Μεταπτυχιακό Μάθημα: Ασφάλεια Συστημάτων Βάσεων Δεδομένων
Κατεύθυνση: Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Εξάμηνο: Χειμερινό 2005-2006

Επιβλέπων: Τζουραμάνης Θεόδωρος, Λέκτορας

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
Πανεπιστήμιο Αιγαίου

Τίτλος Εργασίας: Ασφάλεια σε Υπηρεσίες Ιστού (Security in Web Services)

Κεμαλής Κωνσταντίνος, icsdm05031@icsd.aegean.gr

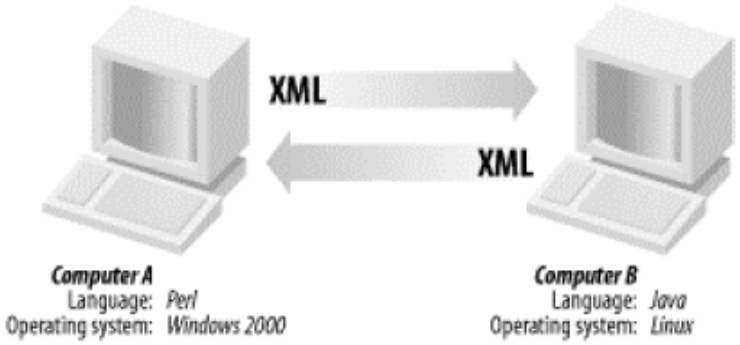
Μακροβασίλης Αθανάσιος, icsdm05032@icsd.aegean.gr

Καρλόβασι, Δεκέμβριος 2005

Περιεχόμενα

1. Εισαγωγή

Η υπηρεσία ιστού (web service) [3, 4, 20] είναι κάθε υπηρεσία που είναι διαθέσιμη μέσω του διαδικτύου (internet) ή ιδιωτικών εταιρικών δικτύων (intranets), χρησιμοποιεί ένα τυποποιημένο σύστημα XML επικοινωνίας και δεν είναι συνδεδεμένη με οποιοδήποτε λειτουργικό σύστημα ή γλώσσα προγραμματισμού (Εικόνα 1).



Εικόνα 1. Μοντέλο υπηρεσιών ιστού [3].

Οι υπηρεσίες ιστού επιτρέπουν σε εφαρμογές και σε διαδικτυακές συσκευές να επικοινωνούν εύκολα η μια με την άλλη και να συνδυάζουν τη λειτουργικότητά τους, για να παρέχουν υπηρεσίες μεταξύ τους.

2. Τεχνολογίες Υπηρεσιών Ιστού

Εφαρμογές που αλληλεπιδρούν μεταξύ τους, μέσω του ιστού πρέπει να είναι ικανές να βρίσκουν η μια την άλλη, να ανακαλύπτουν πληροφορίες που τις επιτρέπει να αλληλοσυνδέονται, να καθορίζουν ποιες είναι οι αναμενόμενες μορφές αλληλοσύνδεσης και να διαπραγματεύονται ποιότητες υπηρεσίας όπως η ασφάλεια και η αξιόπιστη επικοινωνία. Μερικές από αυτές τις ποιότητες υπηρεσίας καλύπτονται με τις υπάρχουσες τεχνολογίες και τα προτεινόμενα πρότυπα ενώ άλλες όχι. Γενικά η κοινότητα υπηρεσιών ιστού εργάζεται για να αντιμετωπίσει όλες αυτές τις απαιτήσεις, αλλά είναι μια εξελικτική διαδικασία, όπως ακριβώς ο ίδιος ο ιστός. Η υποδομή και τα πρότυπα σχεδιάζονται και αναπτύσσονται από την αρχή για να είναι επεκτάσιμα, όπως η XML. Οι υπηρεσίες ιστού απαιτούν αρκετές συγγενικές τεχνολογίες βασισμένες στην XML για να μεταφέρουν και να μετασχηματίζουν δεδομένα μέσα και έξω από προγράμματα και βάσεις δεδομένων. Οι τεχνολογίες αυτές αναλύονται στις παρακάτω ενότητες.

2.1. Extensible Markup Language (XML)

Η γλώσσα XML [2, 20] αναπτύχθηκε από μια Ομάδα Εργασίας κάτω από την επίβλεψη του διεθνούς οργανισμού World Wide Web Consortium (W3C) το 1996. Εδραιώθηκε από τον John Bosak της Sun Microsystems.

