Πανεπιστήμιο Πειραιώς
Τμήμα Ψηφιακών Συστημάτων

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

«Διδακτικής της Τεχνολογίας & Ψηφιακών Συστημάτων,
Κατεύθυνση: Δικτυοκεντρικά Συστήματα»

Διπλωματική Εργασία:

Αυθεντικοποίηση στο Διαδίκτυο (με έμφαση στην Ελλάδα)

Νικόλαος Μαούνης – ΜΕ08088

Επιβλέπων: Κ. Λαμπρινουδάκης

Πειραιάς 2011

Περιεχόμενα

Πρόλογος

Στα πλαίσια αυτής της εργασίας γίνεται μια μελέτη για την αυθεντικοποίηση στην πραγματικότητα των ελληνικών ηλεκτρονικών υπηρεσιών.

Στο κεφάλαιο 1 καλύπτεται θεωρητικά η έννοια της αυθεντικοποίησης στο διαδίκτυο

Στο κεφάλαιο 2 γίνεται μία θεωρητική επισκόπηση των τεχνολογιών που αποτελούν το υπόβαθρο των ηλεκτρονικών υπηρεσιών στην Ελλάδα.

Στο κεφάλαιο 3 εξετάζεται η πραγματικότητα και ο τρόπος λειτουργίας των ελληνικών υπηρεσιών ηλεκτρονικής διακυβέρνησης σε θέματα αυθεντικοποίησης και τέλος στο κεφάλαιο 4 παρουσιάζεται μία πρόταση και μία θεωρητική ανάλυση της πρότασης αυτής για το πώς θα μπορούσαν να βελτιωθούν η ελληνικές e-υπηρεσίες με χρήση συγκεκριμένων τεχνολογιών.

Θα ήθελα να ευχαριστήσω θερμά τον Καθηγητή μου κ. Λαμπρινουδάκη για το ενδιαφέρον που μου δημιούργησε με τη διδασκαλία του ώστε να επιλέξω αυτό το θέμα για την διπλωματική μου εργασία.

1 Εισαγωγή στην Αυθεντικοποίηση

Μέρος της ασφάλειας ενός Πληροφοριακού Συστήματος (ΠΣ) αποτελεί ο έλεγχος της ταυτότητας των χρηστών του. Ο έλεγχος αυτός γίνεται μέσω της ταυτοποίησης και της αυθεντικοποίησης του χρήστη.

Ταυτοποίηση (identification) ονομάζεται η διαδικασία κατά την οποία ένα λογικό υποκείμενο παρέχει σε ένα ΠΣ τις πληροφορίες που απαιτούνται προκειμένου να συσχετιστεί με ένα από τα αντικείμενα που δικαιούνται προσπέλασης στους πόρους του.

Αυθεντικοποίηση (authentication) ονομάζεται η διαδικασία εκείνη κατά την οποία ένα λογικό υποκείμενο παρέχει σε ένα ΠΣ τις πληροφορίες που απαιτούνται προκειμένου να ελεγχθεί η βασιμότητα της συσχέτισης που επιτεύχθηκε κατά τη διαδικασία της ταυτοποίησης.

Η αυθεντικοποίηση συνεπώς αφορά τη διαδικασία κατά την οποία επαληθεύεται η δηλωθείσα ταυτότητα ενός λογικού υποκειμένου. Η ανάγκη αυθεντικοποίησης από ένα σύστημα οφείλεται σε δύο λόγους:

- Η ταυτότητα του λογικού υποκειμένου αποτελεί παράμετρο για τον έλεγχο προσπέλασης στους πόρους του συστήματος.
- Η ταυτότητα του λογικού υποκειμένου πρέπει να καταγράφεται σε ημερολόγια ελέγχου κατά τη διαδικασία πρόσβασης.

Η ταυτοποίηση και η αυθεντικοποίηση αποτελούν δύο σκέλη του πρωτοκόλλου επικοινωνίας που ενεργοποιείται όταν ένα λογικό υποκείμενο αιτείται προσπέλαση στους πόρους ενός ΠΣ.

1.1 Κατηγορίες Αυθεντικοποίησης

Η διαδικασία αυθεντικοποίησης περιλαμβάνει την υποβολή πληροφοριών στο σύστημα εκ των προτέρων γνωστές αποκλειστικά και μόνο στο λογικό υποκείμενο και στο ΠΣ.

Ανάλογα με το είδος του συστήματος, κυριαρχούν τέσσερις βασικοί τρόποι για την εφαρμογή ελέγχων αυθεντικοποίησης. Αυτοί βασίζονται σε:

- Τύπος 1: Κάτι που το λογικό υποκείμενο γνωρίζει (πχ. ένα συνθηματικό ή ένα PIN)
- Τύπος 2: Κάτι που το λογικό υποκείμενο κατέχει (μαγνητική συσκευή αναγνώρισης, πχ. έξυπνη κάρτα ή ψηφιακό πιστοποιητικό)
- Τύπος 3: Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του (συστήματα βιομετρικής τεχνολογίας, πχ. εφαρμογές

δακτυλικών αποτυπωμάτων, αναγνώριση φωνής και ίριδας ματιού)
- Τύπος 4: Κάτι που προσδιορίζει την τοποθεσία που βρίσκεται το λογικό υποκείμενο (πχ. διεύθυνση IP)

Ανάλογα με το επίπεδο ασφαλείας του συστήματος, η βέλτιστη πρακτική αυθεντικοποίησης θα πρέπει να περιλαμβάνει ένα συνδυασμό δύο ή περισσότερων τρόπων από τις παραπάνω κατηγορίες.
Η διαδικασία της αυθεντικοποίησης περιλαμβάνει:
- Την παροχή πληροφορίας από ένα λογικό υποκείμενο στο σύστημα
- Την ανάλυση της πληροφορίας αυτής
- Τον έλεγχο ότι πράγματι η πληροφορία αυτή σχετίζεται με το λογικό υποκείμενο

Προστατευόμενος πόρος	**Κάτι που γνωρίζεις**	**Κάτι που έχεις**	**Κάτι που είσαι**
Πλατφόρμα, Host	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα	Βιομετρικό σύστημα (δακτυλικό αποτύπωμα, γεωμετρία χεριού, αναγνώριση προσώπου0
Σύστημα Διαχείρισης Δικτύου (σύστημα αρχείων και εκτυπώσεων)	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα - Ψηφιακό πιστοποιητικό	Βιομετρικό σύστημα (δακτυλικό αποτύπωμα, γεωμετρία χεριού, αναγνώριση προσώπου0
Υπηρεσία Δικτύου (Web, FTP, Telnet)	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα	
Σύστημα Διαχείρισης Βάσεων Δεδομένων	Όνομα χρήστη/ συνθηματικό		

Για την πραγματοποίηση των παραπάνω διαδικασιών, το σύστημα αποθηκεύει και διαχειρίζεται, με τους ανάλογους μηχανισμούς, τις σχετικές με τα λογικά υποκείμενα πληροφορίες. Επομένως, ένα σύστημα αυθεντικοποίησης αποτελείτε από πέντε βασικά μέρη:

- Το σύνολο A ου περιέχει τις πληροφορίες με βάση τις οποίες κάθε λογικό υποκείμενο αποδεικνύει την ταυτότητά του.
- Το σύνολο C που περιέχει τις συμπληρωματικές πληροφορίες που αποθηκεύει και χρησιμοποιεί το σύστημα ώστε να επικυρώνει πληροφορίες αυθεντικοποίησης.
- Το σύνολο F των συμπληρωματικών συναρτήσεων που δημιουργούν τις συμπληρωματικές πληροφορίες για την αυθεντικοποίηση.
- Το σύνολο L των συναρτήσεων αυθεντικοποίησης που αναγνωρίζουν ένα λογικό υποκείμενο.
- Το σύνολο S των λοιπών συναρτήσεων επιλογής που δίνουν τη δυνατότητα σε ένα λογικό υποκείμενο να δημιουργήσει ή να τροποποιήσει τις πληροφορίες αυθεντικοποίησης ή τις συμπληρωματικές πληροφορίες.

1.2 Πλεονεκτήματα και μειονεκτήματα δεδομένων αυθεντικοποίησης

Για τους παραπάνω τρόπους αυθεντικοποίησης υπάρχουν βασικά πλεονεκτήματα και μειονεκτήματα, τα οποία στηρίζονται στη φύση των δεδομένων αυθεντικοποίησης που χρησιμοποιούνται ξεχωριστά. Αυτά είναι τα ακόλουθα:

Τύπος 1: κάτι που το λογικό υποκείμενο γνωρίζει
Μειονεκτήματα:

- Τα δεδομένα αυθεντικοποίησης μπορούν εύκολα να αντιγραφούν
- Είναι εύκολο να τα μαντέψει κάποιος χωρίς ιδιαίτερες τεχνικές γνώσεις
- Πολύ συχνά μπορούν να αποκαλυφθούν με αυτοματοποιημένες μεθόδους.

Πλεονεκτήματα:

- Εύκολη υλοποίηση και εφαρμογή
- Τροποποιούνται εύκολα
- Δεν χάνονται ή κλέβονται
- Αν και είναι απλά στη χρήση τους, στην περίπτωση που περίπτωση που είναι ένας ισχυρός συνδυασμός αριθμών και γραμμάτων δεν αποκαλύπτονται εύκολα

Τύπος 2: Κάτι που το λογικό υποκείμενο κατέχει
Μειονεκτήματα:
- Υψηλό κόστος
- Μπορούν να χαθούν ή να κλαπούν

Πλεονεκτήματα:
- Δεν αντιγράφονται εύκολα διότι κατασκευάζονται από ειδικά υλικά, τα οποία δεν είναι ευρέως διαθέσιμα

Τύπος 3: Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του.
Μειονεκτήματα:
- Δυσκολίες στην κατασκευή αξιόπιστων συσκευών αναγνώρισης με χαμηλό κόστος
- Δεν είναι αλάνθαστα

Πλεονεκτήματα:
- Παρέχουν μεγαλύτερη ασφάλεια από τους Τύπους 1 και 2.

1.3 Δεδομένα αυθεντικοποίησης

1.3.1 Συνθηματικά

Τα συνθηματικά αποτελούν τον ευρύτερα αποδεκτό τρόπο αυθεντικοποίησης, όπου ο χρήστης πιστοποιεί την ορθότητα της ταυτότητάς του κάνοντας χρήση ενός μυστικού που είναι γνωστό μόνο σε αυτόν. Ο χρήστης πρέπει να απομνημονεύσει το μυστικό κωδικό (something known) και να μην τον αποκαλύπτει σε άλλους χρήστες ή οντότητες. Συνήθως τα συνθηματικά δεν αποθηκεύονται καθώς επιλέγονται με τρόπο ώστε να είναι ευκολομνημόνευτα.

1.3.2 Διακριτικά συνθηματικών μιας χρήσης

Τα διακριτικά συνθηματικών μιας χρήσης είναι συσκευές υλικού οι οποίες αξιοποιούνται για τη δημιουργία συνθηματικών, τα οποία δεν απαιτείται να απομνημονεύει ο χρήστης και τα οποία χρησιμοποιούνται μόνο μια φορά. Η παραγωγή των συνθηματικών στηρίζεται σε συγκεκριμένους αλγόριθμους κρυπτογράφησης. Η επαναχρησιμοποίηση ενός κωδικού για μελλοντική αυθεντικοποίηση του χρήστη δεν είναι δυνατή.

1.3.3 Διακριτικά χαλαρής αποθήκευσης

Τα διακριτικά χαλαρής αποθήκευσης αναφέρονται σε μυστικά κλειδιά, τα οποία αποθηκεύονται σε κάποιο μέσο αποθήκευσης όπως

σκληρός δίσκος, CD, USB token κ.λπ. Τα κλειδιά είναι αποθηκευμένα σε κρυπτογραφημένη μορφή, ενώ η προσπέλασή τους είναι δυνατή μόνο με τη χρήση του κατάλληλου συνθηματικού.

1.3.4 Διακριτικά υλικού-σκληρής αποθήκευσης

Τα διακριτικά υλικού σκληρής αποθήκευσης αναφέρονται σε συσκευές υλικού οι οποίες αποθηκεύουν τα απαιτούμενα μυστικά κλειδιά και προσφέρουν tamper proof προστασία. Όλες οι κρυπτογραφικές διαδικασίες πραγματοποιούνται εσωτερικά στη συσκευή και συνεπώς δεν υπάρχει καμία δυνατότητα ανάγνωσης των κλειδιών από εξωτερικές οντότητες. Για την ενεργοποίηση των κλειδιών συνηθίζεται η χρήση κάποιου συνθηματικού.

1.3.5 Ψηφιακά πιστοποιητικά

Τα ψηφιακά πιστοποιητικά έχουν τη μορφή δυαδικών αρχείων και η λειτουργία τους στηρίζεται στην Κρυπτογραφία Δημόσιου Κλειδιού. Μπορούν να χρησιμοποιηθούν για τον περιορισμό της αποκάλυψης της ταυτότητας του χρήστη, ενσωματώνοντας ψευδώνυμα αντί της πραγματικής ταυτότητάς τους. Η έκδοση ενός ψηφιακού πιστοποιητικού γίνεται μετά από αίτηση του ενδιαφερομένου σε μία Αρχή Πιστοποίησης. Η Αρχή Πιστοποίησης επιβεβαιώνει την ταυτότητα του αιτούντος και εκδίδει το πιστοποιητικό, το οποίο συνοπτικά περιλαμβάνει τα εξής στοιχεία:

- Το ονοματεπώνυμο και διάφορες άλλες πληροφορίες σχετικά με τον κάτοχο του πιστοποιητικού.
- Το δημόσιο κλειδί του κατόχου του πιστοποιητικού.
- Την ημερομηνία λήξης του πιστοποιητικού.
- Το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε.

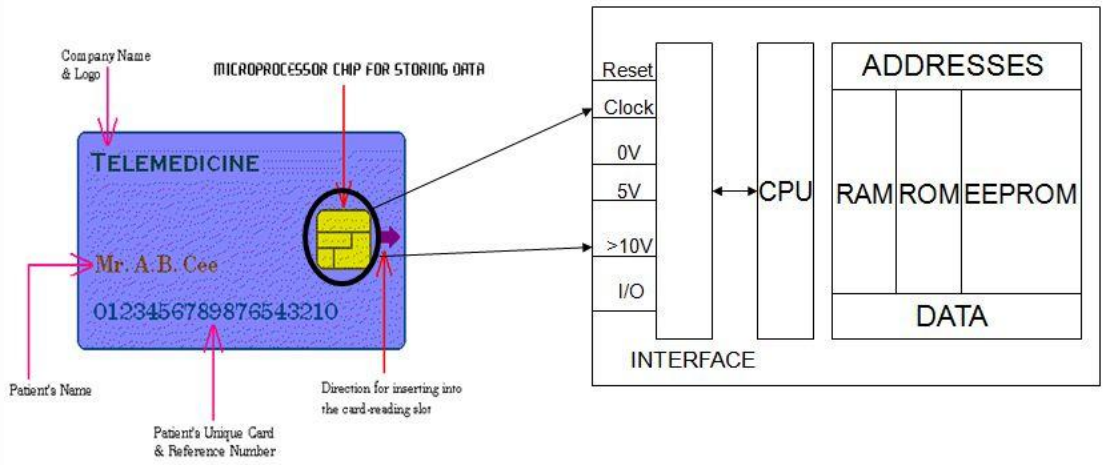
Το πιο διαδεδομένο πρότυπο ψηφιακών πιστοποιητικών είναι το X.509.

1.3.6 Έξυπνες Κάρτες

Η έξυπνη κάρτα είναι μια μικρή πλαστική κάρτα που περιέχει ένα τσιπ υπολογιστή. Οι έξυπνες κάρτες χρησιμοποιούνται μαζί με προσωπικούς αναγνωριστικούς αριθμούς (PIN) για σύνδεση σε ένα δίκτυο, έναν υπολογιστή ή μια συσκευή. Η αυθεντικοποίηση μιας έξυπνης κάρτας μπορεί να γίνει με τη χρήση ψηφιακών πιστοποιητικών και ασύμμετρων κρυπτογραφικών αλγορίθμων ή αξιοποιώντας συμμετρικούς αλγόριθμους κρυπτογράφησης (για παράδειγμα DES). Η χρήση έξυπνης κάρτας αυξάνει την ασφάλεια κατά ένα επίπεδο σε σύγκριση με τον κωδικό πρόσβασης, καθώς είναι δυσκολότερο για κάποιον να κλέψει μια έξυπνη κάρτα και να μάθει το PIN σας απ᾽ότι να μάθει τον κωδικό πρόσβασής σας. Οι έξυπνες κάρτες εκδίδονται συνήθως από τα τμήματα τεχνολογίας πληροφορικής (IT) μεγάλων οργανισμών. Για να χρησιμοποιήσετε μια έξυπνη κάρτα, θα χρειαστείτε επίσης μια *συσκευή ανάγνωσης έξυπνων καρτών*.

Μια έξυπνη κάρτα αποτελείται από τα εξής τμήματα:

- Τη μνήμη εργασίας (working memory – Random Access Memory),η οποία διατηρεί τα περιεχόμενά της μόνο όσο λειτουργεί η κάρτα και αξιοποιείται από τον επεξεργαστή
- Τη μη διαγράψιμη μνήμη ROM (Read Only Memory), η οποία δεν απαιτεί συνεχή τροφοδοσία ρεύματος και αποθηκεύει τα δεδομένα που είναι απαραίτητα για τη λειτουργία της κάρτας.
- Τη μνήμη εφαρμογών (EEPROM) που περιλαμβάνει τη Μυστική Περιοχή (Secret Area) στην οποία φυλάσσεται το Κλειδί Εργοστασίου (Manufacture’s Key) και τα Κύρια και δευτερεύοντα κλειδιά του εκδότη της κάρτας (Primary Issuer key (PIK) and Co-Issuer Key (CIK)) καθώς και ο Μυστικός προσωπικός κωδικός (Personal Identification Number-PIN) και τα Κλειδιά Κρυπτογραφίας
- Την Περιοχή Ιστορικού Πρόσβασης (Access Area) στην οποία γίνεται καταγραφή όλων των προσπαθειών πρόσβασης σε προστατευμένες περιοχές της κάρτας.
- Την περιοχή Ελεύθερης Πρόσβασης (Public Area)
- Την Περιοχή Εργασίας (Work Area) όπου γίνεται αποθήκευση δεδομένων από τις εφαρμογές και προστατεύονται με μυστικά κλειδιά σε ότι αφορά την ανάγνωση, εγγραφή ή/και διαγραφή.


Company Name
& Logo
MICROPROCESSOR CHIP FOR STORING DATA
TELEMEDICINE
Mr. A.B. Cee
0123456789876543210
Patient's Name
Patient's Unique Card
& Reference Number
Direction for inserting into
the card-reading slot
Reset
Clock
0V
5V
>10V
I/O
INTERFACE
CPU
ADDRESSES
RAM
ROM
EEPROM
DATA

1.4 Συστήματα αυθεντικοποίησης

1.4.1 Σύστημα Kerberos

Το Kerberos σύστημα αναπτύχθηκε από το *Massachusetts Institute of Technology (MIT)* για να προστατέψει τις δικτυακές υπηρεσίες που παρέχονταν από το Project Athena και βασίζεται στο μοντέλο διανομής κλειδιών Needham και Schoeder. Οι εκδόσεις 1 έως 3 χρησιμοποιήθηκαν εσωτερικά από το MIT. Παρ' όλο που σχεδιάσθηκε αρχικά για χρήση με το Project Athena, η 4η έκδοση πέτυχε παγκόσμια υιοθέτηση. Λόγω, όμως, του γεγονότος ότι πολλά περιβάλλοντα είχαν απαιτήσεις που δεν μπορούσε να καλύψει η 4η έκδοση, νέα χαρακτηριστικά εισηγήθηκαν με την ανάπτυξη του Kerberos version 5.0 που απευθυνόταν σε περισσότερες περιπτώσεις. Η τρέχουσα έκδοση είναι η 5.0. Το Kerberos είναι ένα σύστημα πιστοποίησης ταυτότητας το οποίο αναπτύχθηκε με την ελπίδα αντικατάστασης του συστήματος που καλείται πιστοποίηση βάσει ισχυρισμού *(authentication by assertion)*. Η πιστοποίηση βάσει ισχυρισμού στηρίζεται στην εξής αρχή: όταν ο χρήστης τρέχει ένα πρόγραμμα που απαιτεί πρόσβαση σε μία δικτυακή υπηρεσία, το πρόγραμμα ανακοινώνει στον server ότι λειτουργεί εκ μέρους του συγκεκριμένου χρήστη. Ο server πιστεύει τα στοιχεία που του παρέχει ο client (δηλαδή το πρόγραμμα) και εξυπηρετεί τον χρήστη χωρίς να ζητά άλλες αποδείξεις. Όπως καταλαβαίνουμε, η παρεχόμενη ασφάλεια είναι πολύ χαμηλού επιπέδου έως και ανύπαρκτη.

Ένα άλλο σύστημα που χρησιμοποιείται πολύ, είναι η συνοδεία του ονόματος του χρήστη από έναν μυστικό κωδικό. Σε αυτό το εναλλακτικό σχήμα πιστοποίησης ταυτότητας υπάρχουν δύο, τουλάχιστον, διαφορετικά μειονεκτήματα. Πρώτον, αποτελεί χάσιμο χρόνο για τον χρήστη. Δεύτερον και σημαντικότερον, είναι ευάλωτο σε επιθέσεις παθητικού τύπου *(passive attacks)*, καθ' ότι ο κωδικός διανύει τη δίκτυο μη κρυπτογραφημένος. Το σύστημα Kerberos καλύπτει ένα σημαντικό κενό των συστημάτων πιστοποίησης ταυτότητας.

Το Kerberos επιτρέπει στις δικτυακές εφαρμογές να αναγνωρίζουν με ασφάλεια την ταυτότητα του χρήστη που ζητά εξυπηρέτηση, χωρίς να στέλνει στο δίκτυο δεδομένα που μπορούν να επιτρέψουν σε ένα πιθανό εισβολέα να προσποιηθεί ότι είναι ο χρήστης και χωρίς να βασίζεται στις διευθύνσεις των μηχανών του δικτύου. Επίσης, η πιστοποίηση ταυτότητας γίνεται από τον application server και η επικοινωνία γίνεται εν γνώση της πιθανότητας ότι η διακινούμενη πληροφορία μπορεί να τροποποιηθεί και να αναγνωστεί κατά βούληση. Το Kerberos προαιρετικά προσφέρει ακεραιότητα και απόρρητη συναλλαγή για τα δεδομένα

που στέλνονται μεταξύ του client και του application server. Σαν application server εννοούμε τον server που προσφέρει υπηρεσίες όπως mail, ftp, http, telnet.

Το σύστημα χρησιμοποιεί μια σειρά από κρυπτογραφημένα μηνύματα για να αποδείξει σε έναν application server ότι ο client λειτουργεί εκ μέρους ενός συγκεκριμένου χρήστη. Για την ανταλλαγή των μηνυμάτων ο Kerberos εκμεταλλεύεται το IP επίπεδο σε συνδυασμό με το UDP πρωτόκολλο. Ο client αποδεικνύει την ταυτότητα του χρήστη παρουσιάζοντας στον application server την απόδειξη ticket, η οποία περιέχει ένα προσωρινό κλειδί κρυπτογράφησης που θα χρησιμοποιηθεί για την επικοινωνία μεταξύ του application server και του χρήστη, και το πιστοποιητικό authenticator, το οποίο αποδεικνύει ότι ο client έχει στην κατοχή του το session key που έχει εκδοθεί για τον χρήστη που ορίζεται στο ticket. Οι αποδείξεις εκδίδονται από ένα αφιερωμένο υπολογιστή που καλείται authentication server (AS). Oauthentication server έχει αποθηκευμένα μυστικά κλειδιά, που καλούνται server keys και τα μοιράζεται με τους application servers. Εγκαθίστανται μέσα από κρυπτογραφημένο κανάλι ή με out-of-bandεπικοινωνία. Το server key πιστοποιεί την αυθεντικότητα των αποδείξεων tickets που λαμβάνει ο client και ο server. Επιπλέον, ο AS έχει αποθηκευμένα κλειδιά που αναφέρονται σε κάθε χρήστη και καλούνται user keys. Όλα τα κλειδιά εμπεριέχονται σε βάση δεδομένων. Τέλος να πούμε ότι κάθε ticket έχει περιορισμένη διάρκεια ζωής και όταν το χρονικό αυτό διάστημα περάσει τότε είναι άχρηστο. Περαιτέρω ανταλλαγή μηνυμάτων απαιτεί την έκδοση νέου ticket.

Οποτεδήποτε ο χρήστης θέλει να έρθει σε επαφή με κάποιον application server, ο client αναλαμβάνει να ξεκινήσει την διαδικασία απόκτησης κατάλληλων διαπιστευτηρίων *(credentials)* για τον θα χρησιμοποιηθούν με τον συγκεκριμένο application server. Μια περιληπτική παρουσίαση της συναλλαγής αυτής βλέπουμε παρακάτω:

Κατεύθυνση του Μηνύματος	*Τύπος Μηνύματος*	*Περιγραφή Μηνύματος*
1. Client ☋ Authentication Server	KRB_AS_REQ	Authentication Request
2. Client ✍ Authentication Server	KRB_AS_REP	Authentication Response
	or	Failed Authentication Request or Other kind of Failure
	KRB_ERROR	

Αίτηση Πιστοποίησης Ταυτότητας

Ο client επικοινωνεί με τον AS στέλνοντας κατάλληλη αίτηση και αυτός απαντά με τα διαπιστευτήρια. Τα διαπιστευτήρια αποτελούνται από (α) ένα session key που χρησιμοποιείται σαν κλειδί κρυπτογράφησης και (β) ενός ticket για τον application server. Το session key και το ticket διαφέρουν για κάθε application server με τον οποίο επικοινωνεί ο χρήστης. Η αίτηση που στέλνει ο client στον AS καλείται authentication request και περιέχει τα στοιχεία της ταυτότητας του client, το όνομα του application server, την ζητούμενη διάρκεια ζωής του ticket και ένα τυχαίο αριθμό που θα χρησιμοποιηθεί για το ταίριασμα της authentication request με την authentication response. Επίσης, ο client μπορεί να καθορίσει συγκεκριμένες επιλογές σχετικές με την φύση τού ticket (renewable, proxiable, forwardable κτλ).

Απάντηση στην Αίτηση Πιστοποίησης Ταυτότητας

Ο AS ψάχνει στην βάση δεδομένων του για να ανακτήσει τα κλειδιά του χρήστη (user key) και του application server (server key). Παράγει με τυχαίο τρόπο το session key και ελέγχει τα πεδία με τις επιλογές του client όσον αναφορά το ticket. Σε απάντηση, ο AS επιστρέφει το session key, την διάρκεια ζωής του ticket και του session key, τον τυχαίο αριθμό από την αίτηση και το όνομα του application server, όλα αυτά κρυπτογραφημένα με το μυστικό κλειδί κωδικό του χρήστη (user key). Μαζί αποστέλλει και το ticket που περιέχει τις ίδιες πληροφορίες που αναφέρθηκαν πριν, κρυπτογραφημένες με το server key. Το ticket θα προωθηθεί από τον client στον server σαν μέρος της αίτησης εξυπηρέτησης. Το ticket έχει ρυθμιστεί σύμφωνα με τις επιλογές του client.

