 2002] Power Richard, “2002 CSI/FBI Computer Crime and Security Survey”, Computer Security Issues & trends, vol. 3, No 1, Spring 2002.
- [Samarati et al., 2001] Pierangela Samarati, Sabrina de Capitani di Vimercati, “Access Control: Policies, Models, and Mechanisms”, R. Focardi and R. Gorrieri (Eds.): FOSAD 2000, LNCS 2171, pp. 137–196, 2001.
- [SAML] Security Assertion Markup Language Specification 1.0, OASIS Standard, May 2002.
- [Seligman et al., 2001] Seligman Len, Rosenthal Arnon, “XML's Impact on Databases and Data Sharing”, IEEE, June 2001.
- [Shannon, 2001] Shannon Bill, “J2EE Specification 1.3 (Final Release)”, Sun Microsystems, Inc., July 2001.

- [Shohoud, 2003] Yasser Shohoud, "Real World XML Web Services", Chapter 1, Pearson Education, Inc, May 2003 (To be published).
- [Skoularidou et al., 2002] Skoularidou V., Kokolakis S., Spinellis D., "Performing Risk Analysis on the Microsoft .NET Platform: Assessment of Risks and Recommendations for Users", working paper, 2002.
- [Sleeper et al., 2001] Brent Sleeper, Bill Robins, "Defining Web Services", The Stencil Group, June 2001.
- [Vaughan, 2002] Vaughan-Nichols J. Steven, "Web Services: Beyond the Hype", February 2002.
- [Warren et al., 2001] Warren Robert, Shah Piyush, "Web Services and Microsoft .NET", Center for Technology Innovation, 2001.
- [Westbridge, 2002] Westbridge Technology, Inc., "XML Application Firewall", 2002.
- [XACML], Extensible Access Control Markup Language Specification 1.0, OASIS Working Draft, November 2002.
- [XKMS], XML Key Management Specification 2.0, W3C Working Draft, March 2002.
- [XML DS] XML Signature Syntax and Processing, W3C Recommendation, February 2002.
- [XML ENC] XML Encryption Syntax and Processing, W3C Proposed Recommendation, October 2002.

Στην ελληνική γλώσσα.

- [Αποστολόπουλος, 1997] Αποστολόπουλος Η., "Δίκτυα Υπολογιστών : Μετάδοση Δεδομένων -Επικοινωνιακό Υποδίκτυο", 1997.
- [Γκρίτζαλης Δ., 2001] Γκρίτζαλης Δ., "Ασφάλεια στις Τεχνολογίες Πληροφοριών και Επικοινωνιών", Οκτώβρης 2001.
- [Γκρίτζαλης Στ., 2002 (1)] Γκρίτζαλης Στ., "Ασφάλεια στο Internet", Συμπληρωματικές διδακτικές σημειώσεις, Πανεπιστήμιο Αιγαίου, Μάρτιος 2002.
- [Γκρίτζαλης Στ., 2002 (2)] Γκρίτζαλης Στ., "Υπηρεσίες Παροχών Υπηρεσιών Πιστοποίησης", Συμπληρωματικές διδακτικές σημειώσεις, Πανεπιστήμιο Αιγαίου, Μάρτιος 2002.
- [Κοκολάκης, 2000] Κοκολάκης Σπ., "Ανάπτυξη και Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων : Εννοιολογικό Πλαίσιο, Μεθοδολογίες και Εργαλεία", Διδακτορική διατριβή, Οικονομικό Πανεπιστήμιο Αθηνών, Ιούνιος 2000.