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

Η XML είναι markup γλώσσα για έγγραφα που περιέχουν δομημένες πληροφορίες. Η markup γλώσσα είναι ένας μηχανισμός που καθορίζει δομές σε ένα έγγραφο. Οι δομημένες πληροφορίες περιλαμβάνουν περιεχόμενο και κάποιες διευκρινίσεις για το ρόλο του περιεχόμενου. Σχεδόν όλα τα έγγραφα έχουν την ίδια δομή. Στην πραγματικότητα, η XML είναι κάτι περισσότερο από markup γλώσσα, είναι μεταγλώσσα, δηλαδή μια γλώσσα που χρησιμοποιείται για να καθορίσει νέες markup γλώσσες.

Όλο και περισσότερές εφαρμογές χρησιμοποιούν XML για να αποθηκεύσουν πληροφορίες λόγω των πλεονεκτημάτων της, κάποια εκ των οποίων είναι:

- Η δομή είναι καθορισμένη με σαφήνεια και μπορεί να περάσει μεταξύ διαφορετικών υπολογιστικών συστημάτων, που ειδάλλως θα ήταν ανίκανα να επικοινωνήσουν.
- Το «ωφέλιμο φορτίο» δεδομένων είναι εμφωλευμένο σε ετικέτες και επομένως αναγνώσιμο από τους χρήστες.
- Λόγω της κειμενικής φύσης τους, τα αρχεία XML είναι δεν εξαρτώνται από την πλατφόρμα του συστήματος.

Τα πλεονεκτήματα αυτά, έκαναν την XML το πλέον κατάλληλο πρότυπο για επικοινωνία μεταξύ υπηρεσιών ιστού. Για να εξασφαλιστεί μια χρήση ανεξάρτητη από πλατφόρμα και γλώσσα για κάθε υπηρεσία ιστού, αναπτύχθηκε το SOAP, το οποίο είναι μια XML εφαρμογή με καθορισμένα στοιχεία και μια προκαθορισμένη δομή. Στην επόμενη ενότητα αναλύεται το πρωτόκολλο SOAP.

2.2. Simple Object Access Protocol (SOAP)

Η μεταφορά δεδομένων έχει κεντρική σημασία στο δικτυωμένο και κατανεμημένο περιβάλλον του παγκόσμιου ιστού. Καθώς η XML έχει προκύψει ως η καταλληλότερη μορφή δεδομένων, η πρόκληση για τον αποστολέα και για τον παραλήπτη είναι να συμφωνήσουν στο πρωτόκολλο μεταφοράς, είτε αυτή πρόκειται να γίνει ανάμεσα σε προγράμματα λογισμικού, είτε ανάμεσα σε μηχανήματα ή οργανισμούς.

Το SOAP [1, 6, 7, 19, 30] είναι ένα πρωτόκολλο σχεδιασμένο για την ανταλλαγή XML εγγράφων μέσω διαφορετικών πρότυπων τεχνολογιών διαδικτύου, συμπεριλαμβανομένων των HTTP, Simple Mail Transfer Protocol (SMTP) και File Transfer Protocol (FTP).

Το SOAP είναι βασικά ένα μοντέλο μονόδρομης επικοινωνίας, το οποίο εγγυάται ότι ένα μήνυμα μεταφέρεται από τον αποστολέα στον παραλήπτη, ενδεχομένως περιλαμβάνοντας ενδιάμεσους σταθμούς που μπορούν να επεξεργαστούν μέρος του μηνύματος ή να το μεταβάλουν.

Ένα μήνυμα SOAP είναι ένα συνηθισμένο XML έγγραφο, το οποίο περιέχει τα ακόλουθα στοιχεία :

- Envelope, το οποίο προσδιορίζει ότι το έγγραφο XML είναι ένα μήνυμα SOAP. Καθορίζει την αρχή και το τέλος του μηνύματος.
- Header, το οποίο περιέχει πληροφορίες επικεφαλίδας. Είναι ένας ευέλικτος μηχανισμός για πρόσθεση χαρακτηριστικών στο SOAP μήνυμα.
- Body, το οποίο παρέχει έναν απλό μηχανισμό για ανταλλαγή υποχρεωτικών πληροφοριών που προορίζονται για τον τελικό αποδέκτη του μηνύματος.
- Fault, το οποίο περιέχει πληροφορίες για λάθη που τυχόν εμφανίστηκαν κατά την επεξεργασία του μηνύματος. Αυτό το στοιχείο εμφανίζεται μόνο σε απαντητικά μηνύματα και δεν πρέπει να εμφανίζεται πάνω από μία φορά μέσα στο Body του μηνύματος.

Συνοψίζοντας, το SOAP είναι ένα πρωτόκολλο βασισμένο σε XML για την αποστολή μηνυμάτων και την παραγωγή κλήσεων απομακρυσμένων διαδικασιών μέσα σε ένα κατανεμημένο περιβάλλον.