Πολλά λάθη μπορούν να προκύψουν και η απάντηση στην αίτηση του client να είναι ένα μήνυμα λάθους. Στο μήνυμα λάθους θα περιέχεται κατάλληλος κωδικοποιημένος αριθμός που θα υποδεικνύει το είδος του λάθους.

Όταν ο client παραλάβει την authentication response, κατ' αρχή ελέγχει κατά πόσο ο τυχαίος αριθμός που είχε συμπεριλάβει στην αίτηση ταιριάζει με αυτόν που περιέχεται στο παραληφθέν μήνυμα. Γι' αυτό το σκοπό χρησιμοποιεί το κλειδί του χρήστη (user key) για να ανακτήσει το session key και το ticket. Αφού επιβεβαιώσει ότι η απάντηση ανταποκρίνεται στην αυθεντική αίτηση, αποκλείονται έτσι την πιθανότητα επίθεσης *replay attack*, συνεχίζει με την επεξεργασία του υπόλοιπου μηνύματος. Το γεγονός ότι τα περιεχόμενα της authentication response ήταν κρυπτογραφημένα με το κλειδί του χρήστη, αποδεικνύει ότι η απάντηση προέρχεται από τον αληθινό AS, ενώ το γεγονός ότι ο client μπορεί να

αποκρυπτογραφήσει τα περιεχόμενα της απάντησης σημαίνει ότι αντιπροσωπεύει τον έγκυρο χρήστη. Εάν το μήνυμα που λάβει ο client είναι μήνυμα λάθους, τότε ερμηνεύει τα περιεχόμενα του και αποφαίνεται για το τι πρέπει να πράξει ώστε να μην επαναληφθεί.

Χρήση Διαπιστευτηρίων

Η ανταλλαγή μηνυμάτων αυτού του σταδίου χρησιμοποιείται από application servers του δικτύου για να πιστοποιήσουν την ταυτότητα του client και κατ' επέκταση την ταυτότητα του χρήστη, και αντιστρόφως. Ο client πρέπει πρώτα να έχει στην κατοχή του τα διαπιστευτήρια για τον συγκεκριμένο application server.

Κατεύθυνση του Μηνύματος	*Τύπος Μηνύματος*	*Περιγραφή Μηνύματος*
1. Client a Application Server	KRB_AP_REQ	Application Request
2. Client ? Application Server	KRB_AP_REP	Application Response
	or KRB_ERROR	Failed Application Request or Other kind of Failure

Η παροχή μόνο του ticket στην αίτηση εξυπηρέτησης δεν αποτελεί ικανοποιητικό στοιχείο για την απόδειξη της ταυτότητας του client. Το ticket μπορεί να χρησιμοποιηθεί από εισβολέα που έχει καταγράψει την διακινούμενη πληροφορία. Η συνοδεία του ticket με επιπλέον πληροφορία (authenticator) που είναι δεμένη με την ταυτότητα του client, εξασφαλίζει ολοκληρωμένη επαλήθευση. Στο authenticator περιλαμβάνεται ένα checksum. Checksum είναι η hash ή digest value του μηνύματος κρυπτογραφημένη με το session key ή άλλο κλειδί.

Αίτηση Εξυπηρέτησης

Μία αίτηση εξυπηρέτησης αποτελείται από δύο μέρη: την απόδειξη ticket και το πιστοποιητικό authenticator. Το authenticator περιλαμβάνει την τρέχουσα ώρα, ένα checksum, ένα προαιρετικό κλειδί κρυπτογράφησης και στοιχεία της ταυτότητας του χρήστη όλα κρυπτογραφημένα με το session key. Το προαιρετικό κλειδί κρυπτογράφησης μπορεί να χρησιμοποιηθεί για κρυπτογράφηση των μελλοντικών μηνυμάτων μεταξύ application server και client.

Τα authenticators δεν μπορούν να ξανά χρησιμοποιηθούν και για κάθε αίτηση εξυπηρέτηση, ακόμα και αν είναι για τον ίδιο application

server, ετοιμάζεται καινούργιο. Authenticators που επαναλαμβάνοντ αι θα απορριφθούν από τον application server.

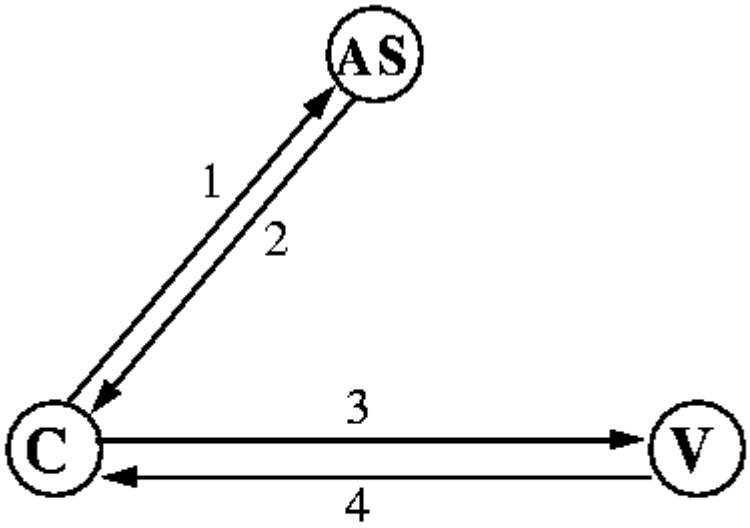
Επεξεργασία και Απάντηση στην Αίτηση Εξυπηρέτησης

Η πιστοποίησης της ταυτότητας του client βασίζεται στο πεδίο της τρέχουσας ώρας, στο authenticator και στο ticket. Όταν ο application server παραλάβει την application request, αποκρυπτογραφεί το ticket με το server key και παίρνει το session key που περιέχεται στο ticket. Με το session key αποκρυπτογραφεί το autheticator και ανακτά τις πληροφορίες για την ταυτότητα του χρήστη και την ώρα αποστολής της αίτησης. Έπειτα ελέγχει το checksum, παράγοντας το δικό του hash value και συγκρίνοντας το με αυτό που προκύπτει από την αποκρυπτογράφηση του checksum. Τέλος ελέγχει το πεδίο της ώρας συγκρίνοντας την τρέχουσα ώρα με την ώρα που περικλείεται στο authenticator. Εάν διαφέρουν περισσότερο από πέντε λεπτά, το μήνυμα απορρίπτεται και θεωρείται προϊόν επίθεσης επανάληψης *(replay attack)*. Το ότι ο server μπορεί να ανακτήσει το session key επιβεβαιώνει ότι έχει στην κατοχή το server key και άρα αποτελεί τον πραγματικό server. Η κρυπτογράφηση του authenticator με το session key και ο έλεγχος της ώρας αποστολής του authenticator, επαληθεύει ότι την ταυτότητα του χρήστη που αναγράφεται στο ticket.

Προαιρετικά, εάν υποστηρίζεται αμοιβαία πιστοποίησης ταυτότητας, ο application server πιστοποιεί την ταυτότητα του στον client. Για να το επιτύχει αυτό, ετοιμάζει την application response, όπου τοποθετεί την ώρα αποστολής που περιεχόταν στην αίτηση και την κρυπτογραφεί με το session key. Ο client όταν θα παραλάβει την απάντηση, θα την αποκρυπτογραφήσει με το session key και θα επιβεβαιώσει ότι περιέχει την σωστή ώρα αποστολής της αιτήσεως. Η ενέργεια αυτή θα πιστοποιήσει στον client ότι επικοινώνησε με τον αυθεντικό server.

Είναι δυνατόν να προκύψει κάποιο λάθος κατά την επιβεβαίωση της ταυτότητας του client οπότε ο application server ανταποκρίνεται με μήνυμα λάθους που περιλαμβάνει τον είδος του λάθους.

Ακολουθεί απλοποιημένη σχηματική αναπαράσταση της λειτουργίας του Kerberos.



1. as_req: c, v, $time_{exp}$, n
2. as_rep: $\{K_{c,v}, v, time_{exp}, n, ...\}K_c$, $\{T_{c,v}\}K_v$
3. ap_req: $\{ts,ck, K_{subsession}, ...\}K_{c,v}$ $\{T_{c,v}\}K_v$
4. ap_rep: $\{ts\}K_{c,v}$ (optional)

$T_{c,v} = K_{c,v}, c, time_{exp}$ ...

Όπου:

c = ταυτότητα του client,

v = ταυτότητα του application server (αλλιώς και verifier),

n = τυχαίος αριθμός,

$K_{c,v}$ = session key,

K_c = user key,

K_v = server key $T_{c,v}$ = ticket,

ts = timestamp, ck = checksum, $K_{subsession}$ = προαιρετικό κλειδί κρυπτογράφησης (sub-session key)

Ticket Granting Server (TGS)

Η παραπάνω συναλλαγή μηνυμάτων παρουσιάζει το εξής πρόβλημα: χρησιμοποιείται κάθε φορά που ο χρήστης θέλει να επικοινωνήσει με κάποιον application server και πρέπει να εισάγει το κλειδί κωδικό του κάθε φορά που θέλει να αποκρυπτογραφήσει τα διαπιστευτήρια που στέλνονται από τον AS. Μία προφανής λύση του προβλήματος είναι η αποθήκευση του κλειδιού στον client. Αλλά κάτι τέτοιο μπορεί να προσθέσει επιπλέον κινδύνους. Ο εισβολέας που αποκτήσει αντίγραφο του κλειδιού μπορεί να προσποιηθεί ότι είναι ο αυθεντικός χρήστης.

Η επίλυση του προβλήματος γίνεται με την εισαγωγή ενός νέου server, του *Ticket Granting Server (TGS)*. Ο TGS και ο AS είναι ξεχωριστοί server, παρ' όλο που μπορούν να βρίσκονται στο ίδιο μηχάνημα. Ο συνδυασμός τους αποτελεί το *Key Distribution Center (KDC)*. Ο ρόλος του TGS είναι ο εξής: πριν να επικοινωνήσει με κάποιον application server ο client ζητά από τον AS, όπως θα έκανε για οποιοδήποτεapplication server, για τα απαραίτητα διαπιστευτήρια, ώστε να επικοινωνήσει πρώτα με τον TGS. Το ticket που παίρνει λέγεται *ticket-granting ticket (TGT)*. Μετά την παραλαβή του TGT, ζητά κανονικό ticket για τον application server όχι από τον AS, αλλά από τον TGS. Εξάλλου, η απάντηση του TGS δεν κρυπτογραφείται με το user key αλλά με το session key που περιεχόταν στο TGT. Μέσα στην απάντηση από τον TGSπεριέχεται καινούργιο session key που θα χρησιμοποιηθεί για την κρυπτογράφηση της υπόλοιπης ανταλλαγής μηνυμάτων.

Το πλεονέκτημα αυτής της μεθόδου είναι ότι ενώ οι κωδικοί κλειδιά των χρηστών δεν αλλάζουν για μεγάλες χρονικές περιόδους (συνήθως μήνες), ένα session key από το TGT είναι έγκυρο μόνο για λίγες ώρες (τυπικά 8 ώρες). Σαν συνέπεια, η αποθήκευση των TGT δεν δημιουργεί σημαντικό ρίσκο και ο χρήστης χρησιμοποιεί τον κωδικό του μόνο κατά την διάρκεια του login.

Αφού ο client αποκτήσει το νέο session key, η διαδικασία συνεχίζεται όπως πριν, με την αποστολή των διαπιστευτηρίων στον application server.

Ticket Granting Service

Η μορφή του μηνύματος για αίτηση TGT είναι σχεδόν παρόμοια με την μορφή της αίτησης σε έναν AS. Η κυριότερη διαφορά είναι ότι η κρυπτογράφηση της απάντησης του TGS γίνεται με το session key, ενώ της απάντησης του AS γίνεται με το user key.

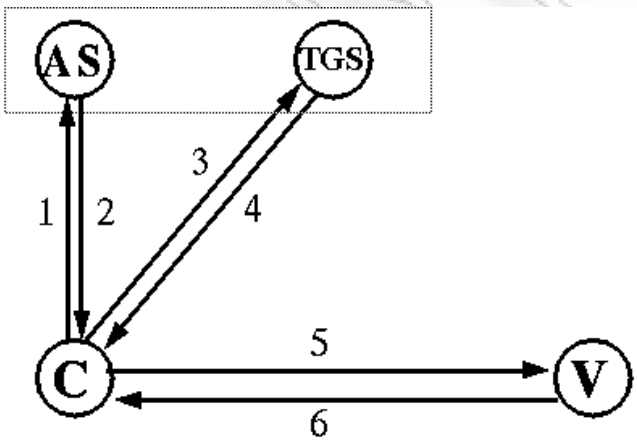
Κατεύθυνση του Μηνύματος	*Τύπος Μηνύματος*	*Περιγραφή Μηνύματος*
1. Client a Ticket Granting Server	KRB_TGS_REQ	TGT Request
2. Client ? Ticket Granting Server	KRB_TGS_REP	TGT Response
	or KRB_ERROR	Failed TGT Request or Other kind of Failure

Η αίτηση στον TGS αποτελείται από πληροφορίες που πιστοποιούν την ταυτότητα του client στον TGS, την ταυτότητα του application server, την ζητούμενη ώρα λήξης του ticket και το TGT κρυπτογραφημένο με το server key του TGS.

Η απάντηση περιέχει τα διαπιστευτήρια για τον application server, κρυπτογραφημένα με το session key που ανέκτησε ο TGS από το TGT. Περιέχεται το καινούργιο session key που θα χρησιμοποιηθεί για την επικοινωνία με τον application server.

Σε περίπτωση λάθους, ο TGS ανταποκρίνεται με μήνυμα λάθους που περιέχει τον κατάλληλο κώδικά λάθους.

Το νέο σχήμα που αναπαριστά την ολοκληρωμένη διαδικασία είναι:



1. as_req: c, tgs, $time_{exp}$, n
2. as_rep: $\{K_{c,tgs}, tgs, time_{exp}, n, ...\}K_c$, $\{T_{c,tgs}\}K_{tgs}$
3. tgs_req: $\{ts, ...\}K_{c,tgs}$ $\{T_{c,tgs}\}K_{tgs}$, v, $time_{exp}$, n
4. tgs_rep: $\{K_{c,v}, v, time_{exp}, n, ...\}K_{c,tgs}$, $\{T_{c,v}\}K_v$
5. ap_req: $\{ts, ck, K_{subsession}, ...\}K_{c,v}$ $\{T_{c,v}\}K_v$
6. ap_rep: $\{ts\}K_{c,v}$ (optional)

Όπου

$T_{c,tgs}$ = ticket-granting ticket

K_{tgs} = TGS server key

$K_{c,tgs}$ = session key

Υπάρχουν δύο τρόποι για την προστασία των δεδομένων στο Kerberos. Με την εφαρμογή κρυπτογράφησης προστατεύεται το απόρρητο της επικοινωνίας, ενώ με την εφαρμογή hash αλγόριθμων διαφυλάσσεται η ακεραιότητα της πληροφορίας. Ο πρώτος τρόπος προστασίας παράγει τα μηνύματα τύπου KRB_SAFE και ο δεύτερος τρόπος παράγει τα μηνύματα τύπου KRB_PRIV.

Δημιουργία Αδιάβλητων Μηνυμάτων (KRB_SAFE)

Όταν ο χρήστης επιθυμεί να μπορεί να ανιχνεύει τυχών τροποποιήσεις των μηνυμάτων που λαμβάνουν χρησιμοποιεί τα μηνύματα τύπου KRP_SAFE. Παράγεται το checksum των δεδομένων του χρήστη μαζί με πληροφορίες ελέγχου, με hash αλγόριθμο, μη αντιστρέψιμο. Το αποτέλεσμα του hash αλγόριθμου κρυπτογραφείται με το session key ή άλλο προσυμφωνημένο κλειδί. Οι πληροφορίες ελέγχου περιλαμβάνουν ένα timestamp και έναν ακέραιο αριθμό ακολουθίας, που χρησιμοποιούνται για προσδιορισμό του μηνύματος και καταπολέμηση του φαινομένου της επίθεσης επανάληψης (replay attack). Η εφαρμογή που λαμβάνει τέτοιο μήνυμα πρώτα ελέγχει την ώρα στο πεδίο timestamp και τον ακέραιο αριθμό ακολουθίας. Αν ο έλεγχος έχει θετικό αποτέλεσμα, υπολογίζεται το checksum των δεδομένων και της πληροφορίας ελέγχου και συγκρίνεται με το παραληφθέν checksum. Σε περίπτωση που η σύγκριση δεν πετύχει, επιστρέφεται στην πηγή του μηνύματος, μήνυμα που προειδοποιεί για την τροποποίηση του μηνύματος.

Δημιουργία Απόρρητων Μηνυμάτων (KRB_PRIV)

Χρησιμοποιείται από χρήστες που θέλουν εξασφαλίσουν την ακεραιότητα των ανταλλασσόμενων δεδομένων. Η εφαρμογή του χρήστη συλλέγει τα δεδομένα μαζί με την πληροφορία ελέγχου και τα κρυπτογραφεί με το sub-session key ή με το session key. Η πληροφορία ελέγχου περιλαμβάνει ένα timestamp και έναν ακέραιο αριθμό ακολουθίας, που χρησιμοποιούνται για προσδιορισμό του μηνύματος και καταπολέμηση του φαινομένου της επίθεσης επανάληψης (replay attack). Όταν μία εφαρμογή λαμβάνει ένα κρυπτογραφημένο μήνυμα πρώτα αποκρυπτογραφεί τα δεδομένα και μετά από επεξεργασίας του αποφαίνεται εάν είναι τροποποιημένα.

Έπειτα ελέγχει την ώρα στο πεδίοtimestamp και τον ακέραιο αριθμό ακολουθίας. Δεδομένου ότι και οι δύο έλεγχοι είναι επιτυχής, το μήνυμα θεωρείται ότι έχει μεταδοθεί με ασφάλεια.

Αλγόριθμοι Κρυπτογράφησης

Τα κρυπτογραφημένα περιεχόμενα παράγονται με την εφαρμογή του καθορισμένου αλγόριθμου στα δεδομένα και σε βοηθητικές πληροφορίες που σχετίζονται με το αλγόριθμο. Οι μηχανισμοί κρυπτογράφησης που χρησιμοποιεί ο Kerberos πρέπει να μπορούν να εγγυηθούν την ακεραιότητα των δεδομένων και συνίστανται μέτρα για την προστασία από επιθέσεις λεξικού *(dictionary attacks)*. Γι' αυτό το σκοπό προστίθονται τα βοηθητικά πεδία και checksum αλγόριθμοι. Οι checksum αλγόριθμοι εφαρμόζονται στα περιεχόμενα προς κρυπτογράφηση και στις βοηθητικές πληροφορίες. Το αποτέλεσμα τους συνοδεύει τα πραγματικά δεδομένα και κρυπτογραφείται μαζί με αυτά.

Σε κατάλληλο πεδίο στην αρχή του μηνύματος και εκτός των κρυπτογραφημένων περιεχομένων, δηλώνεται ο μηχανισμός που χρησιμοποιείται. Εδώ πρέπει να πούμε ότι στις αιτήσεις πιστοποίησης ταυτότητας περιλαμβάνεται πεδίο που ανακοινώνει την προτίμηση του client όσον αναφορά τον μηχανισμό κρυπτογράφησης.

Το Kerberos υποστηρίζει τους εξής μηχανισμούς:

1. DES in CBC mode σε συνδυασμό με τον CRC-32 checksum αλγόριθμο.
2. DES in CBC mode σε συνδυασμό με τον MD4 checksum αλγόριθμο.
3. DES in CBC mode σε συνδυασμό με τον MD5 checksum αλγόριθμο.

Αλγόριθμοι Παραγωγής Checksum

Οι μηχανισμοί παραγωγής checksum μπορούν να διακριθούν σε αυτούς που το αποτέλεσμα των hash αλγόριθμων δεν κρυπτογραφείται και σε αυτούς που χρησιμοποιούνται μαζί με αλγόριθμους κρυπτογράφησης για την παραγωγή κρυπτογραφημένων hash values. Συνιστάται το πρώτο είδος μηχανισμών να εφαρμόζεται μόνο σε περιπτώσεις που ακολουθεί κρυπτογράφηση. Το δεύτερο είδος θεωρείται πιο ασφαλές.

Το Kerberos υποστηρίζει τους παρακάτω μηχανισμούς για την παραγωγή checksum:

1. MD4 checksum algorithm.
2. MD4 σε συνδυασμό με τον DES.

3. MD5 checksum algorithm.
4. MD5 σε συνδυασμό με τον DES.

Μέχρι τώρα θεωρήσαμε ότι το δίκτυο ήταν αρκετά μικρό ώστε ένα Key Distribution Center, αποτελούμενο από έναν Ticket Granting Server και έναν Authentication Server, να είναι αρκετό για να εξυπηρετήσει τις ανάγκες όλων των μηχανών client. Όσο μεγαλώνει το δίκτυο όμως, ο αριθμός των αιτήσεων αυξάνεται και η εξυπηρέτηση γίνεται αργή. Είναι πολλές φορές, λοιπόν, προτιμότερο έως και απαραίτητο να διαχωρίζουμε το δίκτυο σε μικρότερα κομμάτια που καλούνται realms, που το καθένα έχει το δικό του TGS και AS. Συνήθως τα όρια των realms ταυτίζονται με τα όρια των εταιριών, αν και αυτό δεν υποχρεωτικό.

Η διαδικασία *cross-realm authentication* επιτρέπει σε ένα χρήστη να αποδείξει την ταυτότητα του σε έναν application server διαφορετικού realm. Για να επιτευχθεί αυτό ο client ζήτα ένα TGT για τον απομακρυσμένο application server από τον τοπικό AS. Μία τέτοια ενέργεια απαιτεί ο τοπικός AS και ο απομακρυσμένος AS στον οποίο είναι εγγεγραμμένος ο απομακρυσμένος application server να μοιράζονται ένα κλειδί γνωστό ως cross-realm key. Ο client χρησιμοποιεί το αποκτηθέν TGT για να κάνει αίτηση για ticket από τον απομακρυσμένο AS για τον application server του άλλου realm. Ο απομακρυσμένος ASανιχνεύει ότι το TGT έχει εκδοθεί σε διαφορετικό realm, βρίσκει το cross-realm key που μοιράζεται με τον AS του άλλου realm, επαληθεύει την εγκυρότητα του TGT και τέλος εκδίδει ticket και session key για τον client. Μέσα στο ticket περιέχεται έκτος από το όνομα του client αλλά και το όνομα του απομακρυσμένου realm.

Στην 4η έκδοση του Kerberos, ήταν απαραίτητο για έναν AS να μοιράζεται cross-realm κλειδια με όλους τους AS, γεγονός που έκανε αφάνταστα δύσκολη την επικοινωνία. Αρκεί να πούμε ότι για πλήρη διασύνδεση απαιτούνταν ανταλλαγή n^2 κλειδιών όπου n ο αριθμός των realms.

Σε αντίθεση, η 5η έκδοση του Kerberos υποστηρίζει την ιεραρχική διανομή των κλειδιών. Τα realms κατανέμονται ιεραρχικά και κάθε realm μοιράζεται κλειδιά με τα θυγατρικά του realms και με το γονικό του. Για παράδειγμα το realm ISI.EDU μοιράζεται κλειδί με το realm EDU, το οποίο με την σειρά του μοιράζεται κλειδιά με τα MIT.EDU, USC.EDU και WASHINGTON.EDU. Η πιστοποίηση της ταυτότητας ενόςclient στο realm ISI.EDU σε ένα application server στο realm MIT.EDU γίνεται με την απόκτηση ενός TGT από

τον AS στο ISI.EDU για το EDU, με χρήση αυτού του TGT για την απόκτηση νέου TGT από τον ASτου EDU για τον AS του MIT.EDU και τέλος έχουμε την αποστολή αίτησης στον Application server του MIT.EDU ζητώντας ticket για επικοινωνία με τον AS. Η λίστα όλων των realms τα οποία έχει διασχίσει η αίτηση του client καταγράφονται στο τελικό ticket και ο authentication server του απομακρυσμένου realm πραγματοποιεί την τελική απόφαση για το κατά πόσο μπορεί να εμπιστευτεί το μονοπάτι που ακολουθήθηκε. Η επιλογή μικρότερων διαδρομών υποστηρίζεται από το μοντέλο, καθ' ότι μπορούν να βελτιώσουν την απόδοση της διαδικασίας.

Το Kerberos δεν έχει την δυνατότητα να προστατέψει ένα δίκτυο από κάθε είδους απειλή. Λειτουργεί βάσει συγκεκριμένων υποθέσεων όσον αναφορά την υποκείμενη δικτυακή δομή.