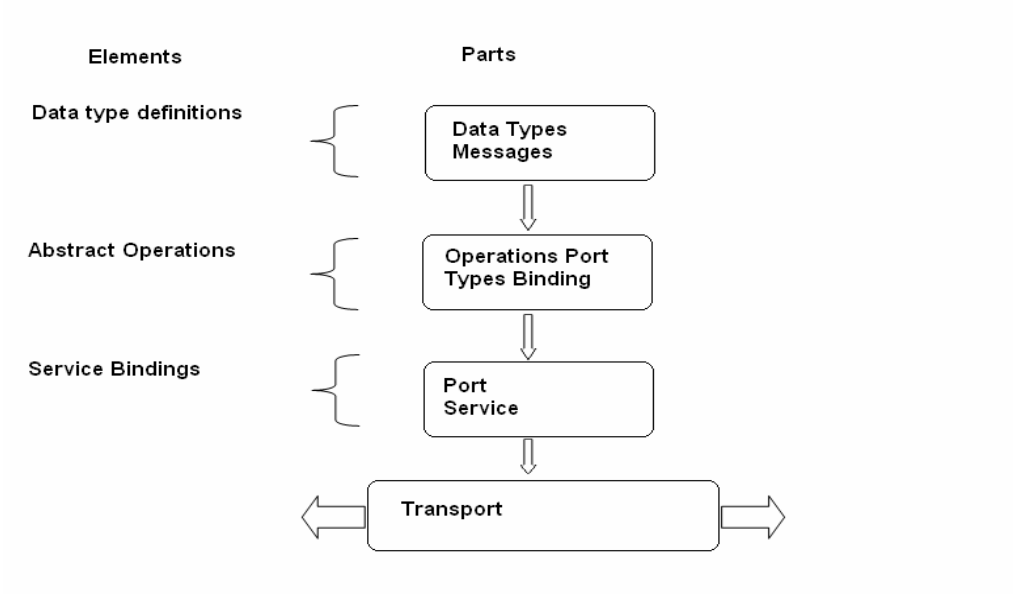
2.3. Web Services Description Language (WSDL)

Το επόμενο βήμα για να ολοκληρωθεί η αρχιτεκτονική επικοινωνίας των υπηρεσιών ιστού είναι να καθοριστεί το πως οι χρήστες θα έχουν πρόσβαση σε μία υπηρεσία μόλις αυτή τεθεί σε

εφαρμογή [27]. Εδώ είναι που παρεμβαίνει η WSDL προδιαγραφή [20, 32]. Αυτή παρέχει ένα συμβόλαιο μεταξύ του αιτούντος και του παροχέα της υπηρεσίας.

Η WSDL αναπτύχθηκε αρχικά από τη Microsoft και την IBM και υποβλήθηκε στο W3C από 25 εταιρείες. Βρίσκεται στην «καρδιά» του μοντέλου των υπηρεσιών του ιστού, παρέχοντας ένα κοινό τρόπο στον οποίο παρουσιάζονται οι τύποι των δεδομένων που λαμβάνουν χώρα στα μηνύματα, οι λειτουργίες οι οποίες πρόκειται να εκτελεστούν στα μηνύματα και η αντιστοίχηση των μηνυμάτων πάνω σε συναλλαγές του δικτύου. Η WSDL έχει XML μορφή, η οποία περιγράφει τι κάνει μια υπηρεσία, πως υλοποιεί τις λειτουργίες της και που θα τη βρούμε.

Η WSDL διαιρείται σε τρία βασικά στοιχεία και επτά τμήματα τα όποια είναι [20]: τα data type definitions, τα abstract operations και τα service bindings (Εικόνα 2). Κάθε βασικό στοιχείο μπορεί να καθοριστεί σε ένα ξεχωριστό XML έγγραφο και να εισαχθεί σε διαφορετικούς συνδυασμούς για να δημιουργήσει μια τελική περιγραφή υπηρεσιών ιστού ή μπορεί όλα να οριστούν σε ένα μόνο έγγραφο. Τα data type definitions (Data types, Messages) προσδιορίζουν τη δομή και το περιεχόμενο των μηνυμάτων. Τα Abstract Operations (Operations, Port Types, Binding) προσδιορίζουν τις λειτουργίες που εκτελούνται στο περιεχόμενο του μηνύματος και τα Service Bindings (Port, Service) προσδιορίζουν τη μετάδοση δεδομένων, η οποία θα μεταφέρει το μήνυμα στον προορισμό του.



Εικόνα 2. Τα τρία βασικά στοιχεία και τα επτά τμήματα του WSDL.

Το μόνο πρόβλημα που παραμένει είναι το πώς ένας ενδεχόμενος χρήστης μπορεί να βρει την αντίστοιχη περιγραφή, δηλαδή το WSDL έγγραφο. Τη λύση σ' αυτό το πρόβλημα έρχεται να δώσει το UDDI, το οποίο αναλύεται στην επόμενη ενότητα.

2.4. UDDI (Universal Description, Discovery and Integration)

Το UDDI [31] ως τεχνική προδιαγραφή παρέχει μια μέθοδο για δημοσίευση και εύρεση των περιγραφών μιας υπηρεσίας. Είναι μια κεντρική υπηρεσία καταλόγου, όπου υπηρεσίες ιστού μπορούν να καταχωρηθούν και να προσδιοριστούν σε έναν παροχέα υπηρεσιών. Είναι μια πρωτοβουλία των εταιρειών IBM, Ariba και Microsoft που το Σεπτέμβριο του 2000 εξέδωσαν την έκδοση 1.0 του UDDI, η οποία επέτρεπε στις επιχειρήσεις τη γρήγορη και δυναμική εύρεση καθώς και συναλλαγή με κάθε άλλη υπηρεσία. Ακολούθησε το UDDI 2.0 το Μάιο του 2001, με επιπλέον χαρακτηριστικά, όπως η υποστήριξη μιας υπηρεσίας ιστού από πολλές γλώσσες διεθνώς και το βελτιωμένο σύνολο επιλογών αναζήτησης. Σήμερα το UDDI βρίσκεται στην έκδοση 3.0.2.

Η δομή των δεδομένων τα οποία αποθηκεύονται στον κατάλογο είναι σε μορφή XML. Τα δεδομένα τα οποία συλλέγονται εντός του καταλόγου χωρίζονται σε τρεις κατηγορίες: λευκές σελίδες (white pages), κίτρινες σελίδες (yellow pages) και πράσινες σελίδες (green pages). Οι λευκές σελίδες περιέχουν γενικές πληροφορίες όπως το όνομα, η περιγραφή, η διεύθυνση επικοινωνίας και μοναδικούς αναγνωριστές όπως είναι οι D-U-N-S αριθμοί ή τα IDs για μια εταιρεία που προσφέρει την υπηρεσία. Αυτές οι πληροφορίες επιτρέπουν σε άλλους να ανακαλύψουν την υπηρεσία ιστού της εταιρείας βασισμένοι πάνω σε κάποιο στοιχείο αναγνώρισης. Οι κίτρινες σελίδες περιέχουν πληροφορίες οι οποίες περιγράφουν μια υπηρεσία χρησιμοποιώντας διαφορετικές κατηγοριοποιήσεις. Αυτές οι πληροφορίες επιτρέπουν στους άλλους χρήστες να ανακαλύψουν την υπηρεσία βασισμένοι στην κατηγοριοποίηση της (π.χ. είναι μια εταιρεία πώλησης ή κατασκευής αυτοκινήτων). Οι πράσινες σελίδες περιλαμβάνουν λεπτομερείς τεχνικές πληροφορίες για μια υπηρεσία ιστού, επιτρέποντας κάποιον να υλοποιήσει μια εφαρμογή για να χρησιμοποιεί την υπηρεσία ιστού. Αυτές οι τρεις κατηγορίες καταφέρνουν να κάνουν εύκολη την αναζήτηση για συγκεκριμένες υπηρεσίες ιστού.

Η UDDI καταχώρηση λειτουργεί όπως το Internet Domain Network Service (DNS). Οι εταιρείες μπορούν να καταχωρηθούν σε οποιονδήποτε ξενιστή (host), όπως IBM, HP, SAP, ή Microsoft και οι πληροφορίες που παρέχουν να τοποθετηθούν στην αντίστοιχη βάση του ξενιστή. Οι ξενιστές αναρτούν WSDL περιγραφές των υπηρεσιών ιστού για καταχώρηση και ανακάλυψη. Η WSDL παρέχει ξεχωριστά αρχεία για καταχώριση και ανακάλυψη υπηρεσιών, χρησιμοποιώντας την δική της XML μορφή εγγράφου.

Κάθε ένας χρήστης μπορεί να διαβάζει τον κατάλογο, να ερευνά για μια επιθυμητή υπηρεσία και να φορτώνει την περιγραφή σε περίπτωση που ταιριάζει από οποιονδήποτε ξενιστή. Οι χρήστες δεν θα διαβάσουν απευθείας μια UDDI καταχώρηση από τη στιγμή που η πληροφορία,

η οποία είναι αποθηκευμένη εντός του καταλόγου δεν είναι απαραίτητα φιλική προς τον αναγνώστη.