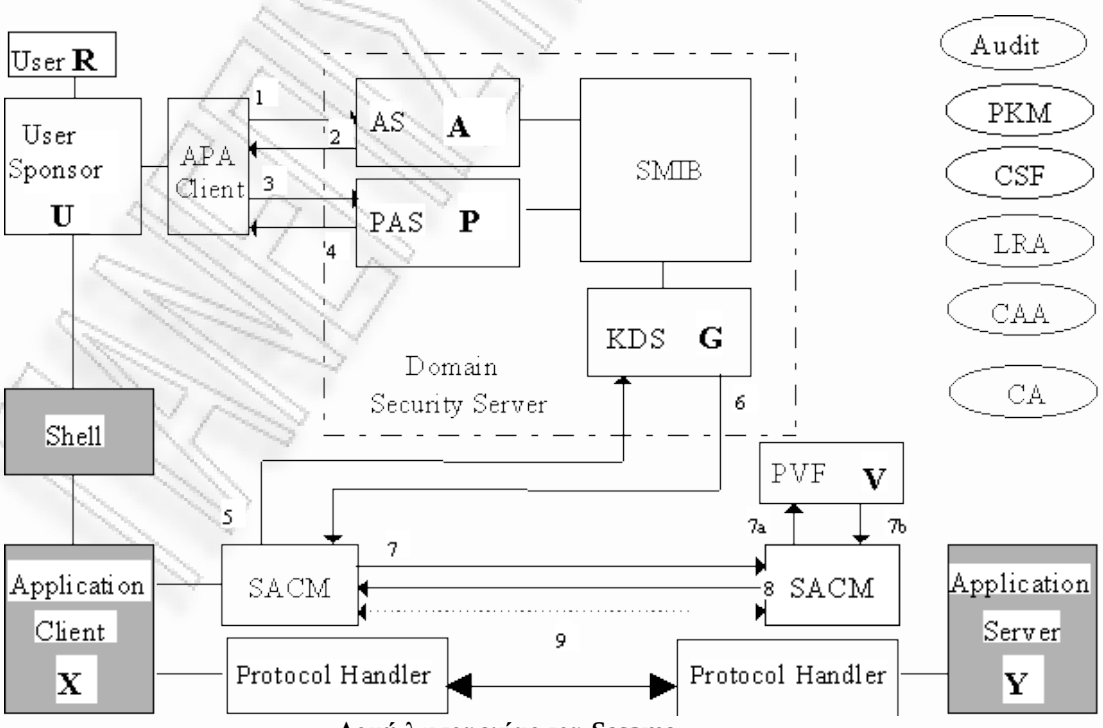
1. Επιθέσεις του τύπου άρνησης εξυπηρέτησης (denial of service attack) δεν μπορούν να αντιμετωπιστούν με το Kerberos. Ένας εισβολέας μπορεί εκμεταλλευόμενος τις αδυναμίες του συστήματος να αποτρέψει έναν server από το να συμμετέχει στα κανονικά βήματα πιστοποίησης. Η ανίχνευση και η επιδιόρθωση τέτοιων καταστάσεων αφήνεται στα χέρια των διαχειριστών και των χρηστών.
2. Οι χρήστες πρέπει να κρατούν τους κωδικούς τους μυστικούς. Το Kerberos δεν είναι σε θέση να προστατέψει το δίκτυο από ασυνείδητους χρήστες που μοιράζουν τους κωδικούς τους ή που δεν είναι αρκετά προσεκτικοί για να τον κρατήσουν κρυφό.
3. Επιθέσεις που βασίζονται στην πρόβλεψη εύκολων κωδικών (password guessing attack) δεν αντιμετωπίζονται από τον Kerberos. Ένας εισβολέας με χρήση ενός λεξικού, μπορεί εύκολα να "σπάσει" μικρούς και εύκολους κωδικούς που αποτελούνται από λέξεις που μπορούν να βρεθούν σε λεξικό.
4. Κάθε μηχανή του δικτύου πρέπει να έχει ένα καλά ρυθμισμένο ρολόι. Μηχανές με ρυθμίσεις ώρας που διαφέρουν σημαντικά (πάνω από 5 λεπτά) μπορεί να δημιουργήσουν πρόβλημα στην πιστοποίηση των timestamps που εμπεριέχονται στα μηνύματα. Έτσι, ένας εισβολέας εκμεταλλευόμενος αυτή την αδυναμία μπορεί να πραγματοποιήσει επίθεση επανάληψης (replay attack). Ή ακόμα βρίσκοντας τον απαραίτητο χρόνο, να σπάσει αδύναμους κωδικούς χρηστών.

1.4.2 Σύστημα Sesame

Το Sesame είναι το Ευρωπαϊκό Σύστημα Ασφαλείας για εφαρμογές που λειτουργούν σε ανομοιογενή υπολογιστικά περιβάλλοντα και δεν αποτελεί εμπορικό προϊόν. Προσφέρει βασικές λειτουργίες ασφαλείας με τις οποίες οι κατασκευαστές υλοποιούν τα τελικά προϊόντα πληροφορικής. Ως τέτοιο, έχει πολλές ομοιότητες με το σύστημα αυθεντικοποίησης Kerberos. Χρησιμοποιεί τις δομές δεδομένων και επιπλέον είναι προσβάσιμο από το πρωτόκολλο 5 του Kerberos. Η τρέχουσα έκδοση του Sesame είναι η 4, ενώ η κύρια αλλαγή από την προηγούμενη έκδοση είναι ότι ολόκληρος ο κώδικας του Kerberos 5 αντικαταστάθηκε από τον κώδικα του Sesame.

Η αρχιτεκτονική του Sesame αποτελείται από τρεις server:

- Εξυπηρετητής αυθεντικοποίησης (Server Authentication – AS): Αποτελεί κεντρικό σημείο της υποδομής αυθεντικοποίησης του χρήστη. Αρχικά ο εκκινητής της διαδικασίας συνδέεται με τον εξυπηρετητή αυθεντικοποίησης για να προχωρήσει.
- Εξυπηρετητής εκχώρησης δικαιωμάτων (Privilege Attribute Server – PAC): Επαληθεύει τα δικαιώματα πρόσβασης του εκκινητή και παράγει ένα πιστοποιητικό προνομίων.
- Εξυπηρετητής εκχώρησης κλειδιών (Key Distribution Server – KDS): Όταν ο εκκινητής επιλέξει τη εφαρμογή που θέλει να συνδεθεί, τότε του απονέμονται πληροφορίες για τα κλειδιά.



Δομή λειτουργίας του Sesame

2 Τεχνολογίες υποδομής στα ΠΣ στην Ελλάδα

Αρχικά θα κάνουμε μία εισαγωγή στις βασικές έννοιες που είναι απαραίτητες για την κατανόηση της αυθεντικοποίησης και της ασφάλειας των Πληροφοριακών Συστημάτων (ΠΣ) καθώς και τον τρόπο με τον οποίο λειτουργούν και διαχειρίζονται δεδομένα τα ΠΣ που χρησιμοποιούνται στις υπηρεσίες ηλεκτρονικής διακυβέρνησης στην Ελλάδα.

2.1 XML

Η γλώσσα σήμανσης GML (Generalized Markup Language) δημιουργήθηκε από την IBM με σκοπό να λύσει το πρόβλημα της κωδικοποίησης εγγράφων για τη χρήση τους σε διάφορα υποσυστήματα. Τα έγγραφα που ήταν κωδικοποιημένα με αυτή τη γλώσσα μπορούσαν να διαμορφωθούν, να αναζητηθούν και να τροποποιηθούν από διάφορα λογισμικά και προγράμματα λόγω της χρήσης ετικετών (tags).

Εμπνευσμένο από την επιτυχία της GML, το Ινστιτούτο ANSI (American National Standards Institute) δημιούργησε την SGML. Η χρήση της διαδόθηκε ταχύτατα και σύντομα αναγνωρίστε ως στάνταρντ από τον διεθνή οργανισμό σχετικά με τα πρότυπα (ISO).

Στα μέσα της δεκαετίας του ’90, το World Wide Web Consortium (W3C) δημιούργησε την XML, μία γλώσσα που θα συνδυάζει την ευελιξία της SGML, αλλά θα έχει σαφώς μικρότερο συντακτικό και θα είναι εύκολη στην εκμάθηση όπως η HTML.

Οι αυστηροί κανόνες σύνταξης της XML και η ανάγκη ώστε να διαχωριστεί το περιεχόμενο από την εμφάνιση ενός δικτυακού τόπου στο σύγχρονο διαδίκτυο, οδήγησαν το W3C ώστε να ξαναγράψει την HTML σε XML και να προκύψει η XHTML.

Οι κανόνες σύνταξης ενός εγγράφου XML περιλαμβάνονται στο DTD (Document Type Definition). Δυστυχώς τα DTD περιγράφουν πως δομούνται τα στοιχεία σε ένα έγγραφο, αλλά δεν περιγράφουν καθόλου το περιεχόμενο των στοιχείων. Για παράδειγμα έχουμε το παρακάτω έγγραφο XML:

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE store SYSTEM "example.dtd">
 <store>
   <account>
     <username>nikma</username>
     <city>maounis</city>
     <realname>Nikos</realname>
   </account>
   <account>
     <username>Johnny</username>
```

```
      <city>Thessaloniki</city>
      <realname>John</realname>
    </account>
  </store>
```

Το DTD για το παραπάνω XML έγγραφο έχει ονομαστεί example.dtd περιέχει τα εξής:

```
<!ELEMENT store (account)*>
<!ELEMENT account (username, city, realname)>
<!ELEMENT username (#PCDATA)>
<!ELEMENT city (#PCDATA)>
<!ELEMENT realname (#PCDATA)>
```

Το πρόβλημα είναι ότι ο χρήστης nikma έχει δώσει ως πόλη τη λέξη maounis, πράγμα το οποίο δεν είναι φυσικά έγκυρο. Το DTD αρχείο περιέχει απλώς πληροφορίες για τα στοιχεία που πρέπει να περιέχονται στο έγγραφο και για το τύπο δεδομένων τους (λέξεις, αριθμοί) και τίποτα σχετικά με την εγκυρότητά τους.

Το πρόβλημα λύνεται με τη χρήση Schemas τα οποία παρέχουν έλεγχο για τις τιμές και την εγκυρότητα των στοιχείων ενός XML εγγράφου. Για παράδειγμα αν χρειάζεται να περιγράψουμε ένα στοιχείο ενός εγγράφου, το οποίο θα δέχεται ημερομηνία, πρέπει να το καθορίσουμε στο schema μας ως εξής:

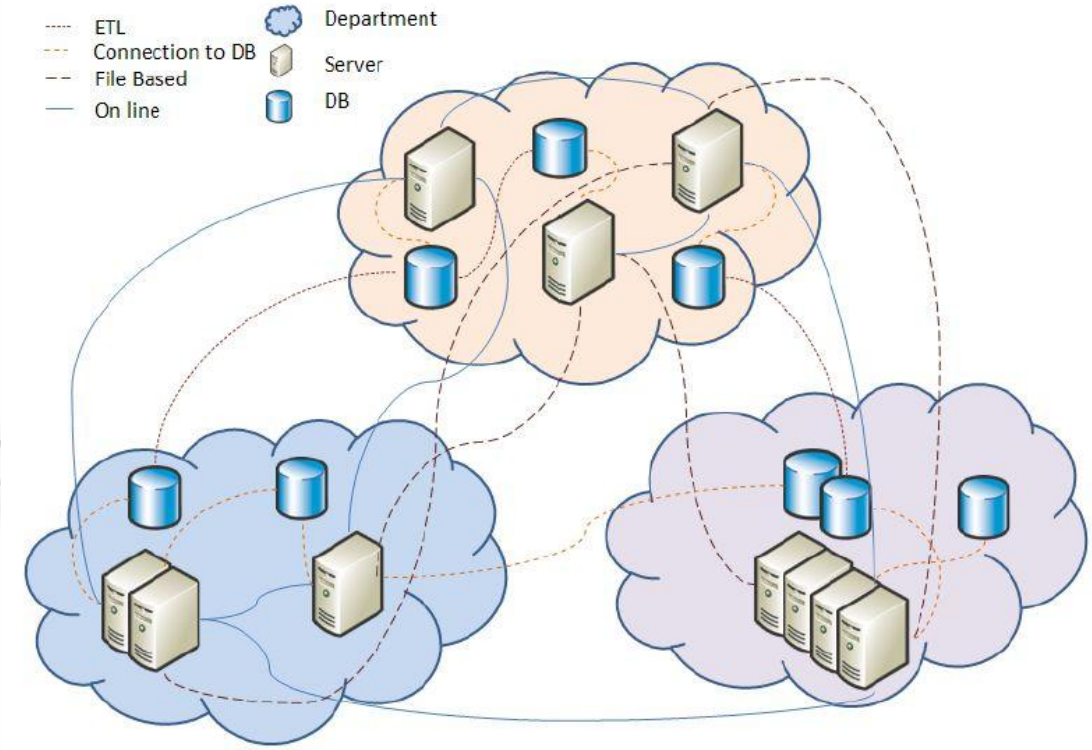
```
<xs:simpleType name="month"
  <xs:restriction base=”xs:integer”>
     <xs:minInclusive value=”1”/>
     <xs:maxInclusive value=”12”/>
  </xs:restriction>
</xs:simpleType>
```

Ο παραπάνω κώδικας καθορίζει ότι το πεδίο του μήνα πρέπει να έχει τιμή από 1 έως 12. Όπως γίνεται κατανοητό τα schemas είναι αρκετά πιο ευέλικτα από τα DTDs για αυτό και χρησιμοποιούνται πλέον περισσότερο. Οι γλώσσες που χρησιμοποιούνται στις πολιτικές διαχείρισης ασφάλειας (SAML και XACML), βασίζονται στην XML (έχουν δημιουργηθεί με τη χρήση XML) χρησιμοποιούν Schemas για να επικυρώσουν τα δεδομένα των εγγράφων και των δηλώσεων. Μία άλλη γνωστή τεχνολογία του διαδικτύου που βασίζεται στην XML και την χρησιμοποιούμε καθημερινά είναι τα RSS Feeds, τα οποία επιτρέπουν την ανάγνωση και τη προβολή του περιεχομένου ενός δικτυακού τόπου, χωρίς ο χρήστης να χρειάζεται να επισκεφτεί με τον browser του το συγκεκριμένο δικτυακό τόπο.

2.2 SOA

Με το πέρασμα των χρόνων και τη διείσδυση της τεχνολογίας στους οργανισμούς, τα πληροφοριακά συστήματα (IT Systems) άρχισαν να γίνονται όλο και πιο πολύπλοκα. Πολλές πλατφόρμες αποτελούν πλέον μέρος ενός σύγχρονου πληροφοριακού συστήματος (για παράδειγμα Windows, Linux, Mac) καθώς και προγράμματα τα οποία εκτελούνται στα συστήματα αυτά και έχουν γραφτεί σε διαφορετικές γλώσσες προγραμματισμού (για παράδειγμα Java, C++, C#). Η πολυπλοκότητα (φαίνεται στην εικόνα 1) αυτή μειώνει την παραγωγικότητα των οργανισμών, αυξάνει το κόστος συντήρησης και λειτουργίας του πληροφοριακού συστήματος και δεν επιτρέπει την εύκολη μεταφορά της τεχνολογίας. Συνοπτικά τα προβλήματα και οι περιορισμοί που προκύπτουν είναι:

- Οι εφαρμογές που χρησιμοποιούνται εντός ενός οργανισμού έχουν αναπτυχθεί ανεξάρτητα η μία από την άλλη με αποτέλεσμα την περιορισμένη λειτουργικότητα.
- Οι διαφορές από πλατφόρμα σε πλατφόρμα, μεταξύ γλωσσών προγραμματισμού και μεταξύ πρωτοκόλλων, δημιουργούν εμπόδια, τα οποία είναι δύσκολο να ξεπεραστούν.
- Οι τεχνολογίες ασφάλειας βασίζονται αποκλειστικά στα όρια του οργανισμού και καθιστούν δύσκολη την συνεργασία του οργανισμού με άλλους οργανισμούς.



Η πολυπλοκότητα ενός σύγχρονου πληροφοριακού συστήματος

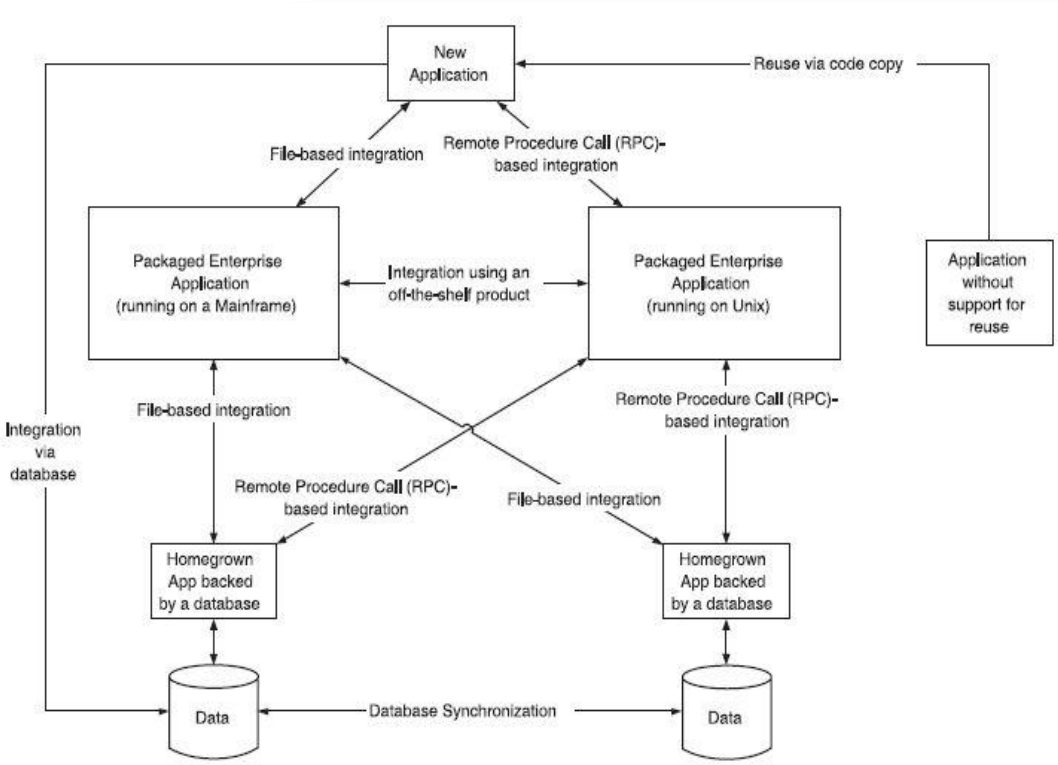
Όλα αυτά τα προβλήματα οδήγησαν στην ανάγκη για μία νέα τεχνολογία πάνω στην οποία θα βασίζονται τα σύγχρονα πληροφοριακά συστήματα, η οποία θα ξεπερνάει τα εμπόδια που αναφέραμε πιο πάνω. Η τεχνολογία που φαίνεται να το πετυχαίνει ονομάζεται SOA (Service Oriented Architecture) και φιλοδοξεί να επαναφέρει στους οργανισμούς την ευελιξία που χρειάζονται και να μειώσει το κόστος υλοποίησης και συντήρησης των συστημάτων τους. Συνοπτικά, οι στόχοι της τεχνολογίας SOA είναι οι εξής:

- Οι εφαρμογές (applications) πρέπει να υλοποιούνται με γνώμονα ότι οι δυνατότητές τους θα χρησιμοποιηθούν από άλλες εφαρμογές ώστε να καθίσταται δυνατή η ταυτόχρονη χρήση υπηρεσιών που προσφέρονται από διαφορετικές εφαρμογές.
- Οι τεχνολογικές διαφορές μεταξύ γλωσσών προγραμματισμού και πλατφορμών δεν πρέπει να παίζει κανένα ρόλο. Η δυνατότητα να συνεργάζονται συστήματα ανεξαρτήτως τεχνολογικής υποδομής (interoperability) πρέπει να είναι ο βασικός στόχος.
- Υιοθέτηση ανοιχτών προτύπων για εύκολη μεταφερσιμότητα της τεχνολογίας και εύκολη συνεργασία ανεξάρτητων συστημάτων.
- Πρέπει να δίνεται προσοχή στη διαχείριση των συστημάτων, ώστε τα πλεονεκτήματα που παρουσιάζονται στα προηγούμενα σημεία να μην οδηγήσουν στο χάος.

2.3 Web services, WSDL και SOAP

2.3.1 Web services

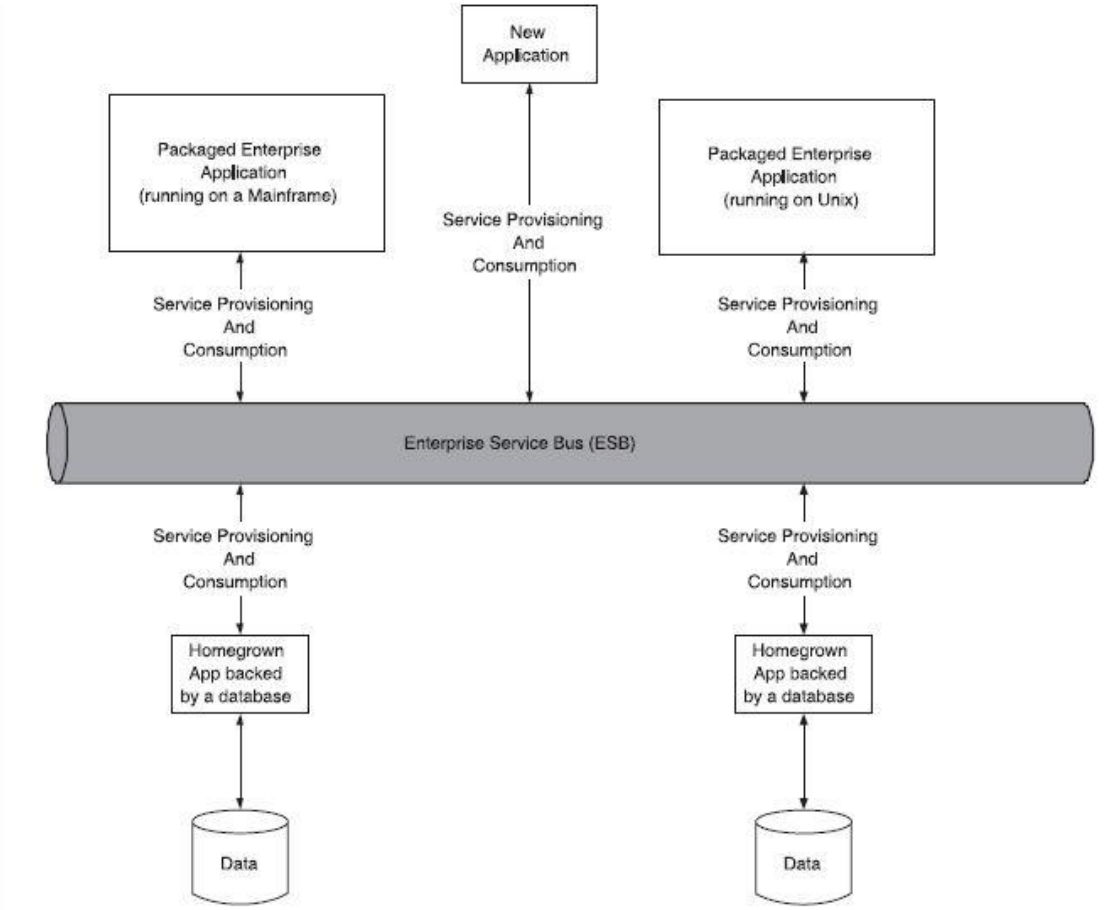
Κατά κανόνα οι εφαρμογές σχεδιάζονται για χρήση από ανθρώπους. Τελευταία με την ραγδαία εξάπλωση των πληροφοριακών συστημάτων και τις εργασίες που αυτά αναλαμβάνουν να διεκπεραιώσουν ο κανόνας αυτός παύει να ισχύει. Οι εφαρμογές πλέον εξάγουν αποτελέσματα, τα οποία χρειάζεται να χρησιμοποιηθούν από άλλες εφαρμογές χωρίς να μεσολαβήσει ο ανθρώπινος παράγοντας. Όταν ένας οργανισμός ήθελε να ενοποιήσει τις δυνατότητες κάποιον συγκεκριμένων εφαρμογών, η λύση ήταν η χρησιμοποίηση ενός νέου προγράμματος που θα περιέχει τις συγκεκριμένες εφαρμογές (αντιγραφή κώδικα ουσιαστικά) κάτι το οποίο είναι εξαιρετικά χρονοβόρο και κοστίζει. Η παρακάτω εικόνα δείχνει ακριβώς αυτή τη χρονοβόρα προσέγγιση.



Σε έναν τυπικό οργανισμό, οι εφαρμογές προορίζονται για τους τελικούς χρήστες και οι τρόποι για τη συνεργασία δύο ή περισσότερων εφαρμογών είναι ad hoc (π.χ. βάσεις δεδομένων, αρχεία, RPC).

Η τεχνολογία SOA λύνει αυτό το πρόβλημα, διότι αντιμετωπίζει τα πληροφοριακά συστήματα σαν ομάδες υπηρεσιών (web services) και όχι σαν ομάδες εφαρμογών. Ως web service ή αλλιώς υπηρεσία, εννοούμε οτιδήποτε είναι δυνατό να χρησιμοποιηθεί από άλλες εφαρμογές ή άλλες υπηρεσίες. Για παράδειγμα, η έξοδος ενός προγράμματος είναι είσοδος σε ένα άλλο άσχετα με την προέλευση, την πλατφόρμα πάνω στην οποία εκτελείται ή τη γλώσσα προγραμματισμού στην οποία γράφτηκε.

Η σύγχρονη προσέγγιση της τεχνολογίας SOA λέει ότι ο σύγχρονος οργανισμός αντί να λειτουργεί με ad hoc όπως φαίνεται στην εικόνα παραπάνω, κάνει χρήση ESB (Enterprise Service Bus) όπως φαίνεται στην εικόνα παρακάτω. Ένας δίαυλος ESB «συγκεντρώνει» όλες τις δυνατότητες που παρέχουν οι εφαρμογές που χρησιμοποιούνται εντός του οργανισμού και τις διανέμει ως υπηρεσίες (web services). Ο οργανισμός δηλαδή λειτουργεί «καταναλώνοντας» web services και όχι κάνοντας χρήση μεμονωμένων εφαρμογών με τους περιορισμούς που αυτό συνεπάγεται. Τα web services περιγράφονται με τη γλώσσα WSDL (Web Services Description Language).



Στη θέση μηχανισμών ad hoc, με τη χρήση SOA, οι εφαρμογές παρέχουν υπηρεσίες για άλλες εφαρμογές. Μερικές εφαρμογές είναι μόνο καταναλωτές. Η διαχείριση των υπηρεσιών γίνεται από τον δίαυλο ESB.

2.3.2 WSDL

Η γλώσσα WSDL (Web Services Description Language) περιγράφει τις εξής λεπτομέρειες για τα web services:

- Τι λειτουργίες επιτελεί η υπηρεσία (web service)
- Ποια πρωτόκολλα και ποια διαμόρφωση χρησιμοποιείται για τις λειτουργίες αυτές (συνήθως χρησιμοποιείται η XML σε συνδυασμό με το πρωτόκολλο SOAP)
- Η τοποθεσία (διεύθυνση) της υπηρεσίας

Η περιγραφή ενός web service είναι πολύ σημαντική διότι παρέχει πληροφορίες σχετικά με την υπηρεσία στους πελάτες (clients).Ένα τυπικό έγγραφο WSDL έχει δομή παρόμοια με ένα τυπικό έγγραφο XML σαν αυτά που περιγράψαμε στην ενότητα 1.1. Ακολουθεί ένα παράδειγμα εγγράφου WSDL:

```
<?xml version="1.0"?>
<definitions name="StockQuote"

targetNamespace="http://example.com/stockquote/definitions"
          xmlns:tns="http://example.com/stockquote/definitions"
          xmlns:xsd1="http://example.com/stockquote/schemas"
          xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
          xmlns="http://schemas.xmlsoap.org/wsdl/">

   <import namespace="http://example.com/stockquote/schemas"
     location="http://example.com/stockquote/stockquote.xsd"/>

    <message name="GetLastTradePriceInput">
        <part name="body" element="xsd1:TradePriceRequest"/>
    </message>

    <message name="GetLastTradePriceOutput">
        <part name="body" element="xsd1:TradePrice"/>
    </message>