Όταν χρειαστεί να γίνει ενημέρωση των δεδομένων, ο χρήστης της εταιρείας θα πρέπει να επιστρέψει στον ξενιστή όπου έγινε η αρχική καταχώρηση των δεδομένων, έτσι ώστε να μπορέσει να εκτελέσει τη λειτουργία της ενημέρωσης.

3. Ασφάλεια σε Υπηρεσίες Ιστού

Η ασφάλεια είναι ένα από τα ποιο σημαντικά και σύνθετα θέματα που αντιμετωπίζει το διαδίκτυο και οι υπηρεσίες ιστού. Η ασφάλεια πρέπει να εξασφαλίσει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων στις υπηρεσίες ιστού. Κανένας άλλος πέραν του παραλήπτη των δεδομένων δεν επιτρέπεται να εξετάσει ή να επέμβει στο περιεχόμενο του μηνύματος. Ακόμη είναι απαραίτητο να ελέγχεται η προσπέλαση στις υπηρεσίες ιστού, ειδικά όταν πολλές υπηρεσίες ιστού χρησιμοποιούνται μαζί, έτσι ώστε μόνο αυτοί που είναι εξουσιοδοτημένοι να μπορούν να τις χρησιμοποιούν. Για να επιτύχουμε όλα αυτά, χρησιμοποιούνται τεχνολογίες οι οποίες περιγράφονται στις επόμενες ενότητες.

3.1. XML Ψηφιακές Υπογραφές

Οι XML ψηφιακές υπογραφές (XML Digital Signatures) [5] είναι ένα πρότυπο για την ασφαλή επικύρωση της προέλευσης των μηνυμάτων. Η προδιαγραφή της XML υπογραφής επιτρέπει στα έγγραφα XML να υπογραφούν με ένα τυποποιημένο τρόπο, χρησιμοποιώντας διαφορετικούς αλγόριθμους ψηφιακής υπογραφής. Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιηθούν για επικύρωση των μηνυμάτων και για μη-αποποίηση.

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

υπογραφή, που ενσωματώνεται μέσα στην υπογραφή, ή ενσωματώνει την υπογραφή μέσα σε αυτό.

Τα στοιχεία μιας XML υπογραφής, όπως φαίνεται στην εικόνα 3, είναι τα εξής:

```
<element name="Signature" type="ds:SignatureType"/>
<complexType name="SignatureType">
  <sequence>
    <element ref="ds:SignedInfo"/>
    <element ref="ds:SignatureValue"/>
    <element ref="ds:KeyInfo" minOccurs="0"/>
    <element ref="ds:Object" minOccurs="0" maxOccurs="unbounded"/>
  </sequence>
  <attribute name="Id" type="ID" use="optional"/>
</complexType>
```

Εικόνα 3. Παράδειγμα XML ψηφιακής υπογραφής.

Το στοιχείο SignedInfo περιλαμβάνει τον αλγόριθμο canonicalization, έναν αλγόριθμο υπογραφής και μια ή περισσότερες αναφορές.

Το στοιχείο SignatureValue περιέχει την πραγματική τιμή της ψηφιακής υπογραφής. Κωδικοποιείται πάντα χρησιμοποιώντας την base64.

Το στοιχείο KeyInfo είναι ένα προαιρετικό στοιχείο που επιτρέπει τον παραλήπτη να λάβει το κλειδί που απαιτείται για να επικυρώσει την υπογραφή. Το KeyInfo μπορεί να περιέχει κλειδιά, ονόματα, πιστοποιητικά και άλλες πληροφορίες διαχείρισης δημόσιου κλειδιού.

Το στοιχείο Object είναι ένα προαιρετικό στοιχείο που μπορεί να εμφανιστεί μια ή περισσότερες φορές. Όταν εμφανίζεται, αυτό το στοιχείο μπορεί να περιέχει οποιαδήποτε δεδομένα. Το στοιχείο Object μπορεί να περιλαμβάνει τον τύπο MIME, την ταυτότητα και τα χαρακτηριστικά κωδικοποίησης.

3.2. XML Κρυπτογράφηση

Οι βασικοί στόχοι της XML κρυπτογράφησης (XML Encryption) [28, 29] είναι:

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

- Παρουσίαση των κρυπτογραφημένων δεδομένων σε XML μορφή.
- Είναι δυνατό τμήματα του XML να κρυπτογραφηθούν επιλεκτικά.

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

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

Τα βασικά στοιχεία μιας κρυπτογράφησης XML είναι:

Το EncryptionMethod είναι ένα προαιρετικό στοιχείο που περιγράφει τον αλγόριθμο κρυπτογράφησης που εφαρμόζεται στα cipher δεδομένα. Εάν το στοιχείο απουσιάζει, ο αλγόριθμος κρυπτογράφησης πρέπει να γίνει γνωστός από τον παραλήπτη αλλιώς η αποκρυπτογράφηση θα αποτύχει.

Το ds:KeyInfo είναι ένα προαιρετικό στοιχείο, που ορίζεται στις ψηφιακές υπογραφές XML, το οποίο φέρει πληροφορίες για το κλειδί που χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα.

Το CipherData είναι ένα υποχρεωτικό στοιχείο που παρέχει τα κρυπτογραφημένα δεδομένα. Πρέπει να περιέχει την κρυπτογραφημένη ακολουθία ως κωδικοποιημένο base64 κείμενο του στοιχείου CipherValue, ή να παρέχει μια αναφορά σε μια εξωτερική θέση που περιέχει την κρυπτογραφημένη ακολουθία μέσω του στοιχείου CipherReference.

Το EncryptionProperties μπορεί να περιέχει πρόσθετες πληροφορίες σχετικά με την παραγωγή του EncryptedType (π.χ. date/time stamp ή ο αύξων αριθμός του κρυπτογραφικού υλικού που χρησιμοποιείται κατά τη διάρκεια της κρυπτογράφησης).

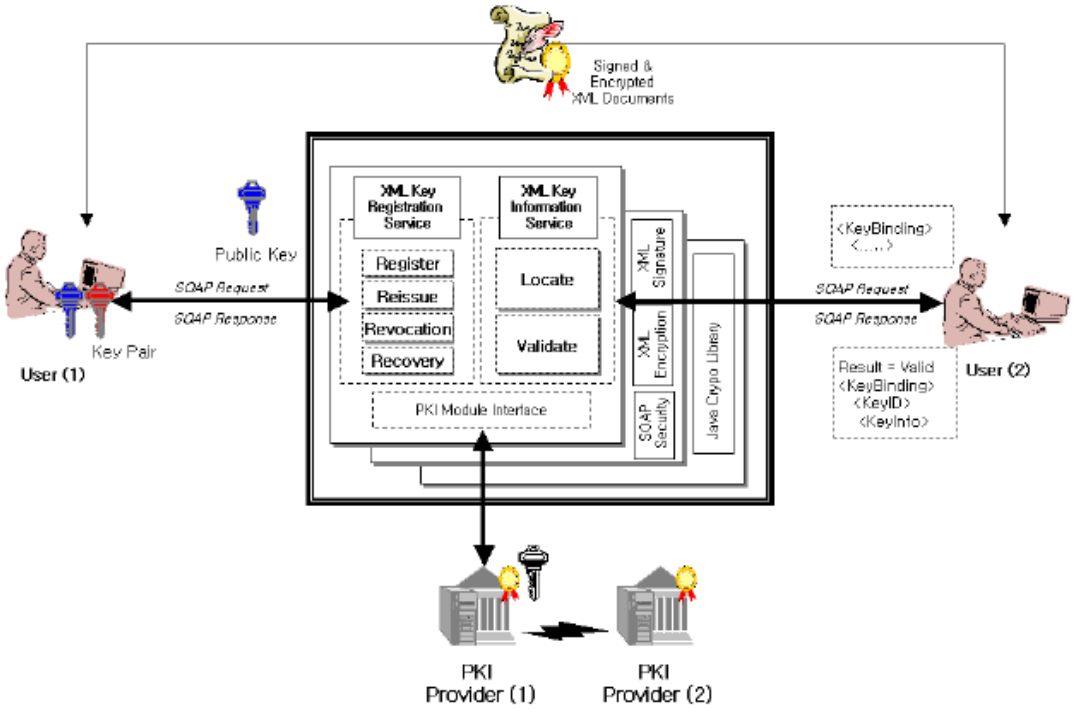
3.3. XML Key Management Specification (XKMS)

Μια από τις μεγαλύτερες απαιτήσεις για την ανάπτυξη όλων αυτών των νέων τεχνολογιών κρυπτογράφησης, ψηφιακών υπογραφών και πιστοποίησης, είναι να διατηρηθούν όλα τα δημόσια και ιδιωτικά κλειδιά, οι ψηφιακές υπογραφές και τα ψηφιακά πιστοποιητικά οργανωμένα και ασφαλή. Αρκετά προϊόντα υποδομής δημόσιου κλειδιού (PKI) της αγοράς σχεδιάστηκαν για να

απλοποιήσουν τη διαχείριση αυτών των συστατικών ασφάλειας. Παρόλα αυτά, δεν υπάρχει ακόμα ένας πρότυπος τρόπος για την προσπέλαση τέτοιων συστημάτων σε ένα περιβάλλον υπηρεσιών ιστού βασισμένων στο πρωτόκολλο SOAP.