    <portType name="StockQuotePortType">
        <operation name="GetLastTradePrice">
           <input message="tns:GetLastTradePriceInput"/>
           <output message="tns:GetLastTradePriceOutput"/>
        </operation>
    </portType>
</definitions>
```

Το παράδειγμα αναφέρεται σε μία υπηρεσία ενημέρωσης για τιμές και αγοραπωλησίες μετοχών. Μέσω της WSDL περιγράφονται και οι πόρτες που θα χρησιμοποιήσει μία υπηρεσία με κώδικα σαν τον παρακάτω:

```
<wsdl:service name="BrokerageService">
      <wsdl:port binding="impl:example1SoapBinding" name="example1">
         <wsdlsoap:address
location="http://localhost:8080/axis/services/example1"/>
      </wsdl:port>
   </wsdl:service>
```

2.3.3 SOAP

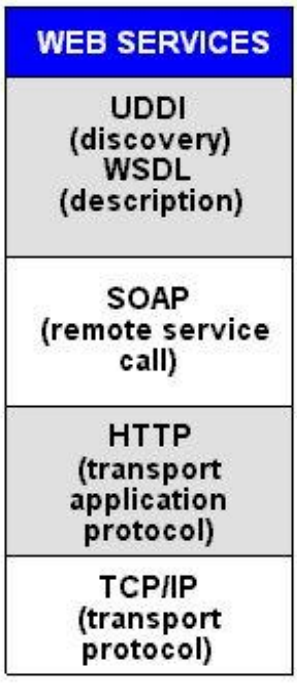
Το SOAP είναι το βασικό πρωτόκολλο για την χρήση web services. Το SOAP παρέχει ένα μοντέλο για την ανταλλαγή μηνυμάτων μεταξύ εφαρμογών. Η εικόνα 4 δείχνει τη θέση του SOAP στην ιεραρχία πρωτοκόλλων για τη χρήση υπηρεσιών.

Το μοντέλο που παρέχει το SOAP έχει τα εξής χαρακτηριστικά:

- Ένα SOAP μήνυμα είναι μία μεταφορά από ένα σημείο σε ένα άλλο. Μπορούν να συνδυαστούν πολλές μεταφορές ώστε να έχουμε request/response μεταξύ των δύο σημείων που ανταλλάζουν τα μηνύματα.

- Κάθε μήνυμα SOAP δημιουργείται από μία εφαρμογή και έχει ένα στάνταρ XML φάκελο (envelope). Το envelope επιτρέπει στις εφαρμογές να βλέπουν το μεταφερόμενο μήνυμα καθώς και τη κωδικοποίησή του.
- Όλα τα λάθη διορθώνονται με τη χρήση του μηχανισμού λαθών του SOAP (SOAP Fault Mechanism).
- Οι εφαρμογές συντάσσουν τα μηνύματά τους με βάση τους κανόνες που καθορίζει το SOAP.
- Τα μηνύματα κωδικοποιούνται με βάση την κωδικοποίηση που ορίζει το SOAP.

Όπως φαίνεται και στην εικόνα 4, το SOAP είναι ένα πρωτόκολλο υψηλού επιπέδου και βρίσκεται πάνω από το επίπεδο εφαρμογής που βρίσκεται το HTTP (Hyper Text Transfer Protocol) στην ιεραρχία πρωτοκόλλων. Τα μηνύματα SOAP μπορούν να μεταφερθούν σαν πρόσθετο σε οποιαδήποτε μεταφορά εφαρμογής, για παράδειγμα με τη χρήση του Java Messaging Service ή ακόμα και με το FTP (File transfer protocol).



Ιεραρχία πρωτοκόλλων στα web services

Τα μηνύματα SOAP έχουν δομή XML εγγράφου με την ακόλουθη δομή:

```
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Header>
       ...
   </soapenv:Header>
   <soapenv:Body>
       ...
   </soapenv:Body>
</soapenv:Envelope>
```

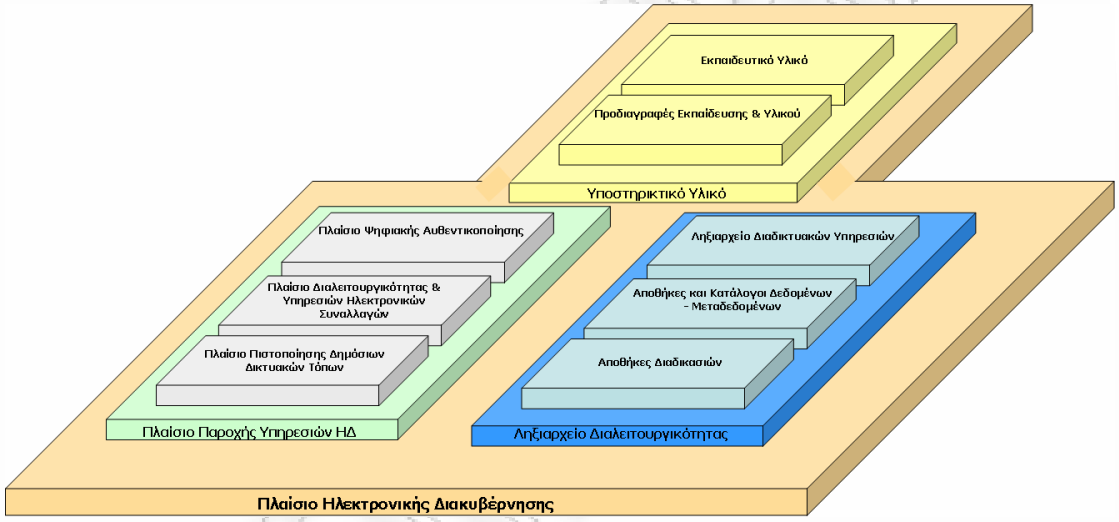
Το βασικό στοιχείο σε ένα μήνυμα SOAP είναι πάντα το στοιχείο envelope που ακολουθείται από ένα χώρο ονομάτων που καθορίζεται από την εκάστοτε προδιαγραφή του SOAP. Το στοιχείο envelope αποτελείται από ένα στοιχείο header το οποίο είναι προαιρετικό και από το στοιχείο body που είναι υποχρεωτικό. Το στοιχείο header μπορεί να περιλαμβάνει μία ή περισσότερες καταχωρήσεις σχετικές με την επέκταση του SOAP (για παράδειγμα δηλώσεις ασφαλείας που επεκτείνουν το SOAP στον τομέα της ασφάλειας). Το στοιχείο body περιέχει τα μηνύματα των εφαρμογών. Το body δεν μπορεί να περιλαμβάνει ελεύθερο κείμενο, αλλά στοιχεία XML (το κείμενο δηλαδή πρέπει να βρίσκεται σε μορφή XML). Το πώς θα ερμηνευτεί ένα μήνυμα SOAP εξαρτάται από την εφαρμογή που θα το χρησιμοποιήσει.

2.4 Πολιτικές ασφάλειας

Μία πολιτική ασφάλειας περιλαμβάνει το σκοπό και τους στόχους της ασφάλειας καθώς επίσης και οδηγίες, διαδικασίες, ρόλους, κανόνες και υπευθυνότητες που αφορούν την προστασία των πληροφοριακών συστημάτων ενός οργανισμού. Η πολιτική ασφάλειας πρέπει να είναι γνωστή στους προγραμματιστές ενός οργανισμού και αυτοί να τις λαμβάνουν υπόψη και σε συνδυασμό με τους πόρους του συστήματος να τις ενσωματώνουν κατάλληλα στο λογισμικό που δημιουργούν.

3 Αυθεντικοποίηση και Ηλεκτρονική διακυβέρνηση στην Ελλάδα

Τα τελευταία χρόνια η χώρα μας έχει κάνει μεγάλα βήματα στο θέμα της ηλεκτρονικής διακυβέρνησης με πάρα πολλές δημόσιες υπηρεσίες να παρέχουν ηλεκτρονικές υπηρεσίες, από το TAXISnet μέχρι τη στρατολογία. Η αρχιτεκτονική της ηλεκτρονικής διακυβέρνησης στη χώρα μας φαίνεται στο παρακάτω σχήμα.



Το πλαίσιο πιστοποίησης δημόσιων διαδικτυακών τόπων καθώς και τις τεχνολογίες που χρησιμοποιούνται στις κρατικές e-υπηρεσίες τα εξηγήσαμε στην εισαγωγή. Ας δούμε τώρα αναλυτικά το πλαίσιο ψηφιακής αυθεντικοποίησης στη χώρα μας.

Οι βασικές έννοιες του ΠΨΑ συνοψίζονται στον παρακάτω πίνακα:

Βασική έννοια	Περιγραφή
Πλαίσιο Ψηφιακής Αυθεντικοποίησης	Ως Πλαίσιο Ψηφιακής Αυθεντικοποίησης, υπό το πρίσμα του Πλαισίου Ηλεκτρονικής Διακυβέρνησης, θεωρείται το σύνολο των απαιτουμένων διαδικασιών αναφορικά με (α) την εγγραφή (β) την ταυτοποίηση και (γ) την αυθεντικοποίηση που πρέπει να ακολουθούνται από τις εμπλεκόμενες οντότητες για την επίτευξη του επιθυμητού επιπέδου ασφάλειας και εμπιστοσύνης μεταξύ των συναλλασσομένων οντοτήτων.
Απαιτήσεις Ασφάλειας	Ως απαιτήσεις ασφάλειας θεωρούνται οι ιδιότητες-χαρακτηριστικά ασφάλειας (Ιδιωτικότητα, Εμπιστευτικότητα, Ακεραιότητα, Αυθεντικοποίηση), οι οποίες απαιτείται να διασφαλίζονται κατά την παροχή μιας ηλεκτρονικής υπηρεσίας.
Ιδιωτικότητα	Ως ιδιωτικότητα νοείται η μη αποκάλυψη προσωπικών πληροφοριών σε μη εξουσιοδοτημένες οντότητες.
Εμπιστευτικότητα	Ως Εμπιστευτικότητα θεωρείται η διαδικασία διασφάλισης μη εξουσιοδοτημένης αποκάλυψης των δεδομένων που αξιοποιούνται κατά τη διεκπεραίωση μιας συναλλαγής.
Ακεραιότητα Δεδομένων	Ως ακεραιότητα των δεδομένων θεωρείται η διαδικασία διασφάλισης μη εξουσιοδοτημένης τροποποίησης των δεδομένων που αξιοποιούνται κατά τη διεκπεραίωση μιας συναλλαγής.
Αυθεντικοποίηση	Ως αυθεντικοποίηση θεωρείται η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης. Συγκεκριμένα, κατά τη διαδικασία αυθεντικοποίησης αναγνωρίζεται και επιβεβαιώνεται η ορθότητα της ταυτότητας ενός χρήστη ή κάποιων χαρακτηριστικών της.
Διαπιστευτήρια-Μηχανισμός Αυθεντικοποίησης	Ως διαπιστευτήρια νοούνται τα εχέγγυα που παρουσιάζει μια οντότητα προκειμένου να αποδείξει τη γνησιότητα ενός ισχυρισμού και συγκεκριμένα της ταυτότητας ή του ρόλου της.
Επίπεδο Εμπιστοσύνης	Η «εμπιστοσύνη» ερμηνεύεται ως «η πίστη στην αξιοπιστία, εντιμότητα, αξία ή ικανότητα κάποιας οντότητας». Υπό το πρίσμα του ΠΨΑ, ως επίπεδο εμπιστοσύνης θεωρείται ο βαθμός βεβαιότητας που έχει μια υπηρεσία για την ορθότητα τόσο της ταυτότητας της ηλεκτρονικής οντότητας που επιθυμεί να διεκπεραιώσει μια συναλλαγή στο πλαίσιο μιας ηλεκτρονικής υπηρεσίας, όσο και των δεδομένων που απαιτούνται για την επιτυχή ολοκλήρωση της συναλλαγής λαμβάνοντας υπόψη και την κρισιμότητα των δεδομένων αυτών (απλά, προσωπικά, ευαίσθητα).
Εγγραφή Οντότητας	Με τον όρο «εγγραφή μιας οντότητας» σε μια υπηρεσία ορίζεται το σύνολο των διαδικασιών δια των οποίων η οντότητα εκδηλώνει ενδιαφέρον χρήσης μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας και παρέχει τα απαιτούμενα στοιχεία για τη λήψη του δικαιώματος αυτού.
Επίπεδο Εγγραφής	Ως επίπεδο εγγραφής θεωρείται η ένταξη σε συγκεκριμένο σύνολο διαδικασιών που ακολουθούνται για τη συλλογή των απαιτούμενων στοιχείων και την πιστοποίηση της ορθότητας, έχοντας ως πεδίο αναφοράς το επίπεδο εμπιστοσύνης που απαιτείται για την παροχή μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας.

Βασική έννοια	Περιγραφή
Επίπεδο Αυθεντικοποίησης	Ως επίπεδο αυθεντικοποίησης θεωρείται η ένταξη μιας οντότητας σε συγκεκριμένου τύπου διαπιστευτήρια για την τεκμηρίωση της εγκυρότητας της ταυτότητάς της, με βάση το επίπεδο εμπιστοσύνης που απαιτείται να διασφαλιστεί για την παροχή μιας συγκεκριμένης ηλεκτρονικής υπηρεσίας.
Ηλεκτρονική Ταυτότητα	Με τον όρο «ηλεκτρονική ταυτότητα» νοείται η ταυτότητα που αξιοποιεί ο χρήστης για την αναγνώρισή του σε μια ηλεκτρονική υπηρεσία.
Ταυτοποίηση	Με τον όρο ταυτοποίηση, υπό το πρίσμα του ΠΨΑ, νοείται η διαδικασία δήλωσης ταυτότητας από το χρήστη στις υπηρεσίες ηλεκτρονικής διακυβέρνησης.
Απλά Δεδομένα	Ως απλά δεδομένα, υπό το πρίσμα του ΠΨΑ, θεωρούνται πληροφορίες που είναι δημοσίως προσπελάσιμες και δεν περιέχονται σε αυτές προσωπικά δεδομένα.
Προσωπικά Δεδομένα	Ως δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα, υπό το πρίσμα του ΠΨΑ, θεωρούνται πληροφορίες που αναφέρονται στο υποκείμενο των δεδομένων, δηλαδή στο φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική (άρθρο 2α σε συνδυασμό με άρθρο 2γ του ν. 2472/97). Δε λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων.
Ευαίσθητα Δεδομένα	Ως ευαίσθητα προσωπικά δεδομένα, προσδιορίζονται στο νόμο (άρθρο 2β του ν. 2472/97, όπως ισχύει) τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.
Αρχή Εγγραφής	Η Αρχή Εγγραφής ή καταχώρισης αποτελεί την οντότητα που είναι υπεύθυνη για τη συλλογή των απαιτούμενων στοιχείων και την πιστοποίηση της ταυτότητας μιας οντότητας που αιτείται εγγραφής σε κάποια ηλεκτρονική υπηρεσία.
Αρχή Πιστοποίησης	Η Αρχή Πιστοποίησης αποτελεί την οντότητα εκείνη που αναλαμβάνει την τεχνική διαχείριση των ψηφιακών πιστοποιητικών για ολόκληρο τον κύκλο ζωή τους.

3.1 Πλαίσιο Ηλεκτρονικής Διακυβέρνησης

Το Πλαίσιο Ηλεκτρονικής Διακυβέρνησης περιλαμβάνει τρία επιμέρους πλαίσια, καθένα από τα οποία ρυθμίζει συγκεκριμένες πτυχές της Ηλεκτρονικής Διακυβέρνησης:

- Το Πλαίσιο Πιστοποίησης Δημόσιων Διαδικτυακών Τόπων (ΠΠ-ΔΔΤ)
- Το Πλαίσιο Διαλειτουργικότητας & Υπηρεσιών Ηλεκτρονικών Συναλλαγών (ΠΔ&ΥΗΣ)
- Το Πλαίσιο Ψηφιακής Αυθεντικοποίησης (ΠΨΑ)

Σε αντιστοιχία με τις καλυπτόμενες υπηρεσίες του ΠΔ&ΥΗΣ, το Πλαίσιο παρέχει επίσης ένα Ληξιαρχείο Διαλειτουργικότητας, το οποίο περιέχει:

- Τυποποιημένες, πρότυπες περιγραφές διαδικασιών
- Τυποποιημένα XML σχήματα δεδομένων και μεταδεδομένων
- Τις καλυπτόμενες τελικές υπηρεσίες ανά φορέα, σε διαφορετικά επίπεδα ηλεκτρονικής ολοκλήρωσης

Τέλος, το Πλαίσιο συμπληρώνεται από προδιαγραφές εκπαίδευσης, εκπαιδευτικό υλικό και υλικό διάδοσης.

Το Πλαίσιο Ηλεκτρονικής Διακυβέρνησης απευθύνεται σε όλους τους φορείς της Δημόσιας Διοίκησης, οι οποίοι διαθέτουν, αναπτύσσουν ή σχεδιάζουν να αναπτύξουν πληροφοριακά συστήματα με σκοπό να παρέχουν πληροφορίες και υπηρεσίες σε πολίτες, επιχειρήσεις και άλλους φορείς. Αναλυτικότερα, το Πλαίσιο απευθύνεται σε:

- Υπουργεία και Γενικές Γραμματείες,
- Περιφέρειες, Νομαρχιακές Αυτοδιοικήσεις, Οργανισμούς Τοπικής Αυτοδιοίκησης,
- Εποπτευόμενους φορείς του Δημόσιου Τομέα,
- Ανεξάρτητες Αρχές,
- Υπόλοιπους φορείς του Δημόσιου Τομέα όπως αυτός ορίζεται βάσει του Ν. 2527/97, άρθρο 1.

3.2 Υποδομή Δημόσιου Κλειδιού

Στα πλαίσια της ασφαλούς επικοινωνίας και των ασφαλών ηλεκτρονικών συναλλαγών μεταξύ των Φορέων του Δημοσίου μέσω εφαρμογών διαδικτύου, απαιτείται η χρήση Ψηφιακών Υπογραφών. Η επικρατέστερη τεχνολογία η οποία παρέχει την απαραίτητη υποδομή για την εφαρμογή και χρήση των ψηφιακών υπογραφών φέρει την ονομασία Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure – PKI). Η Υποδομή Δημόσιου Κλειδιού αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών που πιστοποιεί την εγκυρότητα κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο και παράλληλα προστατεύει την ασφάλεια της συναλλαγής. Το PKI ενσωματώνει

ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Στόχος των Υποδομών Δημόσιου Κλειδιού είναι η διασφάλιση των εξής ιδιοτήτων των δεδομένων:

- Εμπιστευτικότητα (Confidentiality),
- Ακεραιότητα (Integrity),
- Μη Άρνηση Αποδοχής (Non-Repudiation),
- Πιστοποίηση Αυθεντικότητας (Authentication).

Το ΥΠ.ΕΣ. έχει ήδη αναπτύξει τις κατάλληλες υποδομές (για την εφαρμογή και χρήση ψηφιακών υπογραφών) στο πλαίσιο του έργου «Εθνικό Δίκτυο Δημόσιας Διοίκησης - ΣΥΖΕΥΞΙΣ», το οποίο βρίσκεται ήδη σε παραγωγική λειτουργία. Επίσης, στο πλαίσιο του έργου «Εθνική Κεντρική Διαδικτυακή Πύλη - ΕΡΜΗΣ» προβλέπεται αντίστοιχη Υποδομή Δημοσίου Κλειδιού για τις ηλεκτρονικές συναλλαγές των πολιτών και των επιχειρήσεων με τις δημόσιες υπηρεσίες.

Οι υπηρεσίες οι οποίες προσφέρονται από την υποδομή του «ΣΥΖΕΥΞΙΣ», δίνουν τη δυνατότητα στα στελέχη του Δημοσίου, με τη χρήση έξυπνων καρτών που θα τους διατεθούν, να υπογράφουν ψηφιακά τις μεταξύ τους ηλεκτρονικές επικοινωνίες και συναλλαγές. Το θεσμικό πλαίσιο που διέπει τη εφαρμογή και χρήση των Ψηφιακών Υπογραφών παρουσιάζεται στο Π.Δ. 150/2001 (ΦΕΚ 125/Α'/2001) και (ΦΕΚ 1654/2006).

Πρέπει να σημειωθεί ότι ήδη προωθείται σε επίπεδο Ευρωπαϊκής Ένωσης (Ε.Ε), η υποχρεωτική χρήση ψηφιακής υπογραφής και ασφαλούς ηλεκτρονικής διακίνησης πληροφοριών – εγγράφων, στις ηλεκτρονικές συναλλαγές των κρατών – μελών με τις υπηρεσίες τις Ε.Ε.

Η αναλυτική διάρθρωση της Υποδομής Πιστοποίησης και των φορέων που συμμετέχουν ώστε να υλοποιηθεί η υποδομή Δημοσίου Κλειδιού στα πλαίσια του Εθνικού Δικτύου Δημόσιας Διοίκησης προδιαγράφεται στον Κανονισμό Πιστοποίησης (ΦΕΚ 1654/2006).

3.2.1 Διαδικασία Έκδοσης Αναγνωρισμένου Ψηφιακού Πιστοποιητικού

Οι βασικές διαδικαστικές ενέργειες που αφορούν στην έκδοση ενός πιστοποιητικού περιγράφονται συνοπτικά παρακάτω:

- Παράδοση Έξυπνης Κάρτας στον τελικό χρήστη:
- Κατάθεση απαραίτητων εντύπων στο ΚΕΠ για την ταυτοποίηση του τελικού χρήστη και υποβολή της αίτησης για την απόκτηση ψηφιακού πιστοποιητικού υπογραφής και κρυπτογράφησης.
- Παράδοση του φακέλου που περιέχει τους κωδικούς αριθμούς PIN – PUK στον τελικό χρήστη από τον υπάλληλο του ΚΕΠ
- Υποβολή Ηλεκτρονικής Αίτησης, από τον τελικό χρήστη, για την ενεργοποίηση των πιστοποιητικών ψηφιακής υπογραφής

και κρυπτογράφησης μέσω του Δικτυακού τόπου του «ΣΥΖΕΥΞΙΣ»

- Λήψη Πιστοποιητικών Ψηφιακής Υπογραφής και κρυπτογράφησης και αποθήκευση τους στην έξυπνη κάρτα – ενεργοποίηση πιστοποιητικών.

Η πλήρης περιγραφή των βημάτων και της διαδικασίας έκδοσης ψηφιακών πιστοποιητικών ορίζεται από το ΦΕΚ 1654/2006 «Κανονισμός Πιστοποίησης». Υπάρχουν δυο είδη Ψηφιακών Πιστοποιητικών που παρέχονται από την Υποδομή PKI του ΣΥΖΕΥΞΙΣ:

- Κατηγορία-Α: Ψηφιακό πιστοποιητικό για χρήση σε εφαρμογές κρυπτογράφησης και δοκιμές (tests) - "πιστοποιητικό" σύμφωνα με το Προεδρικό διάταγμα 150/2001
- Κατηγορία-Β: Ψηφιακό πιστοποιητικό για εφαρμογές ψηφιακής υπογραφής ηλεκτρονικών εγγράφων και επιβεβαίωσης της ταυτότητας του χρήστη κατά την ηλεκτρονική πρόσβαση του σε ελεγχόμενα σημεία (client authentication), χωρίς περιουσιακό αντικείμενο οποιασδήποτε αξίας -"αναγνωρισμένο πιστοποιητικό" σύμφωνα με το Προεδρικό διάταγμα 150/2001.

3.2.2 Εφαρμογή Ψηφιακών Πιστοποιητικών Στην Επικοινωνία

Παραπάνω παρουσιάστηκαν συνοπτικά οι χρήσεις και οι εφαρμογές που έχουν τα Ψηφιακά Πιστοποιητικά. Στην συνέχεια θα παρουσιαστούν πιο αναλυτικά οι χρήσεις αυτές καθώς και το τι απαιτείται τόσο από πλευράς οργάνωσης, όσο και από πλευράς λογισμικού (software) – υλικού (hardware) ώστε να μπορέσει να χρησιμοποιηθεί η Υποδομή PKI που παρέχεται μέσω του Εθνικού Δικτύου Δημόσιας Διοίκησης – ΣΥΖΕΥΞΙΣ. Στα πλαίσια του ΣΥΖΕΥΞΙΣ είναι δυνατή η επικοινωνία και ανταλλαγή μηνυμάτων μεταξύ των στελεχών των φορέων που συμμετέχουν. Η χρήση Ψηφιακών Πιστοποιητικών στην επικοινωνία αυτή ενδείκνυται για λόγους ασφαλείας. Η ασφάλεια που επιτυγχάνεται με τη χρήση Ψηφιακών Πιστοποιητικών που μπορεί είτε να υπογράφουν ένα μήνυμα είτε να κρυπτογραφούν ένα μήνυμα είτε και τα δύο εγγυάται στην περίπτωση της κρυπτογράφησης τη μη δυνατή σε τρίτους ανάγνωση των πληροφοριών που εμπεριέχονται στο μήνυμα και στην περίπτωση της υπογραφής του μηνύματος εγγυάται την ταυτότητα του αποστολέα του μηνύματος.

Η διαδικασία υπογραφής ενός μηνύματος ηλεκτρονικού ταχυδρομείου με το Ψηφιακό Πιστοποιητικό του χρήστη γίνεται με χρήση της Εφαρμογής Ηλεκτρονικού Ταχυδρομείου και αφού πρώτα ο χρήστης έχει εγκαταστήσει απαραίτητο υλικό για την ανάγνωση των ψηφιακών πιστοποιητικών του από το μέσο (USB Token –

έξυπνη κάρτα) στο οποίο τα έχει αποθηκεύσει σύμφωνα με τη διαδικασία έκδοσης αναγνωρισμένου ψηφιακού πιστοποιητικού που. Η εφαρμογή Ηλεκτρονικού Ταχυδρομείου παρέχει επιλογή ώστε να χρησιμοποιήσει ο χρήστης το Ψηφιακό Πιστοποιητικό του και να υπογράψει το ηλεκτρονικό μήνυμα που αποστέλλει. Εν συνεχεία ο παραλήπτης του ηλεκτρονικού μηνύματος συνδέεται με αντίστοιχη ιστοσελίδα που παρέχεται από την Αρχή Πιστοποίησης του ΣΥΖΕΥΞΙΣ, και ελέγχει κατά πόσο το Ψηφιακό Πιστοποιητικό που υπογράφει το μήνυμα που παρέλαβε είναι έγκυρο και έχει εκδοθεί από την Υπηρεσία Έκδοσης Πιστοποιητικών του ΣΥΖΕΥΞΙΣ.

Εκτός της επαλήθευσης τόσο της εγκυρότητας όσο και της ταυτότητας του Ψηφιακού Πιστοποιητικού η υπογραφή ηλεκτρονικών μηνυμάτων με χρήση Ψηφιακών Πιστοποιητικών εγγυάται και την ακεραιότητα του ηλεκτρονικού μηνύματος που παρελήφθη μιας και η εφαρμογή Ηλεκτρονικού Ταχυδρομείου αναγνωρίζει κατά πόσο το μήνυμα έχει τροποποιηθεί από τη στιγμή που υπογράφηκε. Έτσι τόσο ο παραλήπτης όσο και ο αποστολέας μπορούν να βεβαιώσουν ότι το ηλεκτρονικό μήνυμα είναι το πρωτότυπο και δεν έχει υποστεί κάποια τροποποίηση κατά τη διάρκεια της μεταφοράς του μέσω του δικτύου. Για την κρυπτογράφηση ηλεκτρονικών μηνυμάτων ο παραλήπτης θα πρέπει να έχει δώσει στον αποστολέα το Δημόσιο Κλειδί του. Ο αποστολέας κάνει χρήση του Δημόσιου Κλειδιού για να κρυπτογραφήσει το ηλεκτρονικό μήνυμα και το αποστέλλει. Ο παραλήπτης του μηνύματος που κατέχει το Ιδιωτικό Κλειδί είναι ο μόνος που μπορεί να αποκρυπτογραφήσει το ηλεκτρονικό μήνυμα μιας και είναι ο μόνος που κατέχει το Ιδιωτικό Κλειδί που αντιστοιχεί στο Δημόσιο Κλειδί του Στα πλαίσια της ασφαλούς επικοινωνίας με χρήση μεθόδων κρυπτογράφησης και ψηφιακής υπογραφής θα μπορούσε να χρησιμοποιηθεί η υποδομή PKI που παρέχεται από το Εθνικό Δίκτυο Δημόσιας Διοίκησης – ΣΥΖΕΥΞΙΣ ώστε να προμηθευτεί και να παράσχει στα στελέχη του Ψηφιακά Πιστοποιητικά για να μπορούν να υπογράψουν και να κρυπτογραφήσουν ηλεκτρονικά μηνύματα που αποστέλλονται τόσο για την εσωτερική επικοινωνία όσο και με την επικοινωνία με άλλους φορείς της Δημόσιας Διοίκησης που βρίσκονται στο ΣΥΖΕΥΞΙΣ.

Αναγνώριση υπαλλήλων που έχουν ανάγκη επικοινωνίας με χρήση ηλεκτρονικών μηνυμάτων και παροχή λογαριασμού ηλεκτρονικού ταχυδρομείου όσο και εκκίνηση της διαδικασίας απόκτησης Ψηφιακών Πιστοποιητικών για αυτούς τους χρήστες που διακινούν ευαίσθητες πληροφορίες που απαιτούν κρυπτογράφηση ή που απαιτείται ο έλεγχος από τον παραλήπτη της αυθεντικοποίησης του αποστολέα ή της εγκυρότητας και της μη αλλοίωσης του αρχικού μηνύματος κατά της διάρκεια της μετάδοσής του στο δίκτυο.

Εγκατάσταση εφαρμογής Ηλεκτρονικού Ταχυδρομείου στους υπολογιστές που οι χρήστες τους έχει αναγνωριστεί ότι έχουν ανάγκες επικοινωνίας τόσο εσωτερικά όσο και με τρίτους,

προτείνεται η χρήση του Outlook Express που παρέχεται δωρεάν μαζί με το λειτουργικό σύστημα Windows και υποστηρίζει την χρήση και εφαρμογή Ψηφιακών Πιστοποιητικών ή παρόμοιες εφαρμογές με δυνατότητα εφαρμογής Ψηφιακών Πιστοποιητικών σε ηλεκτρονικά μηνύματα.

Εγκατάσταση των απαραίτητων στοιχείων λογισμικού που απαιτούνται για την αναγνώριση και χρήση των Ψηφιακών Πιστοποιητικών όπως αυτά προδιαγράφονται στη σελίδα: http://pki.syzefxis.gov.gr/page0004.htm καθώς και προμήθεια και εγκατάσταση συσκευών ανάγνωσης Έξυπνων Καρτών για την αναγνώριση των Ψηφιακών Πιστοποιητικών των χρηστών όπως αυτές προδιαγράφονται από το έργο ΣΥΖΕΥΞΙΣ.

3.2.3 Προδιαγραφές αναγνωστών καρτών (smart cart readers)

Η χρήση της έξυπνης κάρτας ΣΥΖΕΥΞΙΣ προϋποθέτει την ύπαρξη αναγνωστών καρτών. Οι προδιαγραφές και τα τεχνικά χαρακτηριστικά που πρέπει να διαθέτουν οι αναγνώστες αυτοί είναι:

Χαρακτηριστικά:

- Δυνατότητα υποστήριξης όλων των ηλεκτρονικών chip καρτών, σύμφωνα με το πρότυπο ISO 7816 και T=0 και/ή T=1.
- Συμβατότητα με το πρότυπο ISO 7816/1/2/3.
- Δυνατότητα αυτόματης διαπίστωσης εισόδου/εξόδου κάρτας.
- Ύπαρξη PC interface: USB, Type: USB (+5V, GND, D+, D-), Connector : USB std - Speed: 1,5 Mbps.
- Υποστήριξη Card interface: Πρότυπο ISO 7816 - 1/2/3, T=0 και T=1
- Ταχύτητα: 9600 - 115 200 bps - προστασία από μικρά κυκλώματα σε όλες τις επαφές.

- Ύπαρξη 8 contact card connector - number of manoeuvres: 100.000
- Ύπαρξη εξωτερικού δείκτη LED για την κατάσταση του αναγνώστη καρτών.
- Δυνατότητα λειτουργίας σε συνθήκες θερμοκρασίας : 0 - 50°C
- Παροχή Ηλεκτρικού ρεύματος: 5V DC

Χαρακτηριστικά Λογισμικού και συμβατότητα:

- Συμβατότητα με PC/SC.
- Αυτόματη ενσωμάτωση σε περιβάλλοντα Windows.
- Προαιρετικό CSP interface.
- Προαιρετικό PKCS#11 interface.

3.2.4 Κρυπτογράφηση και Υπογραφή Αρχείων

Μια εναλλακτική χρήση των Ψηφιακών πιστοποιητικών είναι η κρυπτογράφηση και η υπογραφή Αρχείων π.χ. Adobe Acrobat (pdf) η Microsoft Word (doc) για λόγους ασφαλείας. Η κρυπτογράφηση αρχείων αποσκοπεί στο να μην μπορεί να γίνει ανάγνωση των περιεχομένων των αρχείων από κάποιον που παρέλαβε είτε σκόπιμα είτε ηθελημένα το αρχείο χωρίς να έχει πρόσβαση στην πληροφορία που περιέχει. Η διαδικασία της κρυπτογράφησης των αρχείων είναι απλή και μπορεί να γίνει από τα ίδια τα προγράμματα Adobe Acrobat ή Microsoft Word με τις αντίστοιχες επιλογές που διαθέτουν. Ο αποστολέας του αρχείου πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη του αρχείου και να το χρησιμοποιήσει για να κρυπτογραφήσει το αρχείο. Εν συνεχεία ο μόνος που μπορεί να αποκρυπτογραφήσει το αρχείο και να δει το περιεχόμενό του είναι ο κάτοχος του ιδιωτικού κλειδιού με το αντίστοιχο ζευγάρι δημόσιου κλειδιού.

Η υπογραφή αρχείων με χρήση Ψηφιακών Πιστοποιητικών μπορεί να γίνει για δύο λόγους, ο ένας είναι για να πιστοποιήσει ότι το συγκεκριμένο αρχείο έχει δημιουργηθεί από τον κάτοχο του πιστοποιητικού με το οποίο έχει υπογραφεί και ο δεύτερος είναι για να ελεγχθεί κατά πόσο το αρχείο έχει υποστεί κάποια αλλοίωση μετά το πέρας της υπογραφής του από το Ψηφιακό Πιστοποιητικό κατά τη διάρκεια μεταφοράς του ή μετάδοσης του μέσο του δικτύου. Όταν ένας χρήστης παραλαμβάνει ένα αρχείο υπογεγραμμένο με Ψηφιακή Υπογραφή τότε μπορεί να απευθυνθεί στην Αρχή η οποία έχει εκδώσει το Πιστοποιητικό που χρησιμοποιήθηκε για την υπογραφή και συγκεκριμένα σε ιστοσελίδα που παρέχεται για να εξετάσει ποιος είναι ο κάτοχος του πιστοποιητικού και αν το πιστοποιητικό που χρησιμοποιήθηκε είναι έγκυρο.

Για το πιστοποιητικά που εκδόθηκαν από την αρχή Πιστοποίησης του «ΣΥΖΕΥΞΙΣ» απαιτείται εγκατάσταση του λογισμικού OnSite MSI. Το OnSite MSI είναι ένα πακέτο το οποίο σας δίνει την δυνατότητα να κατεβάσετε τα απαραίτητα ActiveX controls στην περίπτωση που τα Windows που έχετε εγκατεστημένα, δεν επιτρέπουν την εγκατάσταση ψηφιακών πιστοποιητικών. Η Ψηφιακή Υπογραφή σύμφωνα με το Π.Δ. 150/2001 (ΦΕΚ 125/Α'/2001) επέχει θέση ιδιόχειρης υπογραφής.

Για να εφαρμοστεί η χρήση Ψηφιακών Πιστοποιητικών για την κρυπτογράφηση και υπογραφή αρχείων σε δημόσιους φορείς θα πρέπει αρχικά να αναγνωριστούν οι διαδικασίες που παράγουν έγγραφα ή αρχεία τα οποία περιέχουν ευαίσθητες πληροφορίες και για τα οποία κρίνεται ότι είναι απαραίτητη η κρυπτογράφησή τους κατά την αποστολή τους μέσο δικτύων. Εν συνεχεία πρέπει να παράσχει στους χρήστες των εφαρμογών που δημιουργούν τα έγγραφα αυτά Ψηφιακά Πιστοποιητικά με τα οποία θα υπογράφουν τα αρχεία που παράγουν ώστε κατά την αποστολή αυτών ο παραλήπτης να μπορεί να επιβεβαιώσει με ανάγνωση της Ψηφιακής Υπογραφής και σύνδεση με την Αρχή Πιστοποίησης που εξέδωσε το Πιστοποιητικό που χρησιμοποιήθηκε για την υπογραφή την ταυτότητα του αποστολέα, και το κατά πόσο το Ψηφιακό Πιστοποιητικό που δημιουργήθηκε είναι έγκυρο και έχει εκδοθεί από την αρχή Πιστοποίησης που αναφέρει.

Η κρυπτογράφηση και υπογραφή των αρχείων (PDF, DOC) γίνεται από λειτουργίες που προσφέρουν οι εφαρμογές αυτές και θα πρέπει να υπάρχει μέριμνα ώστε κάθε σταθμός εργασίας στον οποίο παράγονται αρχεία η έγγραφα που απαιτούν την κρυπτογράφηση ή την υπογραφή να διαθέτουν το αντίστοιχο λογισμικό. Όπως και στην περίπτωση της εφαρμογής των πιστοποιητικών για την επικοινωνία απαιτείται και η εγκατάσταση τόσο λογισμικού για την ανάγνωση των Ψηφιακών Πιστοποιητικών όσο και Αναγνωστών Καρτών για την ανάγνωση των πιστοποιητικών από το μέσο αποθήκευσής τους που για το δίκτυο ΣΥΖΕΥΞΙΣ είναι μια έξυπνη κάρτα. Η κρυπτογράφηση ενός αρχείου απαιτεί την επικοινωνία μεταξύ του αποστολέα και του παραλήπτη μιας και ο αποστολέας θα πρέπει να κρυπτογραφήσει το αρχείο χρησιμοποιώντας το Δημόσιο Κλειδί του παραλήπτη.

Σε επίπεδο μεταφοράς εγγράφων θα πρέπει να τονίσουμε ότι η χρήση της Υποδομής PKI που έχει δημιουργηθεί στα πλαίσια του Εθνικού Δικτύου Δημόσιας Διοίκησης – ΣΥΖΕΥΞΙΣ επιτρέπει την ασφαλή μεταφορά ηλεκτρονικών εγγράφων, δίνοντας στη δυνατότητα στα στελέχη της Δημόσιας Διοίκησης να επικοινωνούν και να ανταλλάσσουν έγγραφα και αρχεία με γρήγορο παρακάμπτοντας τους παραδοσιακού τρόπους μεταφοράς εγγράφων (δισκέτα, CD, hard-copy) αλλά και ασφαλή ώστε να μην μπορεί η πληροφορία είτε να αλλοιωθεί, είτε να υποκλαπεί αν πρόκειται για ευαίσθητες πληροφορίες ή προσωπικά δεδομένα κτλ.

3.2.5 Προσδιορισμός Ηλεκτρονικής Ταυτότητας

Σύμφωνα με το Πλαίσιο Ψηφιακής Αυθεντικοποίησης για την πρόσβαση σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης 3ου και 4ου επιπέδου απαιτείται ο ασφαλής προσδιορισμός της Ηλεκτρονικής Ταυτότητας με χρήση ψηφιακών πιστοποιητικών που θα εκδίδονται από την κατάλληλη Υποδομή Δημοσίου Κλειδιού (PKI).

Στα πλαίσια του έργου Εθνικού Δικτύου Δημόσιας Διοίκησης ΣΥΖΕΥΞΙΣ υπάρχει όπως έχει ήδη αναφερθεί και παρέχεται προς όλους τους φορείς που συμμετέχουν σε αυτό η κατάλληλη Υποδομή Δημοσίου Κλειδιού. Το ΣΥΖΕΥΞΙΣ παρέχει την Υποδομή Δημοσίου Κλειδιού στους φορείς της δημόσιας διοίκησης που συμμετέχουν στο δίκτυο και όχι σε πολίτες ή επιχειρήσεις.

Το Υπουργείο Εσωτερικών έχει υλοποιήσει στα πλαίσια του έργου της διαδικτυακής Πύλης Ερμής, μία υποδομή, η οποία παρέχει τη δυνατότητα παροχής ψηφιακών πιστοποιητικών σε πολίτες και επιχειρήσεις για την πρόσβαση τους σε υπηρεσίες Ηλεκτρονικής Διακυβέρνησης 3ου και 4ου επιπέδου.

Ο ασφαλής προσδιορισμός της Ηλεκτρονικής Ταυτότητας με χρήση ψηφιακών πιστοποιητικών απαιτείται για τις υπηρεσίες 3ου και 4ου επιπέδου μιας και στις υπηρεσίες αυτές απαιτείται τόσο η αποστολή στοιχείων από την πλευρά του χρήστη προς την υπηρεσία (υπηρεσία 3ο επίπεδο) π.χ. η αποστολή μιας αίτησης συμπληρωμένης με τα στοιχεία του χρήστη, όσο και η αποστολή βεβαιώσεων / εγγράφων / πιστοποιητικών από την υπηρεσία (π.χ. Portal, Υπάλληλος, κ.λπ.) προς το χρήστη (υπηρεσία 4ου επιπέδου).

Η χρήση Ψηφιακών Πιστοποιητικών για να υπογράψει ένας χρήστης μια αίτηση που αποστέλλει ηλεκτρονικά μέσο μιας υπηρεσίας δίνει το δικαίωμα στον παραλήπτη της αίτησης χρησιμοποιώντας την υπηρεσίας που του παρέχει η Αρχή Πιστοποίησης που εξέδωσε το πιστοποιητικό που χρησιμοποιήθηκε από το χρήστη να εξακριβώσει την Ηλεκτρονική Ταυτότητα του χρήστη ώστε να εκκινήσει τη διαδικασία που απαιτείται για την έκδοση του Πιστοποιητικού / Βεβαίωσης / Εγγράφου που ζήτησε αυτός. Από την άλλη δίνει τη δυνατότητα στο χρήστη αν οι πληροφορίες που αποστέλλει αποτελούν προσωπικά δεδομένα και θέλει να διασφαλίσει την προστασίας τους κατά την μεταφορά τους στον παραλήπτη να κρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη το ηλεκτρονικό έγγραφο που αποστέλλει ώστε να μπορεί μόνο ο παραλήπτης με χρήση του ιδιωτικού του κλειδιού να αποκρυπτογραφήσει την αίτηση / έγγραφο και να εκκινήσει αντίστοιχη διαδικασία.

Από την πλευρά του φορέα που παρέχει την ηλεκτρονική υπηρεσία, ο αρμόδιος υπάλληλος που διεκπεραιώνει το αίτημα του χρήστη και εφόσον αφορά υπηρεσία επιπέδου 4 δηλαδή αποστολή από το φορέα προς το χρήστη μιας βεβαίωσης ή αίτησης, απαιτείται η

ηλεκτρονική υπογραφή του εγγράφου από τον υπάλληλο ώστε να μπορεί ο χρήστης να βεβαιώσει ότι το έγγραφο είναι έγκυρο και έχει παραχθεί από το συγκεκριμένο φορέα / χρήστη και να επιβεβαιώσει επίσης και την ακεραιότητα του εγγράφου, δηλαδή ότι το έγγραφο δεν έχει τροποποιηθεί από τη στιγμή της ψηφιακής υπογραφής του και μετά.

Σε περίπτωση που το έγγραφο που θα αποσταλεί από το φορέα προς το χρήστη μέσο της παρεχόμενης υπηρεσίας 4ου επιπέδου περιέχει πληροφορία που αποτελεί προσωπικά δεδομένα, τότε θα πρέπει εκτός της υπογραφής ο υπάλληλος να κρυπτογραφήσει το έγγραφο χρησιμοποιώντας το δημόσιο κλειδί του χρήστη που απέστειλε την αίτηση, ώστε αυτός και μόνο αυτός να έχει δικαίωμα να διαβάσει το περιεχόμενο του εγγράφου.

Η Πύλη ΕΡΜΗΣ παρέχει τη δυνατότητα έκδοσης ψηφιακών πιστοποιητικών προς πολίτες και επιχειρήσεις. Θα πρέπει τόσο οι χρήστες των υπηρεσιών όσοι και αυτοί που υλοποιούν την διαδικασία να κατέχουν ψηφιακά πιστοποιητικά για να κρυπτογραφούν και να υπογράφουν είτε τις αιτήσεις που στέλνουν, είτε τις βεβαιώσεις που εκδίδουν.

Σύμφωνα με το Πλαίσιο Ψηφιακής Αυθεντικοποίησης ο φορέας που υλοποιεί ή παρέχει υπηρεσίες Ηλεκτρονικής Διακυβέρνησης 3ου και 4ου επιπέδου θα πρέπει να προσδιορίζει ασφαλώς την ηλεκτρονική ταυτότητα ενός χρήστη με χρήση ψηφιακών πιστοποιητικών. Για να γίνει αυτό θα πρέπει ο φορέας να καταγράψει και να κατηγοριοποιήσει τις υπηρεσίες που παρέχει ανάλογα με το επίπεδο που αυτές ανήκουν. Στις περιπτώσεις που οι υπηρεσίες που παρέχονται ταξινομούνται στο επίπεδο 3 ή 4 θα πρέπει να υποστηρίξει τον προσδιορισμό της Ηλεκτρονικής Ταυτότητας με χρήση Ψηφιακών Υπηρεσιών για τις υπηρεσίες αυτές.

Από τη στιγμή που αναγνωρισθούν οι υπηρεσίες αυτές και οι αντίστοιχες διαδικασίες στο εσωτερικό επίπεδο που τις υλοποιούν θα πρέπει οι υπάλληλοι που εμπλέκονται σε αυτές και ειδικότερα στα στάδια της παραλαβής της αίτησης από το χρήστη αλλά και της δημιουργίας εγγράφου που θα πρέπει να αποσταλεί ηλεκτρονικά στο χρήστη να κάνουν χρήστη της Υποδομής Δημοσίου Κλειδιού. Ειδικότερα, κατά την παραλαβή αίτησης από το χρήστη μέσω αντίστοιχης λειτουργίας της Διαδικτυακής Πύλης θα πρέπει ο υπάλληλος να ελέγχει τα στοιχεία που αναγράφονται στην αίτηση με τα στοιχεία που έχει καταχωρημένα η Αρχή Πιστοποίησης για το συγκεκριμένο ψηφιακό πιστοποιητικό που χρησιμοποιήθηκε για την υπογραφή της. Ο έλεγχος αυτός γίνεται μέσο υπηρεσίας (ιστοσελίδας) που παρέχει η Αρχή Πιστοποίησης που εξέδωσε το συγκεκριμένο πιστοποιητικό σε τρίτους για να μπορούν να επιβεβαιώσουν τόσο την εγκυρότητά του όσο και τα στοιχεία του κατόχου του πιστοποιητικού. Εν συνεχεία θα πρέπει αρμόδιος υπάλληλος μόλις διεκπεραιωθεί το αίτημα και παραχθεί το έγγραφο που αιτήθηκε ο χρήστης να χρησιμοποιήσει το ψηφιακό του

πιστοποιητικό για να το υπογράψει και αν πρόκειται για στοιχεία που αποτελούν προσωπικά δεδομένα του χρήστη να χρησιμοποιήσει το δημόσιο κλειδί του για να τα κρυπτογραφήσει. Έτσι ο χρήστης παραλαμβάνοντας το ηλεκτρονικό έγγραφο που αιτήθηκε θα μπορεί και να το αποκρυπτογραφήσει χρησιμοποιώντας το ιδιωτικό του κλειδί και να χρησιμοποιήσει την ψηφιακή υπογραφή με την οποία υπεγράφη από τον υπάλληλο το έγγραφο για να βεβαιώσει την ακεραιότητά του και την εγκυρότητά του μέσω της Αρχής Πιστοποίησης που εξέδωσε το πιστοποιητικό με το οποίο υπεγράφη το έγγραφο που παρέλαβε. Συνεπώς ο Φορέας θα πρέπει αναγνωρίζοντας τα στελέχη του που εμπλέκονται σε διαδικασίες που υλοποιούν υπηρεσίες 3ου και 4ου επιπέδου να εκδώσει Ψηφιακά Πιστοποιητικά για αυτούς ώστε να μπορούν να υπογράφουν τα έγγραφα που παράγουν Επίσης απαιτείται η επιμόρφωση των στελεχών που εμπλέκονται σε διαδικασίες κρυπτογράφησης και υπογραφής αρχείων ώστε να κατανοήσουν και να μπορούν να χρησιμοποιήσουν τα εργαλεία που απαιτούνται τόσο για τη διενέργεια κρυπτογράφησης ή υπογραφής όσο και για τον προσδιορισμό της Ηλεκτρονικής Ταυτότητας του αποστολέα της αίτησης.

Η υποδομή PKI παρέχει τη δυνατότητα για χρήση των Ψηφιακών Πιστοποιητικών για τον έλεγχο πρόσβασης σε εφαρμογές. Ο έλεγχος πρόσβασης με χρήση των Ψηφιακών Πιστοποιητικών χρησιμοποιείται είτε για έλεγχο της πρόσβασης ενός στελέχους ενός Δημόσιου Φορέα σε μια εφαρμογή ενός άλλου φορέα στα πλαίσια του Εθνικού Δικτύου Δημόσιας Διοίκησης ΣΥΖΕΥΞΙΣ, είτε για τον έλεγχο πρόσβασης ενός στελέχους ενός δημόσιου φορέα εσωτερικά στις εφαρμογές του φορέα. Αντί να χρησιμοποιείται η κλασική προσέγγιση Login/Password για την είσοδο σε μια εφαρμογή συνδέεται το Ψηφιακό Πιστοποιητικό με το χρήστη που έχει δικαίωμα να αποκτήσει πρόσβαση στην εφαρμογή.

Η προτεινόμενη λύση για τον έλεγχο της πρόσβασης τόσο των εσωτερικών χρηστών όσο και των στελεχών της δημόσιας διοίκησης που συμμετέχουν στο Εθνικό Δίκτυο Δημόσιας Διοίκησης – ΣΥΖΕΥΞΙΣ σε υπηρεσίες που παρέχονται μεταξύ των φορέων του δικτύου σε άλλους φορείς μπορεί να αξιοποιήσει τόσο την Υποδομή PKI που παρέχεται από το ΣΥΖΕΥΞΙΣ όσο και το πρωτόκολλο LDAP που επιτρέπει τη διαχείριση χρηστών, των λογαριασμών τους και των δικαιωμάτων χρήσης. Θα πρέπει τόσο να εγκατασταθεί ένας εξυπηρετητής LDAP που θα συνδέει τα Ψηφιακά πιστοποιητικά των χρηστών με τις αντίστοιχες εφαρμογές αλλά και τα δικαιώματα χρήσης που έχει ο κάθε χρήστης στην εφαρμογή, όσο και να παραμετροποιηθούν αντίστοιχα οι εφαρμογές ώστε να υποστηρίξουν τη διασύνδεση με τον εξυπηρετητή LDAP.

Ο κάθε χρήστης για να συνδεθεί με την εφαρμογή θα πρέπει να εισάγει το ψηφιακό πιστοποιητικό που έχει στην κατοχή του χρησιμοποιώντας αναγνώστη έξυπνων καρτών και η εφαρμογή αφού

διαβάσει το ψηφιακό πιστοποιητικό του χρήστη να συνδεθεί με τον LDAP εξυπηρετητή.

Ο εξυπηρετητής LDAP θα επαληθεύει την εγκυρότητα του ψηφιακού πιστοποιητικού και θα αναζητεί στη βάση τα αντίστοιχα δικαιώματα που έχει ο χρήστης του συγκεκριμένου ψηφιακού πιστοποιητικού για κάθε εφαρμογή και θα ενημερώνει την αντίστοιχη εφαρμογή για να επιτρέψει ή όχι την πρόσβαση και να ορίσει τα δικαιώματα που θα έχει ο χρήστης.

3.2.6 Προϋποθέσεις Χρήσης Υποδομής PKI

Για να μπορέσει να αξιοποιηθεί η Υποδομή Δημοσίου Κλειδιού PKI και οι εφαρμογές που αυτή παρέχει και που παρουσιάστηκαν στις προηγούμενες ενότητες θα πρέπει να γίνουν και οι ακόλουθες ενέργειες που περιγράφουν τη γενικότερη κατεύθυνση αλλαγής του και τη δυνατότητά παροχής ολοκληρωμένων υπηρεσιών Ηλεκτρονικής Διακυβέρνησης από φορείς της Δημόσιας Διοίκησης αλλά και άλλους, αντίστοιχης λειτουργίας, οργανισμούς.
Ενέργειες που θα πρέπει να γίνουν:

- Κατηγοριοποίηση των υπηρεσιών που παρέχονται ώστε να δημιουργηθούν οι κατάλληλες υποδομές για την ταυτοποίηση των χρηστών με χρήση PKI όπου αυτό απαιτείται (3ου και 4ου επιπέδου υπηρεσίες)
- Επιμόρφωση των υπαλλήλων που εμπλέκονται στις διαδικασίες που υλοποιούν τις προσφερόμενες υπηρεσίες Ηλεκτρονικής Διακυβέρνησης όσον αφορά τη χρήση και εφαρμογή του PKI, την αναγνώριση της ταυτότητας των χρηστών, την κρυπτογράφηση αλλά και υπογραφή εγγράφων.
- Αναβάθμιση των εφαρμογών που υπάρχουν σήμερα και δεν υποστηρίζουν τη δυνατότητα χρήσης Ψηφιακών Πιστοποιητικών.
- Δημιουργία πολιτικής ασφαλείας και πολιτικής διαχείρισης δικαιωμάτων χρηστών στις εφαρμογές αλλά και διαχείριση αυτών με χρήση του Πρωτοκόλλου LDAP και αντίστοιχου εξυπηρετητή.