Η XKMS [8, 9, 26] δημιουργήθηκε κάτω από την επίβλεψη του W3C, με σκοπό να παρέχει ένα τυποποιημένο σύνολο XML ορισμών για τη διαχείριση των υπηρεσιών πιστοποίησης, κρυπτογράφησης και ψηφιακών υπογραφών. Αυτό επιτρέπει στους σχεδιαστές να έχουν μια έμπιστη τρίτη οντότητα που βρίσκει και παρέχει τα κατάλληλα κλειδιά και πιστοποιητικά. Αυτή η έμπιστη τρίτη οντότητα ενεργεί σαν μεσάζοντας, ο οποίος απελευθερώνει τον προγραμματιστή της υπηρεσίας ιστού από την υποχρέωση να ελέγχει τη διαθεσιμότητα των κλειδιών ή των πιστοποιητικών και να εξασφαλίζει την εγκυρότητά τους. Η αρχιτεκτονική της υπηρεσίας XKMS παρουσιάζεται στην εικόνα 4.

Η XKMS περιλαμβάνει δυο μέρη: την XML Key Information Service Specification (X-KISS) και την XML Key Registration Service Specification (X-KRSS). Και οι δύο αυτές προδιαγραφές βασίζονται στη γλώσσα XML, χρησιμοποιούν το SOAP και οι σχέσεις μεταξύ των μηνυμάτων καθορίζονται από την WSDL. Παρόλα αυτά μπορούν να υπάρξουν εκφράσεις XKMS σε άλλο συμβατό σχήμα κωδικοποίησης.



Εικόνα 4. Αρχιτεκτονική της υπηρεσίας XKMS [26]

Η προδιαγραφή X-KISS καθορίζει ένα πρωτόκολλο για να υποστηρίζει την αποστολή από μια εφαρμογή σε μια υπηρεσία της επεξεργασίας της πληροφορίας κλειδιού που συνδέεται με μια

XML υπογραφή, μια XML κρυπτογράφηση, ή άλλη χρήση του στοιχείου <ds:KeyInfo> της XML υπογραφής.

Η X-KISS επιτρέπει σε έναν πελάτη μιας τέτοιας υπηρεσίας να αποστείλει μέρος ή όλες τις εργασίες που απαιτούνται για την επεξεργασία των στοιχείων <ds:KeyInfo> μιας XML υπογραφής σε μια XKMS υπηρεσία. Ένας βασικός στόχος του σχεδιασμού του πρωτοκόλλου είναι να ελαχιστοποιήσει την πολυπλοκότητα των εφαρμογών. Ως πελάτης της XKMS υπηρεσίας, η εφαρμογή απαλλάσσεται από την πολυπλοκότητα και τη σύνταξη του ελλοχεύοντος PKI που χρησιμοποιείται για να καθιερώσει σχέσεις εμπιστοσύνης. Το ελλοχεύον PKI μπορεί να βασίζεται σε μια διαφορετική προδιαγραφή όπως X.509/PKIX, SPKI ή PGP. Η προδιαγραφή X-KISS περιλαμβάνει δυο λειτουργίες:

Locate: Η υπηρεσία αυτή αναλύει ένα στοιχείο <ds:Keyinfo>, αλλά δεν απαιτεί από την υπηρεσία να κάνει μια δήλωση σχετικά με την ισχύ των δεδομένων που συνδέονται στο στοιχείο <ds:Keyinfo>.

Validate: Η υπηρεσία αυτή επιτρέπει όλα αυτά που κάνει η υπηρεσία Locate και επιπλέον, ο πελάτης μπορεί να λάβει μια δήλωση που διευκρινίζει την κατάσταση της σύνδεσης μεταξύ του δημόσιου κλειδιού και άλλων δεδομένων. Επιπλέον, η υπηρεσία αντιπροσωπεύει ότι η κατάσταση κάθε στοιχείου δεδομένων που επιστρέφεται είναι έγκυρο και ότι όλα είναι συνδεδεμένα στο ίδιο δημόσιο κλειδί.