- Δημιουργία λίστας εργαζομένων που θα πρέπει να αποκτήσουν ψηφιακό πιστοποιητικό από την Υποδομή PKI του ΣΥΖΕΥΞΙΣ ώστε να μπορούν να κάνουν χρήση των δυνατοτήτων που προσφέρονται όπου αυτή απαιτείται.
- Αναγνώριση των σταθμών εργασίας που απαιτούν την υποστήριξη Ψηφιακών Πιστοποιητικών ώστε να γίνει προμήθεια των απαραίτητων αναγνωστών καρτών αλλά και του αντίστοιχου λογισμικού για τη χρήση της Ψηφιακής Υπογραφής όπου δεν διατίθεται.

- Παροχή λογαριασμών e-mail σε όλα τα στελέχη που απαιτείται να ανταλλάξουν πληροφορίες με τρίτους φορείς ή / και πολίτες ή / και επιχειρήσεις ώστε να μπορεί να γίνει η επικοινωνία αυτή γρηγορότερη αλλά και να υποστηρίζει τη χρήση Ψηφιακών Πιστοποιητικών.

3.3 Θέματα ιδιωτικότητας

Η αξιοποίηση υπηρεσιών ηλεκτρονικής διακυβέρνησης απαιτεί συλλογή και επεξεργασία διαφορετικού είδους πληροφοριών, όπως προσωπικών δεδομένων, των οποίων η προστασία, επεξεργασία και μη αποκάλυψη και δημοσιοποίηση αποτελεί βασική κανονιστική απαίτηση, σύμφωνα με τις ειδικότερες προϋποθέσεις και εγγυήσεις της σχετικής νομοθεσίας (ν. 2472/97), που πρέπει να εκπληρώνεται από τις υπηρεσίες ηλεκτρονικής διακυβέρνησης.

Η συνταγματική και έννομη τάξη αναγνωρίζει την πληροφοριακή ιδιωτικότητα (informational privacy) ως το δικαίωμα και τη δυνατότητα του ατόμου να γνωρίζει, να ελέγχει και καταρχήν να προσδιορίζει τη χρήση των προσωπικών πληροφοριών του από άλλες οντότητες, ιδιώτες και κράτος. Ως ιδιωτικότητα ορίζεται η μη αποκάλυψη προσωπικών πληροφοριών σε μη εξουσιοδοτημένες οντότητες η οποία αποτελεί βασική παράμετρο της σχετικής νομοθεσίας που αναγνωρίζεται ρητά (άρθρο 10 ν.2472/97), ενώ η παραβίασή της τιμωρείται και με ποινικές κυρώσεις (άρθρο 22 § 4 ν. 2472/97). Το δικαίωμα στην ιδιωτικότητα αναφέρεται στη δυνατότητα ελέγχου της χρήσης των προσωπικών πληροφοριών.

Ως δεδομένα προσωπικού χαρακτήρα ή προσωπικά δεδομένα νοείται κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων, δηλαδή στο φυσικό πρόσωπο, στο οποίο αναφέρονται τα δεδομένα και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική (άρθρο 2α σε συνδυασμό με άρθρο 2γ του ν. 2472/97). Δεν λογίζονται ως δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιορισθούν τα υποκείμενα των δεδομένων. Στον όρο "προσωπικά δεδομένα" περιλαμβάνονται και αυτά τα οποία χρησιμοποιούνται συνήθως για τον προσδιορισμό της ταυτότητας του προσώπου. Με το σύνηθες προσδιοριστικό της ταυτότητας ενός προσώπου, το όνομα, μπορούν να εξομοιωθούν ο αριθμός της

κοινωνικής ασφάλισης, ο αριθμός του δελτίου ταυτότητας, ο αριθμός πελάτη και άλλα παρόμοια στοιχεία. Ως στοιχεία που δηλώνουν την ταυτότητα ενός προσώπου έχουν γίνει αποδεκτά και νομιμοποιητικά στοιχεία που αποδίδονται σε πρόσωπα ή επιλέγονται από αυτά (π.χ. κωδικός αναγνώρισης ή πρόσβασης, αριθμός PIN κ.α.).

Οι προσωπικές πληροφορίες μπορεί να αφορούν τις σχέσεις ενός προσώπου προς πρόσωπα ή τις σχέσεις προς πράγματα. Σε αυτές τις σχέσεις αντιστοιχούν πληροφορίες τόσο για τα εξωτερικά στοιχεία όσο και για ψυχικές καταστάσεις (απόψεις, κίνητρα, επιθυμίες), ενέργειες, αντιδράσεις, τρόπους συμπεριφοράς, ανεξάρτητα από το αν αφορούν το παρόν ή το παρελθόν και πόσο ανατρέχουν σε αυτό. Είναι αναμφισβήτητο ότι στις πληροφορίες προσωπικού χαρακτήρα εντάσσονται και οι σχέσεις προς το περιβάλλον. Ως τέτοιες νοούνται, για παράδειγμα, στοιχεία για την περιουσιακή κατάσταση, για την επαγγελματική και οικονομική δραστηριότητα, την οικογενειακή κατάσταση, τις προσωπικές δραστηριότητες και σχέσεις (συνήθειες του ελεύθερου χρόνου, συμμετοχή και δραστηριοποίηση σε ενώσεις, καταναλωτική συμπεριφορά) καθώς και για τις σχέσεις και καταστάσεις ιδιωτικού και δημοσίου δικαίου (ιδιοκτησία, συμβατικές σχέσεις, διοικητικές άδειες κλπ.). Ως ευαίσθητα προσδιορίζονται σαφώς στο νόμο (άρθρο 2β του ν. 2472/97, όπως ισχύει) τα δεδομένα που αφορούν στη φυλετική ή εθνική προέλευση, στα πολιτικά φρονήματα, στις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, στη συμμετοχή σε συνδικαλιστική οργάνωση, στην υγεία, στην κοινωνική πρόνοια και στην ερωτική ζωή, στα σχετικά με ποινικές διώξεις ή καταδίκες, καθώς και στη συμμετοχή σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Οι βασικές υποχρεώσεις της Διοίκησης σχετικά με τη διασφάλιση της Ιδιωτικότητας όταν παρέχονται υπηρεσίες ηλεκτρονικής διακυβέρνησης με χρήση δεδομένων προσωπικού χαρακτήρα, είναι:

- Κατά τη συλλογή και επεξεργασία δεδομένων θα πρέπει να λαμβάνεται πρόνοια ώστε να υπάρχει σαφής προσδιορισμός και διαχωρισμός των δεδομένων προσωπικού και στατιστικού χαρακτήρα.
- Θα πρέπει να διασφαλίζεται, με διαδικασίες ανωνυμοποίησης/ πολλαπλής κωδικοποίησης, ότι από τα δεδομένα στατιστικού χαρακτήρα δεν είναι δυνατός ο προσδιορισμός της ταυτότητας των φυσικών προσώπων.
- Με εγκυκλίους και άλλα μέσα ενημέρωσης-εκπαίδευσης θα πρέπει να καταστούν γνωστές και σαφείς στους δημόσιους υπαλλήλους οι κατηγορίες των ευαίσθητων δεδομένων για να αποφευχθεί σχετική σύγχυση (π.χ. παρατηρείται σχετική σύγχυση μεταξύ των δεδομένων που αφορούν φυλετική ή εθνική προέλευση (φυλετική ή εθνική μειονότητα) που

συνιστούν ευαίσθητα δεδομένα και αυτών που αφορούν την ιθαγένεια που συνιστούν απλά δεδομένα).

4 Προτάσεις για βελτίωση των ελληνικών e-υπηρεσιών

Κατά τη διάρκεια της έρευνας για την εκπόνηση της εργασίας το βασικό πρόβλημα που παρατήρησα στις ελληνικές e-υπηρεσίες είναι ότι ο χρήστης για κάθε υπηρεσία πρέπει να κάνει εγγραφή και να παρέχει εκ νέου τα διαπιστευτήριά του. Για παράδειγμα αν κάποιος πολίτης θέλει να εκδώσει πιστοποιητικό στρατολογικής κατάστασης, πιστοποιητικό γεννήσεως και να υποβάλλει φορολογική δήλωση ηλεκτρονικά, πρέπει να εγγραφεί στα site της στρατολογίας, του ΚΕΠ και του TAXIS αντίστοιχα (εκτός αν τα έγγραφα που θέλει εκδίδονται μέσω της πύλης «ΕΡΜΗΣ»). Το ίδιο ισχύει και για τις υπηρεσίες, κάθε υπηρεσία ή αρχή ταυτοποιείται και αυθεντικοποιείται για κάθε e-service που χρησιμοποιεί χωριστά. Εφόσον στις η-υπηρεσίες χρησιμοποιούνται σύγχρονες τεχνολογίες όπως web-services, soap και xml, η υλοποίηση ενός συστήματος διαχείρισης πολιτικών ασφαλείας είναι ιδιαίτερα απλή και δεν απαιτεί νέα τεχνολογική υποδομή. Η λύση που προτείνω είναι η χρήση της γλώσσας SAML η οποία επιτρέπει την δημιουργία πολιτικών ασφαλείας καθώς και τη μεταφορά δεδομένων ασφαλείας μεταξύ web services.

4.1 SAML

Η SAML (Security Assertion Markup Language) είναι μία γλώσσα που καθορίζει ένα πλαίσιο (framework) για την ανταλλαγή πληροφοριών ασφαλείας μεταξύ οργανισμών. Η SAML αναπτύχθηκε από το SSTC (Security Services Technical Committee) του οργανισμού OASIS (Organization for the Advancement of Structured Information Standards).

Η SAML βασίζεται στη γλώσσα XML. Οι πληροφορίες ασφαλείας περιγράφονται με τη μορφή αιτημάτων SAML τα οποία εμπιστεύονται οι εφαρμογές που διαχειρίζονται το επίπεδο της ασφάλειας. Το SSTC, το οποίο αναπτύσσει την SAML, παρέχει αναλυτική τεχνική περιγραφή για τη γλώσσα SAML, δίνοντας πληροφορίες για τις περιπτώσεις χρήσεις της, καθώς επίσης και τους βασικούς κανόνες σύνταξης.

4.2 Χρησιμότητα της SAML

Ας δούμε όμως γιατί είναι τόσο χρήσιμη η γλώσσα SAML στην ανταλλαγή πληροφοριών σχετικών με την ασφάλεια.

Περίπτωση εισόδου με διατήρηση στοιχείων: Πολλές online εφαρμογές, καθώς και πολλά web-site επιτρέπουν στο χρήστη να δώσει τα στοιχεία του μία φορά (sign-in) και στη συνέχεια τα στοιχεία του αποθηκεύονται ώστε να μην χρειάζεται να τα δίνει κάθε φορά. Οι εφαρμογές αυτές χρησιμοποιούν συνήθως cookies, τα οποία αποθηκεύονται τοπικά στον browser του χρήστη. Το πρόβλημα είναι ότι δεν μπορεί να γίνει ανταλλαγή cookies μεταξύ διακομιστών DNS με αποτέλεσμα τα δεδομένα ασφαλείας που αποθηκεύονται σε cookies σε έναν DNS διακομιστή να μην είναι ποτέ διαθέσιμα σε έναν άλλο διακομιστή. Παρ' όλα αυτά οι εφαρμογές αυτές κάνουν συχνά χρήση τεχνολογίας MDSSO, η οποία μέσω συγκεκριμένων μηχανισμών επιτρέπει την ανταλλαγή δεδομένων ασφαλείας μεταξύ διακομιστών. Παρ' ότι όμως οι μηχανισμοί αυτοί μπορεί να θεωρούνται αξιόπιστοι εντός μίας επιχείρησης ή ενός οργανισμού, αυτό συχνά δεν συμβαίνει μεταξύ διαφορετικών οργανισμών που χρησιμοποιούν διαφορετικές τεχνολογίες και πρωτόκολλα. Λύση στο πρόβλημα αυτό δίνει η SAML, η οποία παρέχει ένα αναγνωρισμένο συντακτικό, το οποίο δεν σχετίζεται με κάποια συγκεκριμένη πλατφόρμα και επιτρέπει την ανταλλαγή πληροφοριών σχετικά με έναν χρήστη από έναν διακομιστή ιστού σε κάποιον άλλο ανεξάρτητα από το DNS domain.

Ταυτότητα οργανισμού: Όταν οι online υπηρεσίες θέλουν να πραγματοποιήσουν συνεργατική χρήση εφαρμογών για τους κοινούς τους χρήστες, είναι απαραίτητο να και οι δύο πλευρές να «καταλαβαίνουν» τα πρωτόκολλα και το συντακτικό ανταλλαγής πληροφοριών καθώς επίσης και να έχουν έναν κοινό τρόπο αντιμετώπισης των χρηστών σχετικά με το ποιος είναι ο κάθε χρήστης και τι δικαιώματα πρέπει να έχει κατά τη χρήση του συστήματος ή της εφαρμογής. Αυτό προϋποθέτει ότι ο χρήστης θα έχει μία ενιαία ταυτότητα, τα δεδομένα της οποίας θα μοιράζονται και θα ανταλλάσσονται μεταξύ των web services. Η χρήση κοινής ταυτότητας μειώνει το κόστος αποθήκευσης δεδομένων αφού πολλές υπηρεσίες χρησιμοποιούν κοινή βάση χρηστών και δεν χρειάζεται κάθε μία να διατηρεί τα δικά της δεδομένα χρηστών.

Ευελιξία πρωτοκόλλων: Τα αιτήματα ασφαλείας (assertions) που διατυπώνονται με την SAML μπορούν να χρησιμοποιηθούν και εκτός ενός προγράμματος αποκλειστικά γραμμένου στην διαχείριση αιτημάτων με ένα πρωτόκολλο της SAML. Αυτό είναι ιδιαίτερα χρήσιμο σε μεγάλους οργανισμού και εταιρείες καθώς τα αιτήματα της SAML μπορούν να ενωθούν με άλλα αιτήματα ασφαλείας που χρησιμοποιούν το πρωτόκολλο SOAP.

4.3 Περιπτώσεις χρήσης της SAML

4.3.1 Συμμετέχοντες σε μία αλληλεπίδραση με χρήση της SAML

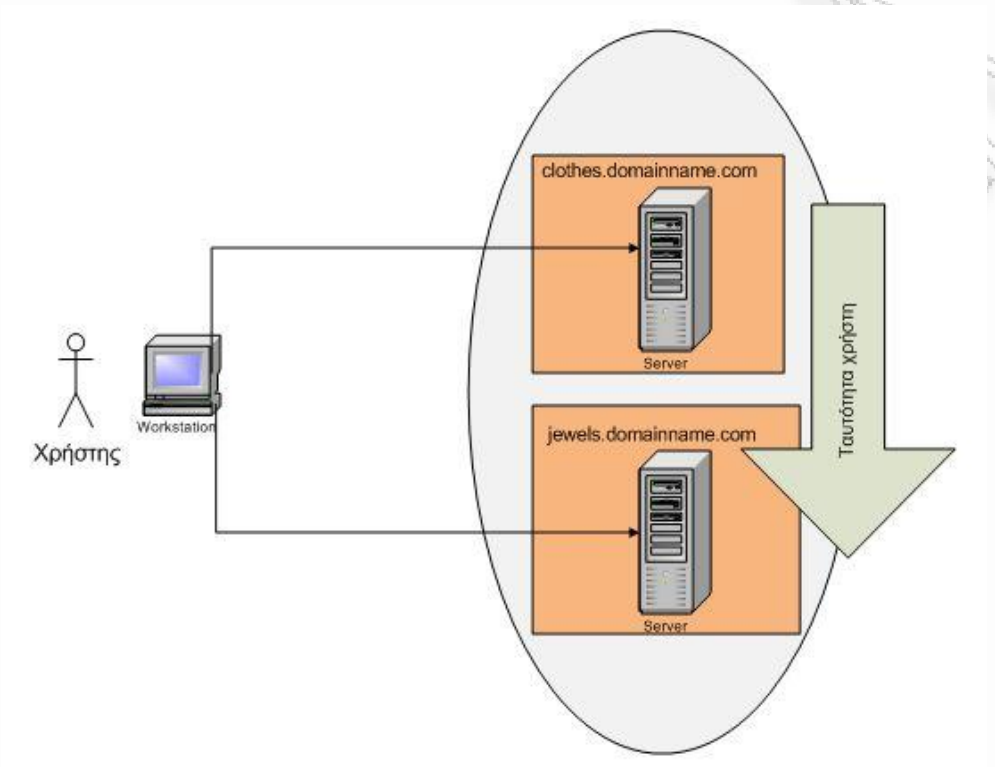
Οι ανταλλαγές πληροφοριών της SAML λαμβάνουν χώρα συνήθως μεταξύ δύο συστημάτων (το ένα σύστημα κάνει το αίτημα ασφαλείας [asserting party] και το άλλο εξετάζει και απορρίπτει ή δέχεται το αίτημα [relying party]). Η SAML υποστηρίζει τρεις τύπους δηλώσεων: την *αυθεντικοποίηση (authentication)* όπου το υποκείμενο που περιγράφεται έχει αυθεντικοποιηθεί μέσω κάποιου μηχανισμού, την *εξουσιοδότηση (authorization)*, όπου επιτρέπεται ή απαγορεύεται η πρόσβαση σε κάποιο πόρο του υποκειμένου που περιγράφεται στη δήλωση (assertion) και το *χαρακτηριστικό (attribute)* όπου το υποκείμενο συνδέεται με μία λίστα χαρακτηριστικών που περιγράφεται στη δήλωση (π.χ. ένα user profile). Οι αρχές (SAML asserting parties) εκδίδουν τις δηλώσεις. Οι αρχές είναι όσοι και οι τύποι δηλώσεων που εκδίδουν.

Για παράδειγμα μία δήλωση θα μπορούσε να αναφέρει ότι: Ο Νικόλαος Μαούνης με email: nikospsy2k@gmail.com και αριθμό μητρώου E03104 είναι αυθεντικοποιημένος (authenticated) με τη χρήση κωδικού πρόσβασης. Το σύστημα μετά μπορεί να κάνει χρήση αυτής της δήλωσης για να επιτρέψει ή να απαγορεύσει την πρόσβαση σε συγκεκριμένους πόρους του.

4.3.2 Μεταφορά στοιχείων χρήστη μεταξύ δικτυακών τόπων

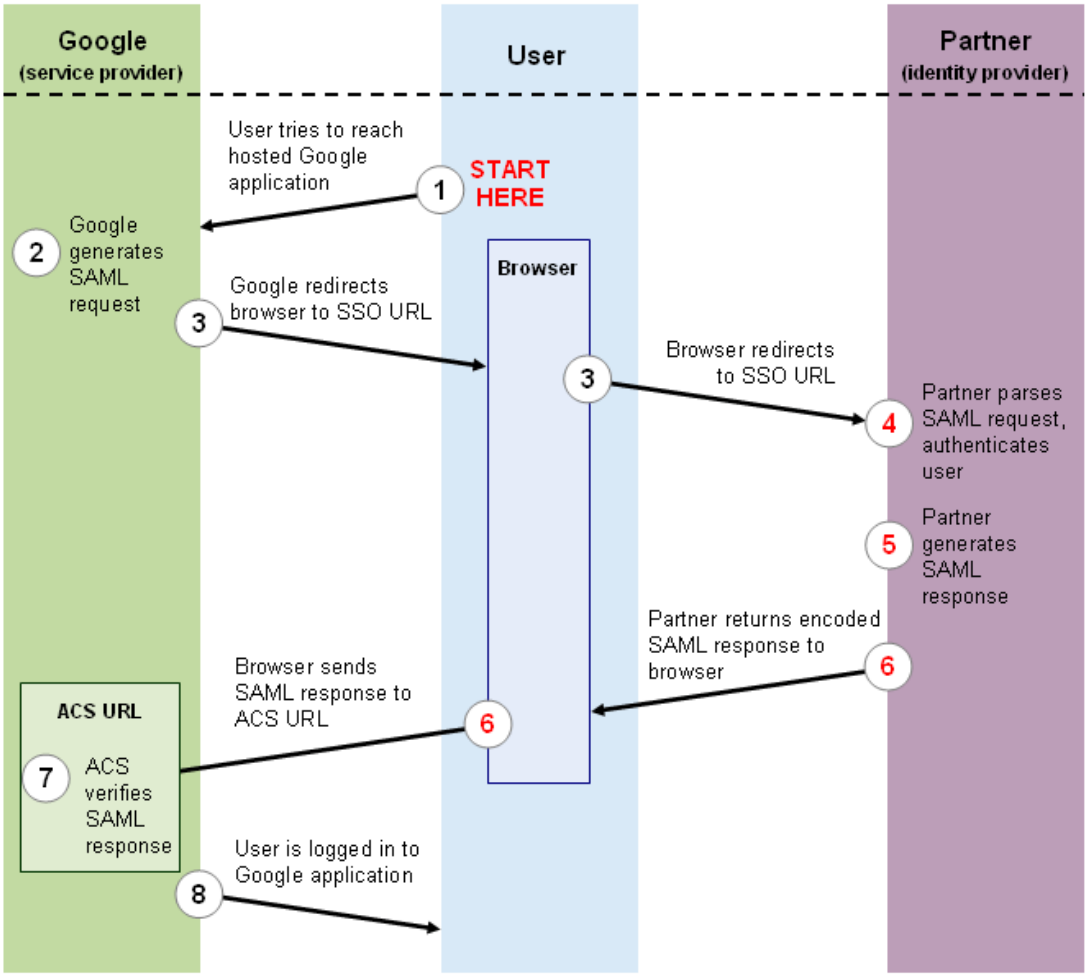
Η σημαντικότερη χρήση της SAML αυτή τη στιγμή είναι στο διαδίκτυο, στη χρήση web services όπου ένας δικτυακός τόπος μεταφέρει δεδομένα για κάποιον χρήστη και του δίνει πρόσβαση σε κάποιον άλλο δικτυακό τόπο. Η περίπτωση αυτή ονομάζεται Multi-domain web single sign-on (γνωστό ως SSO). Ένα παράδειγμα αυτής της περίπτωσης το οποίο συναντάμε καθημερινά στο διαδίκτυο είναι το εξής: έστω ότι ένας χρήστης πραγματοποιεί online αγορές από το κατάστημα με διεύθυνση http://clothes.domainname.com και για κάποιο λόγο μεταφέρεται στο συνεργαζόμενο (ή «συγγενικό») με το πρώτο κατάστημα http://jewels.domainname.com για να συνεχίσει τις αγορές του. Θεωρούμε ότι οι δύο αυτοί δικτυακοί τόποι έχουν συμφωνήσει στη χρήση κοινών κανόνων αυθεντικοποίησης και εξουσιοδότησης. Το site που παρέχει την ταυτότητα χρήση (http://clothes.domainname.com) δηλώνει στο site που παρέχει την υπηρεσία (http://jewels.domainname.com) ότι ο χρήστης έχει αυθεντικοποιηθεί και έχει συγκεκριμένα χαρακτηριστικά (attributes). Εφόσον ο δικτυακός τόπος jewels.domainname.com εμπιστεύεται το

δικτυακό τόπο clothes.domainname.com τότε εμπιστεύεται και το ότι ο χρήστης είναι σωστά αυθεντικοποιημένος και του παρέχει πρόσβαση στους πόρους του.



Αναπαράσταση του παραδείγματος για τη μεταφορά ταυτότητας

Το SSO είναι πολύ διαδεδομένο πλέον στο διαδίκτυο, με καλύτερο παράδειγμα τη χρησιμοποίησή του από το Google για την πρόσβαση στην υπηρεσία Google Apps (πακέτο εφαρμογών όπως τα Docs, το Gmail και το Analytics). Η πορεία που ακολουθεί το log-in ενός χρήστη όταν επιχειρεί να εισέλθει στις εφαρμογές του Google φαίνεται στο παρακάτω σχήμα.



Google SAML για τα Google Apps

Οι βιβλιοθήκες, τα APIs και ο κώδικας για την υλοποίηση μίας εφαρμογής single-sign-on με τη χρήση της SAML σαν αυτή του σχήματος, παρέχονται για ελεύθερη χρήση (κάτω από την άδεια Apache License 2.0) και σε όλες τις διαδεδομένες πλατφόρμες ανάπτυξης λογισμικού (Java, C#, Perl, Ruby) από την ιστοσελίδα του Google Code.

4.3.3 Περίπτωση ενοποίησης ταυτότητας μεταξύ δικτυακών τόπων

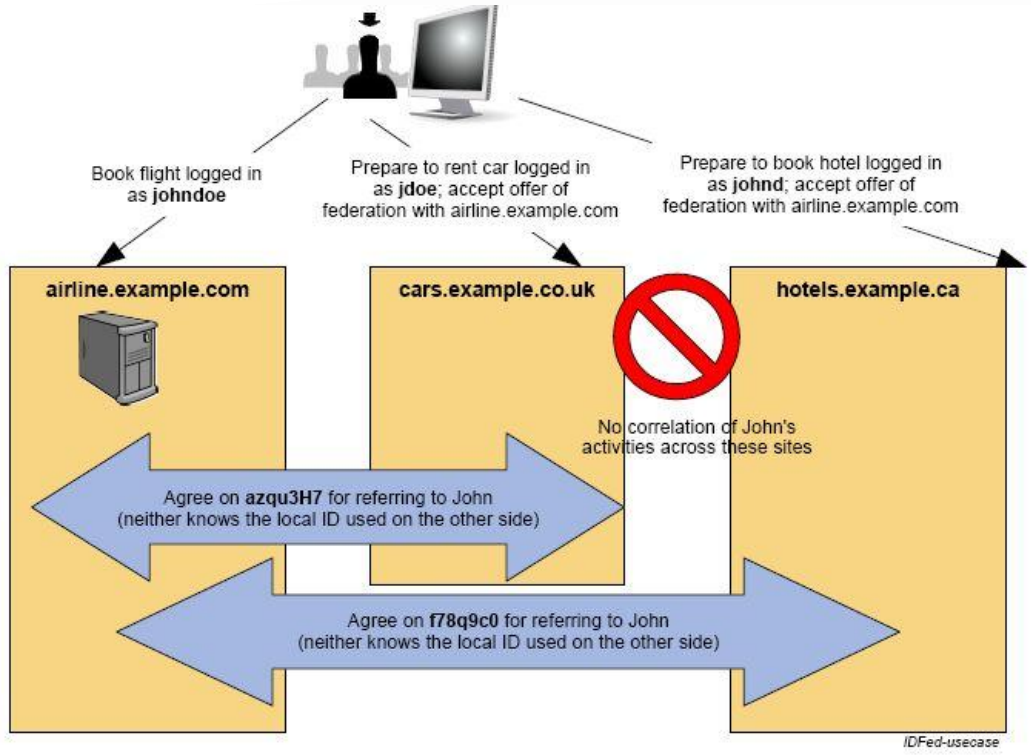
Όπως αναφέραμε παραπάνω, οι παροχοί υπηρεσιών μπορούν να ενοποιούν ταυτότητες χρηστών μεταξύ των υπηρεσιών τους χρησιμοποιώντας ένα σετ χαρακτηριστικών (attributes) με βάση το οποίο θα ορίζονται τα δικαιώματα και οι προσβάσεις των χρηστών.

Υπάρχουν όμως αρκετά σημεία, τα οποία πρέπει να λάβουν υπόψην τους οι εταιρείες πριν κάνουν χρήση ενοποιημένων ταυτοτήτων χρήστη. Για παράδειγμα:

- Έχουν οι χρήστες λογαριασμούς στους δικτυακούς τόπους, οι οποίοι πρόκειται να κάνουν χρήση ενοποιημένης, κοινής ταυτότητας;
- Θα μπορεί η δημιουργία και η διαγραφή ενοποιημένων λογαριασμών χρήστη να γίνεται δυναμικά από τους χρήστες;
- Θα χρειάζεται ανταλλαγή των χαρακτηριστικών της ταυτότητας χρήστη μεταξύ των εταιρειών που θα κάνουν χρήση της ενοποιημένης ταυτότητας;
- Θα πρέπει η επιβεβαίωση της ενοποιημένης ταυτότητας να γίνεται από προσωρινούς ελεγκτές (π.χ. cookies), οι οποίοι θα καταστρέφονται μετά την έξοδο του χρήστη;
- Οι πληροφορίες που θα ανταλλάζουν οι εταιρείες για τους χρήστες πρέπει να είναι κρυπτογραφημένες;

Η SAML στην τελευταία της έκδοση (έκδοση 2.0) υποστηρίζει τη δυναμική δημιουργία ενοποιημένων ταυτοτήτων (federated identities). Πολλές φορές η ανταλλαγή δεδομένων που σχετίζονται με ταυτότητες χρηστών μπορεί να γίνει και χωρίς την ανταλλαγή μηνυμάτων SAML μεταξύ των πληροφοριακών συστημάτων των εταιρειών. Για παράδειγμα ο παροχός ο οποίος έχει τα στοιχεία για τους λογαριασμούς των χρηστών μπορεί να τα μεταβιβάζει σε έναν παροχό υπηρεσιών μέσω βάσεων δεδομένων ή ροών δεδομένων (feeds), κάτι που αρκετές φορές απαιτεί την παρέμβαση ανθρώπου και δεν γίνεται αυτόματα. Εναλλακτικά η ταυτότητα χρήστη μπορεί να χρησιμοποιείται σε μία δήλωση SAML (SAML assertion) και στη συνέχεια να μεταβιβάζεται μεταξύ των παροχών υπηρεσιών. Τέλος η χρήση ενοποιημένων ταυτοτήτων μπορεί να γίνει μετά από επαγγελματική συμφωνία των εταιρειών που θα αναφέρει ότι ο παροχός ταυτότητας χρήστη θα αναφέρεται σε κάποιον χρήστη βασιζόμενος σε συγκεκριμένα χαρακτηριστικά (attributes) και τιμές χωρίς να απαιτείται καμία περεταίρω συντήρηση ή αναβάθμιση των στοιχείων των χρηστών από τις εταιρείες. Το IdP discovery της SAML επιτρέπει τον εντοπισμό χρηστών που επισκέπτονται δικτυακούς τόπους που κάνουν χρήση ενοποιημένης ταυτότητας.

Το παράδειγμα που ακολουθεί είναι από τον επίσημο οδηγό του OASIS για την SAML 2.0 και δείχνει με ποιο τρόπο υλοποιείται μέσω SAML η χρήση ενοποιημένης ταυτότητας.



Υλοποίηση ενοποιημένης ταυτότητας μεταξύ δικτυακών τόπων με χρήση του IdP της SAML 2.0

Το σχήμα δείχνει το εξής:

1. Ο χρήστης κλείνει μία πτήση στο δικτυακό τόπο με URL airline.example.com χρησιμοποιώντας το λογαριασμό johndoe.
2. Στη συνέχεια επισκέπτεται το δικτυακό τόπο cars.example.com για να νοικιάσει ένα αυτοκίνητο. Ο δικτυακός τόπος βλέπει μέσω του browser του χρήστη ότι ο χρήστης δεν έχει εισέλθει (δεν έχει κάνει log-in) αλλά και ότι προηγουμένως έχει επισκεφθεί το δικτυακό τόπο airline.example.com που είναι IdP partner με το cars.example.com. Έτσι ρωτάει το χρήστη αν θα ήθελε να χρησιμοποιήσει την ενοποιημένη ταυτότητα.
3. Ο χρήστης αποδέχεται τη χρήση ενοποιημένης ταυτότητας και έτσι ο web-browser επισκέπτεται ξανά το airline.example.com και δημιουργεί ένα νέο ψευδώνυμο, το **azqu3H7**, για όταν ο χρήστης επισκέπτεται το site cars.example.com. Το ψευδώνυμο αυτό παραπέμπει στο λογαριασμό johndoe του χρήστη. Και οι δύο δικτυακοί τόποι συμφωνούν ώστε να το χρησιμοποιούν για να αναφέρονται στο συγκεκριμένο χρήστη σε μελλοντικές συναλλαγές.
4. Στη συνέχεια ο χρήστης μεταφέρεται ξανά στο δικτυακό τόπο cars.example.com με μία δήλωση SAML (assertion) που αναφέρει ότι ο χρήστης με το ψευδώνυμο **azqu3H7** έχει κάνει log-in στον IdP. Επειδή όμως είναι η πρώτη φορά που ο δικτυακός τόπος cars.example.com βλέπει αυτό το

ψευδώνυμο, δεν γνωρίζει σε ποιον τοπικό λογαριασμό (δηλαδή λογαριασμό στο cars.example.com) ανήκει.

5. Έτσι ο χρήστης πρέπει να εισέλθει στο cars.example.com με τον «τοπικό» του λογαριασμό jdoe. Στη συνέχεια το cars.example.com θα προσθέσει το διακριτικό (identifier) **azqu3H7** στον τοπικό λογαριασμό jdoe για μελλοντική χρήση με τον Id Partner airline.example.com.
6. Αφού ο χρήστης νοικιάσει το αυτοκίνητο που επιθυμεί, επισκέπτεται το δικτυακό τόπο hotels.example.ca για να κλείσει δωμάτιο σε κάποιο ξενοδοχείο.
7. Η διαδικασία δημιουργίας ενιαίας ταυτότητας επαναλαμβάνεται μεταξύ των δικτυακών τόπων airline.example.com και hotels.example.ca, δημιουργώντας ένα νέο ψευδώνυμο **f78q9C0**, για τον IdP χρήστη johndoe, το οποίο θα χρησιμοποιείται όταν θα επισκέπτεται το hotels.example.ca.
8. Τέλος, ο χρήστης ξανά-μεταφέρεται στο hotels.example.ca με μία νέα δήλωση SAML. Ο δικτυακός τόπος (όπως ακριβώς έγινε και προηγουμένως) απαιτεί ο χρήστης να εισέλθει με τον τοπικό του λογαριασμό ώστε να δημιουργηθεί η ενιαία ταυτότητα.

Στο μέλλον όποτε ο συγκεκριμένος χρήστης θέλει να χρησιμοποιήσει αυτά τα τρία site θα κάνει log-in στο airline.example.com και ο δικτυακός τόπος θα πιστοποιεί το χρήστη με τα ψευδώνυμα στους άλλους δύο δικτυακούς τόπους.

4.4 Αρχιτεκτονική της SAML

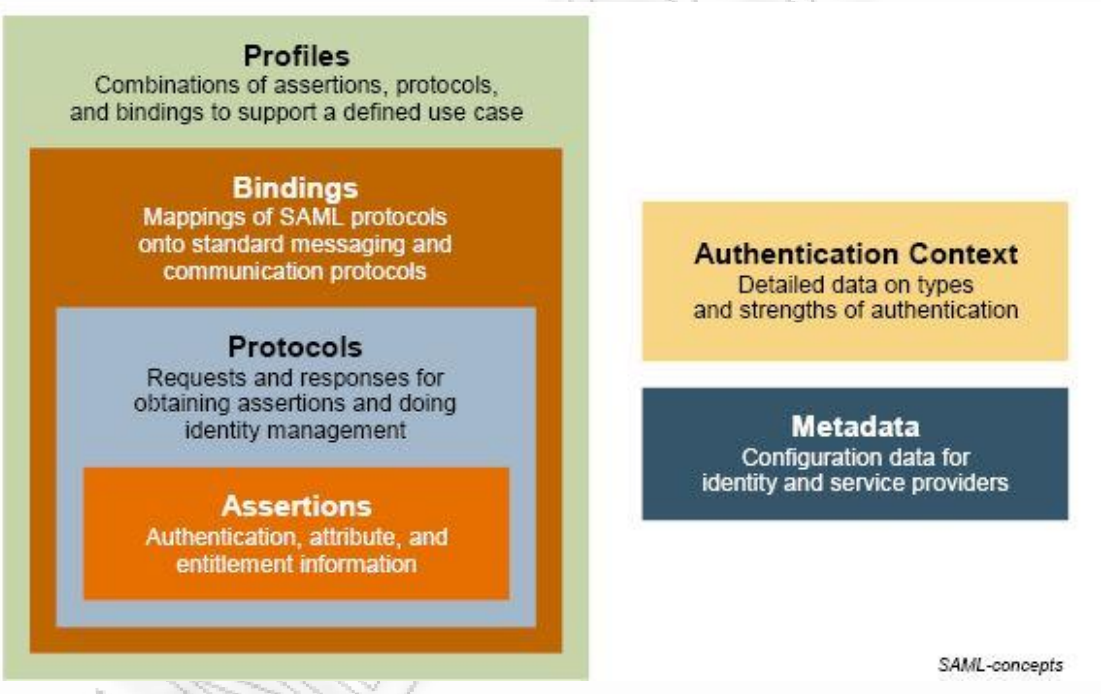
4.4.1 Βασικές έννοιες της SAML

Η SAML αποτελείται από στοιχεία που ονομάζονται μπλοκ, τα οποία επιτρέπουν, ανάλογα με τη σύνθεσή τους, διάφορες χρήσεις και δυνατότητες. Τα μπλοκ επιτρέπουν τη μεταφορά στοιχείων σχετικά με ταυτότητες, αυθεντικοποιήσεις, εξουσιοδοτήσεις και χαρακτηριστικά μεταξύ αυτόνομων οργανισμών, οι οποίοι έχουν αναπτύξει σχέσεις εμπιστοσύνης. Η βασική προδιαγραφή της SAML περιγράφει τόσο τη δομή και το περιεχόμενο των δηλώσεων, όσο και των μηνυμάτων που διαβιβάζονται με κάποιο υποστηριζόμενο πρωτόκολλο.

Οι δηλώσεις SAML (SAML assertions) μεταφέρουν στοιχεία, τα οποία σύμφωνα με την πλευρά που κάνει τη δήλωση είναι αληθή. Το SAML XML Schema περιγράφει το πώς πρέπει να δομούνται αυτές οι δηλώσεις, ώστε να είναι έγκυρες. Οι δηλώσεις δημιουργούνται συνήθως από τα asserting parties (η πλευρά που κάνει τη δήλωση) και βασίζονται σε κάποιο αίτημα που κάνει μία άλλη πλευρά που

ονομάζεται relying party (επειδή βασίζεται στη δήλωση για να πάρει μία απόφαση). Το μηνύματα του πρωτόκολλου της SAML χρησιμοποιούνται για να κάνουν πιστοποιημένα αιτήματα SAML και να επιστρέφουν τις κατάλληλες απαντήσεις. Η δομή και το περιεχόμενο αυτών των μηνυμάτων περιγράφεται στο SAML-defined protocol XML Schema. Τα SAML bindings (αντιστοιχίσεις) περιγράφουν πως μπορούν να μεταφέρονται μηνύματα SAML με συνηθισμένα πρωτόκολλα μεταφοράς όπως το HTTP και το SOAP.

Ακόμη τα SAML profiles περιγράφουν πως υλοποιούνται οι διάφορες περιπτώσεις χρήσης της SAML που περιγράψαμε πιο πάνω (για παράδειγμα το SSO). Ουσιαστικά τα προφίλ περιγράφουν τη δομή των δηλώσεων SAML, των SAML πρωτοκόλλων και των SAML bindings με σκοπό να λυθούν συνήθη προβλήματα των οργανισμών. Τέλος, τα SAML attributes profiles περιγράφουν πως πρέπει να γίνεται η ανταλλαγή δηλώσεων σε συχνά χρησιμοποιούμενα περιβάλλοντα (X.500, LDAP κατάλογοι κ.α.).



Συνοπτικός πίνακας βασικώς εννοιών της SAML

Δύο ακόμη έννοιες είναι πολύ βασικές κατά τη σχεδίαση και υλοποίηση ενός περιβάλλοντος SAML:

- Τα μεταδεδομένα (*metadata*), τα οποία είναι ένας τρόπος διατύπωσης και διαμοίρασης πληροφοριών μεταξύ των συμμετεχόντων σε ένα σύστημα που κάνει χρήση της SAML. Για παράδειγμα, μία Αρχή που χρησιμοποιεί SAML αντιστοιχίσεις (*bindings*), μπορεί να διατυπώσει με τη χρήση SAML XML metadata πληροφορίες που σχετίζονται με

πληροφορίες σχετικά με την κρυπτογράφηση κλειδιών, πρόσθετες πληροφορίες σχετικά με ταυτότητες και πληροφορίες σχετικά με υπογραφές.

- Πολλές φορές, ένας παροχός υπηρεσιών, χρειάζεται λεπτομερής πληροφορίες, σχετικά με τον τύπο της αυθεντικοποίησης που έχει γίνει σε έναν χρήστη από έναν παροχό ταυτοτήτων. Οι πληροφορίες αυτές μπορούν να μεταδοθούν με τη χρήση SAML authentication contexts, τα οποία δημιουργούνται με βάση συγκεκριμένο XML Schema και συγκεκριμένες κλάσεις.

Φυσικά δεν πρέπει να ξεχνάμε ότι η SAML βασίζεται στην XML, πράγμα που σημαίνει ότι είναι επεκτάσιμη και ότι ο καθένας μπορεί να δημιουργήσει τις δικές του δεσμεύσεις (bindings) και τα δικά του προφίλ.

4.4.2 Προχωρημένες έννοιες της SAML

Μία δήλωση SAML (assertion) μπορεί να περιέχει ένα στοιχείο που ονομάζεται SubjectConfirmation. Πρακτικά το στοιχείο αυτό καθορίζει τις προϋποθέσεις κάτω από τις οποίες επιτρέπεται σε κάποιον που θέλει να χρησιμοποιήσει μία δήλωση SAML να το κάνει. Η οντότητα που προσπαθεί να χρησιμοποιήσει τη δήλωση, υπερασπίζεται το δικαίωμά της να το κάνει, προβάλλοντας τις σχέσεις που έχει με το αντικείμενο. Μία δήλωση μπορεί να περιέχει πολλά SubjectConfirmation στοιχείο, αλλά μία οντότητα πρέπει να ικανοποιεί μόνο ένα από αυτά για να κάνει χρήση της δήλωσης. Το SubjectConfirmation δηλαδή παρέχει στοιχεία σε μία αρχή relying (relying party) ώστε αυτή να επικυρώσει τη σχέση της αρχής που θέλει να κάνει χρήση της δήλωσης με το αντικείμενο της δήλωσης. Το χαρακτηριστικό Method καθορίζει μία συγκεκριμένη μέθοδο, την οποία πρέπει να χρησιμοποιήσει το relying party για να πάρει την απόφασή του.

Η SAML 2.0 παρέχει τρία διαφορετικά σενάρια ασφαλείας, καθορίζοντας τρεις τιμές, τις οποίες μπορεί να πάρει το χαρακτηριστικό Method του στοιχείου SubjectConfirmation:

urn:oasis:names:tc:SAML:2.0:cm:holder-of-key
urn:oasis:names:tc:SAML:2.0:cm:sender-vouches
urn:oasis:names:tc:SAML:2.0:cm:bearer

Στην περίπτωση του holder-of-key, το relying party επιτρέπει σε οποιαδήποτε αρχή που γνωρίζει τις πληροφορίες ενός κλειδιού, που περιέχονται στο υπο-στοιχείο SubjectConfirmationData του στοιχείου SubjectConfirmation, να κάνει χρήση της δήλωσης SAML. Στο μοντέλο bearer, το relying party επιτρέπει σε οποιαδήποτε αρχή

μεταφέρει τη δήλωση, να τη χρησιμοποίει εφόσον πληροί και τις υπόλοιπες προϋποθέσεις. Στο μοντέλο sender-vouches, το relying party χρησιμοποιεί άλλα κριτήρια για να αποφασίσει ποιος θα επιτρέπεται να χρησιμοποιεί την δήλωση.

4.4.3 Συστατικά ενός περιβάλλοντος της SAML

Στην ενότητα αυτή γίνεται μία αναλυτική περιγραφή των συστατικών που χρησιμοποιούνται για την δημιουργία δηλώσεων, αντιστοιχίσεων, προφίλ και πρωτοκόλλων σε ένα περιβάλλον χρήσης της SAML.

Δηλώσεις (assertions): Η SAML επιτρέπει σε μία αρχή (asserting party) να κάνει μία δήλωση πληροφοριών ασφαλείας (assertion statement) σχετικά με κάποιο υποκείμενο ή θέμα (subject). Για παράδειγμα, μία δήλωση SAML θα μπορούσε να αναφέρει ότι το υποκείμενο «John Doe», έχει την ηλεκτρονική διεύθυνση «john.doe@example.com» και είναι μέλος ενός γκρουπ «μηχανικών».

Μία δήλωση περιέχει απαραίτητες και προαιρετικές πληροφορίες που υποστηρίζονται σε όλες τις αναφορές της. Συνήθως περιέχει και ένα υποκείμενο (αν όχι υπαρκτό πρόσωπο, τότε καθορίζεται από την ταυτότητά του [για παράδειγμα ένα πιστοποιητικό]) καθώς επίσης και κανόνες, οι οποίοι χρησιμοποιούνται για την επικύρωση της δήλωσης.

Η SAML καθορίζει τρία είδη τοποθετήσεων, τα οποία μπορούν να περιέχονται σε μία δήλωση:

- *Τοποθετήσεις αυθεντικοποίησης (authentication statements):* Οι τοποθετήσεις αυθεντικοποίησης δημιουργούνται από μία αρχή, η οποία έχει αυθεντικοποιήσει έναν χρήστη με επιτυχία. Περιγράφει επίσης τα μέσα που χρησιμοποιήθηκαν καθώς και την ώρα κατά την οποία έγινε η αυθεντικοποίηση.
- *Τοποθετήσεις χαρακτηριστικών (attribute statements):* Οι τοποθετήσεις χαρακτηριστικών περιέχουν συγκεκριμένα χαρακτηριστικά ταυτότητας, τα οποία σχετίζονται με το υποκείμενο. Για παράδειγμα μία τοποθέτηση χαρακτηριστικού, θα μπορούσε να αναφέρει ότι ο χρήστης «John Doe» είναι κάτοχος «Premium» συνδρομής.
- *Τοποθετήσεις απόφασης εξουσιοδότησης (authorization decision statements):* Αυτές οι τοποθετήσεις περιγράφουν τα δικαιώματα που έχει το υποκείμενο (για παράδειγμα αν ο χρήστης «John Doe» μπορεί να πραγματοποιήσει αγορές.

Πρωτόκολλα (protocols): Η προδιαγραφή της SAML περιγράφει μία σειρά από πρωτόκολλα τύπου ερώτησης/απάντησης (request/response):

- *Πρωτόκολλο ερώτησης αυθεντικοποίησης (Authentication request protocol):* Το πρωτόκολλο αυτό περιγράφει το πώς μία αρχή μπορεί να ζητά τοποθετήσεις αυθεντικοποίησης ή τοποθετήσεις χαρακτηριστικών (authentication και attribute statements). Το προφίλ SSO (single-sign-on) που περιγράψαμε σε προηγούμενη ενότητα, χρησιμοποιεί αυτό το πρωτόκολλο όταν ανακατευθύνει (κάνει redirect) έναν χρήστη από έναν παροχό υπηρεσιών (Service Provider) σε έναν IdP και χρειάζεται μία δήλωση για να εγκαθιδρύσει μία συνθήκη ασφαλείας μεταξύ του χρήστη και του Service Provider.
- *Single Logout πρωτόκολλο:* Το πρωτόκολλο αυτό περιγράφει έναν μηχανισμό, ο οποίος επιτρέπει σχεδόν ταυτόχρονη έξοδο (logout) από όλες τις ενεργές συνεδρίες (sessions) που σχετίζονται με μία αρχή. Το logout μπορεί να γίνει είτε από τον χρήστη, είτε αυτόματα από τον service provider ή τον IdP επειδή έληξε η συνεδρία (session timeout), είτε μετά από εντολή του διαχειριστή του συστήματος.
- *Πρωτόκολλο ερωτημάτων δηλώσεων (Asserting query and request protocol):* Το πρωτόκολλο αυτό περιγράφει μία σειρά ερωτημάτων, με βάση τα οποία μπορεί να αποκτηθεί μία δήλωση SAML. Η φόρμα Request του πρωτοκόλλου μπορεί να ζητήσει μία συγκεκριμένη δήλωση από μία αρχή χρησιμοποιώντας το ID της δήλωσης. Η φόρμα Query πως ένα relying party μπορεί να ζητήσει δηλώσεις (νέες ή υπάρχουσες) με συγκεκριμένο υποκείμενο και συγκεκριμένο τύπο τοποθετήσεων.
- *Artifact Resolution Protocol:* Το πρωτόκολλο αυτό περιγράφει έναν μηχανισμό με βάση τον οποίο τα SAML μηνύματα μπορούν να διαβιβάζονται με τη χρήση μιας τιμής μικρού μήκους, που ονομάζεται artifact. Ο παραλήπτης του artifact χρησιμοποιεί το πρωτόκολλο Artifact Resolution για να ζητήσει από το δημιουργό του μηνύματος να το ερμηνεύσει και να στείλει πίσω το κανονικό μήνυμα. Τα artifact συνήθως μεταφέρονται με τη χρήση μιας SAML αντιστοιχίας (binding), για παράδειγμα με HTTP Redirect, ενώ το resolution request/response γίνεται με τη χρήση συγχρονισμένης αντιστοίχισης, για παράδειγμα με το SOAP.
- *Πρωτόκολλο διαχείρισης δείκτη ονόματος (Name Identifier Management Protocol):* Το πρωτόκολλο αυτό παρέχει έναν μηχανισμό ώστε οι παροχοί υπηρεσιών ή οι IdPs να μπορούν να αλλάζουν την τιμή ή τη διαμόρφωση ενός Id με βάση το οποίο αναφέρονται σε κάποιον χρήστη. Το πρωτόκολλο παρέχει επίσης έναν μηχανισμό ώστε να τερματίζεται ο συσχετισμός ενός Id με κάποιον χρήστη.
- *Πρωτόκολλο αντιστοίχησης δείκτη ονόματος (Name Identifier Mapping Protocol):* Το πρωτόκολλο αυτό παρέχει έναν

μηχανισμό ώστε να γίνεται προγραμματιστικά η αντιστοίχηση ενός SAML Name ID σε κάποιο άλλο. Για παράδειγμα ένας παροχός υπηρεσιών, μπορεί να ζητήσει από κάποιον IdP το ID ενός χρήστη ώστε να το χρησιμοποιήσει σε μία εφαρμογή που χρησιμοποιεί από κοινού με κάποιον άλλο παροχό υπηρεσιών.

Αντιστοιχήσεις (bindings): Τα SAML bindings περιγράφουν με λεπτομέρειες, πως μπορούν να μεταφέρονται τα μηνύματα των πρωτοκόλλων της SAML με πρωτόκολλα μεταφοράς. Τα bindings που υπάρχουν στην SAML 2.0 είναι:

- *HTTP Redirect Binding:* Καθορίζει το πως μπορούν να μεταφέρονται τα μηνύματα των πρωτοκόλλων της SAML με χρήση μηνυμάτων ανακατεύθυνσης HTTP.
- *HTTP Post Binding:* Καθορίζει το πως μπορούν να μεταφέρονται μηνύματα των πρωτοκόλλων της SAML με τη μέθοδο POST των HTML φορμών.
- *HTTP Artifact Binding:* Καθορίζει το πως μεταφέρεται ένα artifact από τον αποστολέα στον παραλήπτη με τη χρήση HTTP (είτε με τη χρήση μίας φόρμας HTML, είτε με τη χρήση query string στο URL).
- *SAML SOAP Binding:* Καθορίζει το πως μεταφέρονται μηνύματα των SAML πρωτοκόλλων με το πρωτόκολλο SOAP 1.1 (και πως χρησιμοποιείται το πρωτόκολλο SOAP πάνω από το HTTP).
- *Reverse SOAP (PAOS) Binding:* Καθορίζει μία πολύ-επίπεδη ανταλλαγή μηνυμάτων μέσω SOAP/HTTP, η οποία επιτρέπει σε έναν HTTP client να απαντά με τη χρήση SOAP.
- *SAML URI Binding:* Καθορίζει το πώς μπορούν να ανακτηθούν δηλώσεις SAML με τη χρήση URI (uniform resource identifier).

Προφίλ (Profiles): Τα προφίλ καθορίζουν το πώς συνδυάζονται τα πρωτόκολλα, τα bindings και οι δηλώσεις της SAML ώστε να παρέχουν την καλύτερη δυνατή συνεργασία των συστημάτων (interoperability) σε συγκεκριμένα σενάρια χρήσης. Τα προκαθορισμένα προφίλ της SAML 2.0 είναι:

- *Web Browser SSO Profile:* Καθορίζει το πώς χρησιμοποιούνται το Authentication Request πρωτόκολλο, τα SAML response μηνύματα και οι δηλώσεις για να επιτευχθεί το Single-Sign-On στους κλασσικούς browsers. Καθορίζει επίσης το πώς χρησιμοποιούνται τα μηνύματα σε συνδυασμό με τα HTTP Redirect, HTTP POST και HTTP Artifact bindings.
- *Enhanced Client and Proxy (ECP) Profile:* Καθορίζει ένα συγκεκριμένο SSO προφίλ, όπου συγκεκριμένοι πελάτες (clients) ή διαμεσολαβητές (proxies) μπορούν να χρησιμοποιούν τα Reverse-SOAP (PAOS) και SOAP bindings.

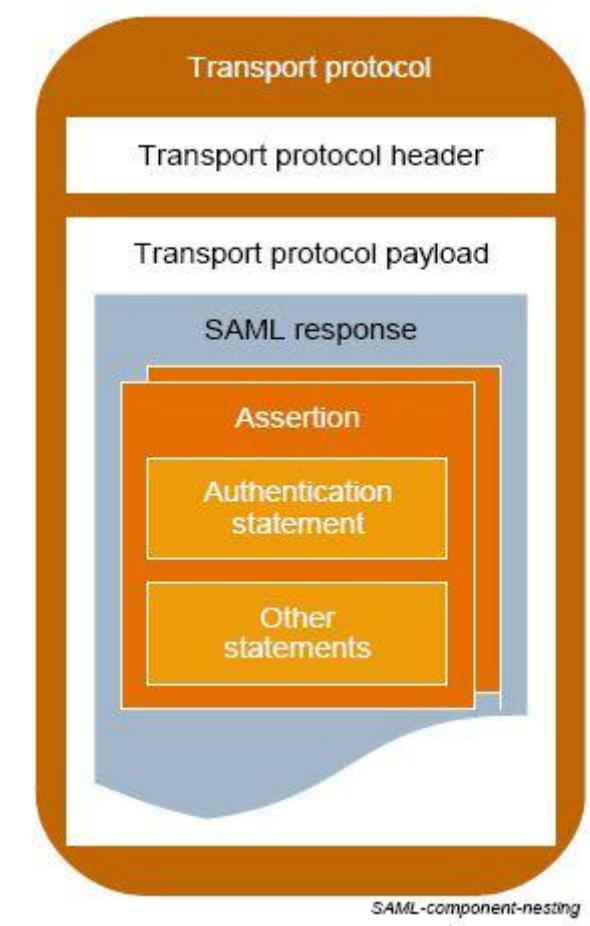
- *Identity Provider Discovery Profile:* Καθορίζει έναν μηχανισμό που επιτρέπει στους παροχούς υπηρεσιών να βλέπουν ποιους παροχούς ταυτοτήτων έχει επισκεφτεί ο χρήστης.
- *Single Logout Profile:* Καθορίζει το πώς μπορεί να χρησιμοποιηθεί το SAML Single Logout πρωτόκολλο μαζί με τα SOAP, HTTP Redirect, HTTP POST και HTTP Artifacts bindings.
- *Assertion Query/Request Profile:* Καθορίζει το πώς χρησιμοποιείται το SAML Query and Request πρωτόκολλο πάνω σε μία σύγχρονη αντιστοίχιση (synchronous binding), όπως είναι η αντιστοίχιση SOAP.
- *Artifact Resolution Profile:* Καθορίζει το πώς χρησιμοποιείται το Artifact Resolution πρωτόκολλο πάνω από ένα synchronous binding σαν το SOAP, ώστε να ανακτήσει το μήνυμα στο οποίο αναφέρεται ένα artifact.
- *Name Identifier Management Profile:* Καθορίζει το πώς μπορεί να χρησιμοποιηθεί το Name Identifier Management πρωτόκολλο σε συνδυασμό με τις αντιστοιχίσεις SOAP, HTTP Redirect, HTTP POST και HTTP Artifact.
- *Name Identifier Mapping Profile:* Καθορίζει το πώς χρησιμοποιείται ένα synchronous binding από το πρωτόκολλο Name Identifier Mapping.

4.4.4 XML Δομή της SAML και παραδείγματα

Σχέση μεταξύ των συστατικών της SAML

Μία δήλωση (assertion) περιέχει τοποθετήσεις (statements) και κάποιες πληροφορίες, οι οποίες σχετίζονται με τις τοποθετήσεις αυτές ή με τη δήλωση συνολικά. Μία δήλωση SAML, μεταφέρεται μεταξύ των αρχών με ένα response μήνυμα του πρωτοκόλλου SAML, το οποίο με τη σειρά του μεταφέρεται με ένα πρωτόκολλο μεταφοράς.

Η παρακάτω εικόνα δείχνει μία συνηθισμένη περίπτωση μεταφοράς ενός SAML μηνύματος: μία δήλωση SAML περιέχει διάφορες τοποθετήσεις και όλο το μήνυμα περιέχεται σε μία απάντηση SAML (SAML response), η οποία με τη σειρά της μεταφέρεται από κάποιο είδος πρωτοκόλλου (συνήθως πρωτόκολλο μεταφοράς).



Σχέση των συστατικών της SAML

Δήλωση, Υποκείμενο και δομή τοποθέτησης

Το παράδειγμα που ακολουθεί, δείχνει μία απλή SAML δήλωση με μία τοποθέτηση αυθεντικοποίησης. Πρέπει να σημειωθεί ότι η αλλαγή σειράς όταν γράφουμε κώδικα σε XML αγνοείται σε περίπτωση που συμβαίνει μεταξύ στοιχείων (δηλαδή αφού κλείσει ένα tag και πριν ανοίξει το επόμενο), αλλά παίζει ρόλο όταν συμβαίνει εντός ενός tag, δηλαδή αφού ανοίξει και πριν κλείσει, καθώς θεωρείται μέρος της τιμής του στοιχείου που βρίσκεται μέσα στο tag. Εδώ όμως, είμαστε υποχρεωμένοι να αλλάζουμε σειρά, ώστε να χωράει ο κώδικας στη σελίδα. Το παράδειγμα περιέχει αρίθμηση στις σειρές, ώστε να είναι εύκολη η επεξήγησή του στη συνέχεια.

```
1: <saml:Assertion xmlns:saml=”urn:oasis:names:tc:SAML:2.0:assertion”
2:   Version="2.0"
3:   IssueInstant="2005-01-31T12:00:00Z">
4:   <saml:Issuer Format=urn:oasis:names:SAML:2.0:nameid-
format:entity>
5:     http://idp.example.org
6:   </saml:Issuer>
```

```
7:   <saml:Subject>
8:     <saml:NameID
9: Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
10: j.doe@example.com
11:    </saml:NameID>
12:  </saml:Subject>
13:  <saml:Conditions
14:    NotBefore="2005-01-31T12:00:00Z"
15:    NotOnOrAfter="2005-01-31T12:10:00Z">
16:  </saml:Conditions>
17:  <saml:AuthnStatement
18:    AuthnInstant="2005-01-31T12:00:00Z"
SessionIndex="67775277772">
19:      <saml:AuthnContext>
20:        <saml:AuthnContextClassRef>
21:          urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtect
edTransport
22:        </saml:AuthnContextClassRef>
23:      </saml:AuthnContext>
24:   </saml:AuthnStatement>
25: </saml:Assertion>
```

Στην γραμμή 1, ξεκινά η δήλωση και καθορίζεται ο χώρος ονομάτων (namespace) που χρησιμοποιείται. Κάθε στοιχείο ξεκινά με το πρόθεμα saml:.
Στις γραμμές 2 έως 6 παρέχονται πληροφορίες σχετικά με τη φύση της δήλωσης: ποια έκδοση της SAML χρησιμοποιείται, πότε δημιουργήθηκε η δήλωση και ποιος εξέδωσε τη δήλωση.
Οι γραμμές 7 έως 12 παρέχουν πληροφορίες σχετικά με το υποκείμενο (subject) της δήλωσης, στο οποίο αναφέρονται όλες οι τοποθετήσεις. Το υποκείμενο έχει ένα name identifier που βρίσκεται στη γραμμή 10 (j.doe@example.com) το οποίο παρέχεται με τη μορφή που περιγράφεται στην γραμμή 9 (στην προκειμένη περίπτωση είναι eimailAddress). Η SAML υποστηρίζει διάφορα name identifiers και δίνει και τη δυνατότητα στο χρήστη να δημιουργήσει τα δικά του.
Οι γραμμές 14 και 15 καθορίζουν την περίοδο εγκυρότητας της δήλωσης (για πόσο δηλαδή θα ισχύει). Οι ημερομηνίες που περιέχονται σε αυτό το στοιχείο (timestamps) χρησιμοποιούν τον τύπο δεδομένων XML Schema dateTime.
Οι γραμμές 17-24 δηλώνουν ότι το υποκείμενο αυθεντικοποιήθηκε την ημερομηνία και ώρα που αναφέρεται με τη χρήση ενός μηχανισμού μεταφοράς κωδικών (password-protected mechanism). Για παράδειγμα ο χρήστης δίνει των κωδικό του, ο οποίος καταχωρείται μέσω μίας συνεδρίας που προστατεύεται με το SSL. Η SAML παρέχει αρκετούς προκαθορισμένους μηχανισμούς αυθεντικοποίησης και παρέχει τη δυνατότητα στο χρήστη να προσθέσει τους δικούς του.
Το στοιχείο <Name ID> μέσα στο <Subject> παρέχει τη δυνατότητα για χρήση name identifiers που βασίζονται σε διαφορετικά φορμά. Η SAML υποστηρίζει εξ' ορισμού τα εξής φορμά:

- Email address
- X.509 subject name
- Windows domain qualified name
- Kerberos principal name
- Entity identifier
- Persistent identifier
- Transient identifier

Οι δείκτες Persistent Identifier παρέχουν μία μόνιμη ιδιωτική «συμφωνία», διότι παραμένουν συσχετισμένοι με τις τοπικές ταυτότητες ενός παροχού υπηρεσιών έως ότου αυτές διαγραφούν ή μετακινηθούν. Οι Transient Identifiers υποστηρίζουν ανωνυμία, διότι χρησιμοποιούν δείκτες «μιας χρήσης», οι οποίοι δημιουργούνται στον IdP, δεν είναι συσχετισμένοι με κάποιον τοπικό χρήστη και καταστρέφονται όταν λήξει η συνεδρία (session timout).

Όταν δημιουργούνται Persistent Identifiers από έναν IdP, χρησιμοποιούνται μόνο για κάποιον συγκεκριμένο service provider, ο οποίος είναι ο μόνος που γνωρίζει την ύπαρξή τους. Οι δείκτες αυτοί δημιουργούνται μόνο για έναν συγκεκριμένο χρήστη και για χρήση με τον συγκεκριμένο παροχό υπηρεσιών. Ο παροχός υπηρεσιών δεν γνωρίζει την ύπαρξη άλλων τέτοιων δεικτών, που συσχετίζουν τον συγκεκριμένο χρήστη με άλλους παροχούς. Παρ' όλα αυτά, η SAML παρέχει υποστήριξη για την περίπτωση συνεργασίας (affiliation concept) δύο ή περισσότερων service providers. Μία άλλη λύση είναι να χρησιμοποιούν οι service providers το Name Identifier Mapping πρωτόκολλο και να αλληλεπιδρούν συνέχεια με τον IdP για την λήψη στοιχείων ταυτοτήτων.

Δομή τοποθέτησης χαρακτηριστικού (attribute)

Οι πληροφορίες χαρακτηριστικών παρέχονται είτε ως πρόσθετο των πληροφοριών αυθεντικοποίησης στην περίπτωση του Single-Sign-On (SSO), είτε ως απάντηση (response) σε ένα attribute query από κάποιο relying party. Η δομή χαρακτηριστικών (attribute structure) της SAML δεν περιγράφει κάποιο συγκεκριμένο τύπο δεδομένων που πρέπει να χρησιμοποιείται για τον καθορισμό των χαρακτηριστικών. Ο κώδικας παρακάτω, δείχνει μία τοποθέτηση χαρακτηριστικού:

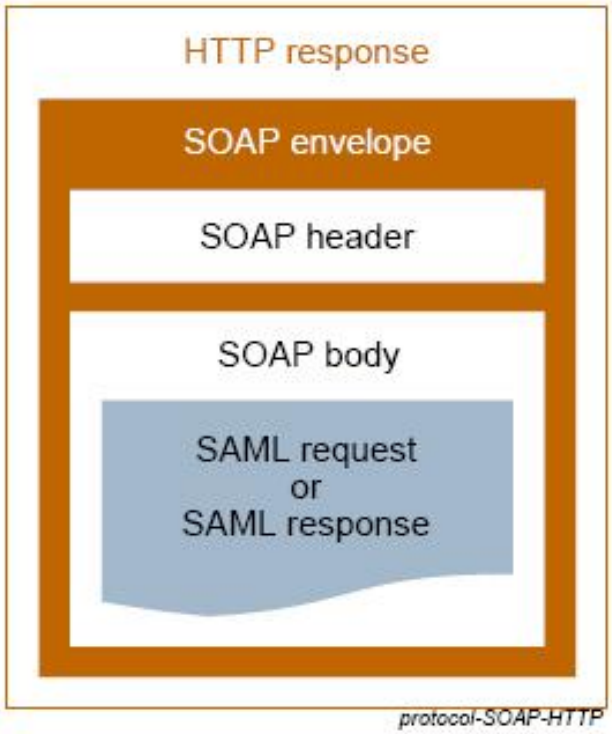
```
1: <saml:AttributeStatement>
2:  <saml:Attribute
3:   xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
4:   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
5:   Name="urn:oid:2.5.4.42"
6:   FriendlyName="givenName">
7:   <saml:AttributeValue xsi:type="xs:string"
8:     x500:Encoding="LDAP">John</saml:AttributeValue>
9:  </saml:Attribute>
10: <saml:Attribute
11: NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
```

```
12:  Name="LastName">
13:   <saml:AttributeValue
14:     xsi:type="xs:string">Doe</saml:AttributeValue>
15:  </saml:Attribute>
16:  <saml:Attribute
17:   NameFormat="http://smithco.com/attr-formats"
18:   Name="CreditLimit">
19:   xmlns:smithco="http://www.smithco.com/smithco-schema.xsd"
20:    <saml:AttributeValue xsi:type="smithco:type">
21:      <smithco:amount currency="USD">500.00</smithco:amount>
22:    </saml:AttributeValue>
23:  </saml:Attribute>
24: </saml:AttributeStatement>
```

Μία τοποθέτηση μπορεί να περιέχει περισσότερα από ένα χαρακτηριστικά (όπως στο παράδειγμα παραπάνω που υπάρχουν 3 χαρακτηριστικά, τα οποία ξεκινούν στις γραμμές 2, 10 και 16). Σε κάθε χαρακτηριστικό, καθορίζεται ένα φορμά ονόματος (γραμμές 4, 11, 17), το οποίο καθορίζει πως θα διερμηνευτεί το όνομα. Το παράδειγμα αυτό χρησιμοποιεί δύο προκαθορισμένα προφίλ χαρακτηριστικών της SAML, ενώ δημιουργεί και ένα τρίτο. Το πρώτο attribute του παραδείγματος χρησιμοποιεί το προφίλ X.500/LDAP attribute για να καθορίσει την τιμή του χαρακτηριστικού LDAP που φέρει το αναγνωριστικό OID "2.5.4.42". Αυτό το χαρακτηριστικό έχει σαν friendly name σε έναν κατάλογο LDAP το givenName και έχει την τιμή «John». Το δεύτερο χαρακτηριστικό του παραδείγματος, χρησιμοποιεί το Basic Attribute προφίλ, έχει το όνομα LastName και έχει την τιμή «Doe». Το τρίτο χαρακτηριστικό καθορίζει ένα όνομα, το οποίο δεν χρησιμοποιεί κάποιο από τα προκαθορισμένα προφίλ της SAML, αλλά κάποιο ενός τρίτου δημιουργού (της Smith Co.). Η χρήση ιδιωτικών φορμά και ονομάτων (όπως του τρίτου χαρακτηριστικού), μπορεί να προκαλέσει πρόβλημα στη συνεργασία δύο συστημάτων. Τα προβλήματα αυτά ονομάζονται interoperability issues. Ο τύπος της τιμής ενός χαρακτηριστικού καθορίζεται είτε με απλούς τύπους δεδομένων (όπως στις γραμμές 7, 14), είτε με τύπους δομημένους σε XML (όπως στις γραμμές 20 έως 22).

Δομή μηνύματος και SOAP binding

Σε περιβάλλοντα όπου τα συστήματα που χρησιμοποιούν την SAML υποστηρίζουν το πρωτόκολλο SOAP (αυτό συμβαίνει στο 90% των περιπτώσεων), μπορεί να χρησιμοποιηθεί το SOAP-over-HTTP binding για την ανταλλαγή μηνυμάτων του πρωτοκόλλου request/response. Στο παρακάτω σχήμα φαίνεται πως μεταφέρεται ένα SAML response μήνυμα στο σώμα ενός SOAP φακέλου, ο οποίος με τη σειρά του είναι μέρος ενός HTTP response. Πρέπει να σημειωθεί, ότι η SAML δεν κάνει χρήση του SOAP body από τη φύση της, αλλά αυτό μπορεί να υλοποιηθεί προγραμματιστικά σε περιβάλλονται που χρησιμοποιούν την SAML εφόσον χρειάζεται.



Ένα SAML μήνυμα μεταφέρεται μέσα σε έναν φάκελο SOAP, ο οποίος μεταφέρεται με ένα HTTP response.

Το παρακάτω XML έγγραφο, δείχνει ένα SAML query μήνυμα, το οποίο μεταφέρεται μέσα σε έναν φάκελο SOAP (SOAP envelope).

```
1. <?xml version="1.0" encoding="UTF-8"?>
2. <env:Envelope
3.   xmlns:env="http://www.w3.org/2003/05/soap/envelope/">
4.   <env:Body>
5.     <samlp:AttributeQuery
6.       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
7.       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
8.       ID="aaf23196-1773-2113-474a-fe114412ab72"
9.       Version="2.0"
10.      IssueInstant="2006-07-17T20:31:40Z">
11.      <saml:Issuer>http://example.sp.com</saml:Issuer>
12.      <saml:Subject>
13.        <saml:NameID
14.        Format="urn:oasis:names:tc:SAML:1.1:nameid-
           format:X509SubjectName">
15.        C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
16.        </saml:NameID>
17.      </saml:Subject>
18.      <saml:Attribute
19.        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
           format:uri"
20.        Name="urn:oid:2.5.4.42"
21.        FriendlyName="givenName">
22.      </saml:Attribute>
23.    </samlp:AttributeQuery>
24.  </env:Body>
25. </env:Envelope>
```

Στο παραπάνω παράδειγμα παρατηρούμε ότι στη γραμμή δύο ξεκινά ο φάκελος soap με των κώδικα `<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap/envelope/">`. Το attribute query ξεκινά στη γραμμή 5 και βρίσκεται μέσα σε ένα

φάκελο SOAP, ο οποίος ξεκινά στη γραμμή 4. Στη γραμμή 6-10 βρίσκονται τα υποχρεωτικά και κάποια προαιρετικά XML χαρακτηριστικά, συμπεριλαμβανομένου του ID του μηνύματος και των χώρων ονομάτων της SAML. Στις γραμμές 11-22 καθορίζονται τα προαιρετικά χαρακτηριστικά (όπως το givenName) που αναμένονται να επιστραφούν σε αυτόν που έκανε το συγκεκριμένο request.

Το επόμενο παράδειγμα δείχνει ένα απαντητικό (response) XML μήνυμα του πρωτοκόλλου SAML response, το οποίο μεταφέρεται μέσα σε έναν φάκελο SOAP:

```
1: <?xml version="1.0" encoding="UTF-8"?>
2: <env:Envelope
     xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
3:    <env:Body>
4:      <samlp:Response
5:        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
6:        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
7:        Version="2.0"
8:        ID="i92f8b5230dc04d73e93095719d191915fdc67d5e"
9:        IssueInstant="2006-07-17T20:31:41Z"
10:       InResponseTo="aaf23196-1773-2113-474a-fe114412ab72 ">
11:       <saml:Issuer>http://idp.example.org</saml:Issuer>
12:       <samlp:Status>
13:         <samlp:StatusCode
           Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
14:       </samlp:Status>
15:           ...SAML assertion...
16:     </samlp:Response>
17:    </env:Body>
18: </env:Envelope>
```

Στη γραμμή 10, το XML στοιχείο InResponseTo, αναφέρεται στο request, στο οποίο απαντά η συγκεκριμένη δήλωση. Στις γραμμές 7-14 υπάρχουν πρόσθετες πληροφορίες, απαραίτητες για την επεξεργασία της απάντησης. Στις σειρά 15 (*…SAML assertion…*) μπορεί να προστεθεί η δήλωση που θα περιέχει το givenName και τα άλλα στοιχεία που ζητήθηκαν με το request μήνυμα του προηγούμενου παραδείγματος.

4.4.5 Προσωπικά δεδομένα και SAML

Στο χώρο της τεχνολογίας και της πληροφορικής με τον όρο προσωπικά δεδομένα (privacy) αναφερόμαστε είτε στη δυνατότητα ενός χρήστη να ελέγχει το πώς μοιράζονται τα στοιχεία του και το πώς χρησιμοποιούνται, είτε σε διάφορους μηχανισμούς, οι οποίοι επικεντρώνονται στην προστασία των προσωπικών δεδομένων του χρήστη από τον κίνδυνο των παροχών υπηρεσιών (ένας τέτοιος

κίνδυνος είναι η ανταλλαγή ηλεκτρονικών διευθύνσεων μεταξύ παροχών με σκοπό την προώθηση προϊόντων).

Η SAML χρησιμοποιείται συχνά σε περιπτώσεις όπου πρέπει να λαμβάνεται υπόψην η προστασία των προσωπικών δεδομένων του χρήστη, για αυτό και παρέχει μία σειρά δυνατοτήτων για το σκοπό αυτό:

- Η SAML υποστηρίζει τη χρήση ψευδωνύμων μεταξύ ενός παροχού ταυτοτήτων και ενός παροχού υπηρεσιών. Αυτά τα ψευδώνυμα, δεν επιτρέπουν από μόνα τους την ύποπτη συνεργασία μεταξύ παροχών υπηρεσιών (παρόλα αυτά, ένας παροχός ταυτοτήτων θα μπορούσε να δηλώνει έναν χρήστη με τον ίδιο identifier σε κάθε παροχό υπηρεσιών [global identifier]).
- Η SAML υποστηρίζει τους transient identifiers, οι οποίοι εξασφαλίζουν ότι κάθε φορά που ένας χρήστης χρησιμοποιεί έναν παροχό υπηρεσιών μέσω διαδικασίας SSO, ο παροχός αυτός δεν μπορεί να διαπιστώσει αν ο χρήστης έχει ξαναχρησιμοποιήσει την υπηρεσία στο παρελθόν.
- Οι μηχανισμοί Authentication Context επιτρέπουν την αυθεντικοποίηση ενός χρήστη σε ένα επαρκές και εξασφαλισμένο επίπεδο ανάλογα με τους πόρους στους οποίους ο χρήστης θέλει να αποκτήσει πρόσβαση.

4.4.6 Ασφάλεια στην SAML

Η ανταλλαγή δηλώσεων μεταξύ ενός asserting party και ενός relying party, δεν εξασφαλίζει από μόνη της την ακεραιότητα και την ασφάλεια ενός συστήματος. Τα ερωτήματα που προκύπτουν είναι «πως το relying party εμπιστεύεται τις δηλώσεις που λαμβάνει» και «πως προστατεύεται το σύστημα από επιθέσεις τύπου "man-in-the-middle", οι οποίες μπορούν να υπεξαιρέσουν δηλώσεις για μελλοντική χρήση». Υπάρχουν συγκεκριμένοι μηχανισμοί ασφαλείας για κάθε SAML binding. Γενικά όταν θέλουμε ασφάλεια και προστασία των μηνυμάτων είναι καλό να χρησιμοποιείται HTTP over SSL 3.0 ή TLS 1.0. Όταν ένα relying party ζητά μία δήλωση από ένα asserting party ενδείκνυται η χρήση ψηφιακών υπογραφών ή η χρήση SSL 3.0 και TLS 1.0. Όταν ένα απαντητικό μήνυμα (response) μεταφέρεται σε ένα relying party μέσω του web browser του χρήστη (για παράδειγμα με τη χρήση του HTTP POST binding), το μήνυμα αυτό πρέπει να είναι ψηφιακά υπογεγραμμένο με τη χρήση XML υπογραφής.

5 Βιβλιογραφία

5.1 Βιβλία

[1] R. Kanneganti, P. Chodavarapu, *SOA Security*, Manning, 2008

[2] E. Pulier, H. Taylor, *Understanding Enterprise SOA*, Manning, 2005

[3] A. Rotem-Gal-Oz, *SOA Patterns (MEAP-Early Access Program)*, Manning, 2009

[4] N. Josuttis, *SOA in Practice: The Art of Distributed System Design*, O'Reilly, 2007

[5] S. Garfinkel, *Web Security, Privacy & Commerce (2nd Edition): Security for Users, Administrators and ISPs*, O'Reilly, 2002

[6] E. Ray, *Learning XML (2nd Edition)*, O'Reilly, 2003

[7] Σ. Κάτσικας, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, *Ασφάλεια Πληροφοριακών Συστημάτων*, Εκδόσεις Νέων Τεχνολογιών, 2004

[8] Σ. Κάτσικας, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, *Ασφάλεια Δικτύων Υπολογιστών: Τεχνολογίες και Υπηρεσίες σε περιβάλλοντα Ηλεκτρονικού Επιχειρείν & Ηλεκτρονικής Διακυβέρνησης*, Παπασωτηρίου, 2003

[9] R. Turner, *The Essential Guide to XML Technologies*, Prentice Hall, 2002

[10] K. Laudon, J. Laudon, *Essentials of Management Information Systems: Managing the Digital Firm (6th Edition)*, Prentice Hall, 2005

[11] B. Brogden, C. Minnick, *JAVA Developer's Guide to E-Commerce with XML and JSP*, SYBEX, 2001

5.2 Papers

[12] S. Cantor, J. Kemp, R. Philpott, E. Maler, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite*, http://www.oasis-open.org/committees/documents.php?wg_abbrev=security, 2007

[13] N. Ragouzis, J. Hughes, R. Philpott, E. Maler, P. Madsen, T. Scavo, *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, OASIS, http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.pdf, 2008

[14] J. Hughes, S. Cantor, J. Hodges, F. Hirsch, P Mishra, R. Philpott, E. Maler, *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite*, OASIS-Sun Microsystems, 2006

[15] *Πλαίσιο Ψηφιακής Διακυβέρνησης V.2.0*, Ελληνική Κυβέρνηση, 2010

5.3 Δικτυακοί τόποι

[16] *OASIS Security Services (SAML)*, http://www.oasis-open.org/committees/security

[17] *SAML XML.org – Online community for the Security Assertion Markup Language (SAML) OASIS Standard*, http://saml.xml.org

[18] *E-gif.gov.gr – Ελληνικό Πλαίσιο Παροχής Υπηρεσιών Ηλεκτρονικής Διακυβέρνησης και ανάπτυξης Προτύπων Διαλειτουργικότητας,* http://www.e-gif.gov.gr

[19] F. Cohen, *IBM: Debunking SAML myths and misunderstandings*, http://www.ibm.com/developerworks/xml/library/x-samlmyth.html

[20] *O'Reilly Media, Spreading the knowledge of Innovators,* http://www.oreilly.com

[21] *Google Code,* http://code.google.com