Οι λειτουργίες Locate και Validate χρησιμοποιούνται και οι δύο για να λάβουν πληροφορία για ένα δημόσιο κλειδί από μια υπηρεσία XKMS και προσπαθούν και οι δύο να παρέχουν τη σωστή πληροφορία στον αιτούντα. Οι υπηρεσίες Locate και Validate διαφέρουν στο βαθμό στον οποίο η υπηρεσία εγγυάται για την αξιοπιστία της επιστρεφόμενης πληροφορίας. Μια υπηρεσία Locate πρέπει να προσπαθήσει να παρέχει μόνο πληροφορία που είναι αξιόπιστη στο καλύτερο της γνώσης της, αλλά δεν παρέχει οποιαδήποτε διαβεβαίωση ότι θα το κάνει. Μια υπηρεσία Validate αναλαμβάνει να επιστρέψει μόνο την πληροφορία που ήταν θετικά επικυρωμένη από την υπηρεσία XKMS επειδή ικανοποιεί συγκεκριμένα κριτήρια επικύρωσης.

Κανένα ενιαίο σύνολο κριτηρίων επικύρωσης δεν είναι κατάλληλο για κάθε περίσταση. Εφαρμογές που περιλαμβάνουν οικονομικές συναλλαγές είναι πιθανό να απαιτήσουν την εφαρμογή πολύ ειδικών κριτήριων επικύρωσης.

Η προδιαγραφή X-KRSS καθορίζει ένα πρωτόκολλο για μια υπηρεσία ιστού που δέχεται καταχώρηση των πληροφοριών δημόσιων κλειδιών. Μόλις καταχωρηθεί, το δημόσιο κλειδί μπορεί να χρησιμοποιηθεί από κοινού με την X-KISS, ή μια υποδομή δημόσιου κλειδιού (PKI) όπως τα X.509 και PKIX [11].

Η X-KRSS περιγράφει ένα πρωτόκολλο για την καταχώρηση και την επακόλουθη διαχείριση των πληροφοριών δημόσιου κλειδιού. Το πρωτόκολλο επιτρέπει την πιστοποίηση του αιτούντος και στην περίπτωση που το ζευγάρι κλειδιών παράγεται από τον πελάτη, απόδειξη της κατοχής (Proof of Possession) του ιδιωτικού κλειδιού. Ένα μέσο της μετάδοσης του ιδιωτικού κλειδιού στον πελάτη παρέχεται στην περίπτωση που το ιδιωτικό κλειδί παράγεται από την υπηρεσία καταχώρησης.

Η προδιαγραφή X-KRSS υποστηρίζει τις λειτουργίες που αναφέρονται παρακάτω. Σημειώνεται ότι μια υπηρεσία XKMS μπορεί να προσφέρει όλες ή καμία από αυτές τις λειτουργίες.

Register: Η πληροφορία είναι συνδεδεμένη σε ένα ζευγάρι δημόσιου κλειδιού μέσω μιας σύνδεσης κλειδιού.

Reissue: Μια προηγουμένως καταχωρημένη σύνδεση κλειδιού επανεκδίδεται.

Revoke: Μια προηγουμένως καταχωρημένη σύνδεση κλειδιού ανακαλείται.

Recover: Το ιδιωτικό κλειδί που συνδέεται με μια σύνδεση κλειδιού ανακτάται.

Η XKMS έχει πολλά πλεονεκτήματα, τα σημαντικότερα από τα οποία είναι:

- Ευκολία στη χρήση: Η φιλική για τον προγραμματιστή σύνταξη που χρησιμοποιείται στο XKMS αποβάλλει την ανάγκη για εργαλεία PKI. Η προδιαγραφή XKMS επιτρέπει στους προγραμματιστές να υλοποιούν γρήγορα χαρακτηριστικά εμπιστοσύνης, που ενσωματώνουν κρυπτογραφική υποστήριξη για τις XML ψηφιακές υπογραφές και την XML κρυπτογράφηση χρησιμοποιώντας τα τυποποιημένα εργαλεία XML.
- Γρήγορη στην ανάπτυξη: Με την απλούστευση της ανάπτυξης εφαρμογών, η XKMS αφαιρεί την ανάγκη για ανάπτυξη PKI και αντ' αυτού, μετακινεί την πολυπλοκότητα του PKI στα τμήματα από την πλευρά του διακομιστή.
- Ανοικτό πρότυπο: Η XKMS είναι ένα ανοικτό πρότυπο για διανομή και καταχώριση κλειδιών.
- Αντοχή στο χρόνο: Υποστηρίζει τις νέες και αναδυόμενες εξελίξεις του PKI, δεδομένου ότι οι μελλοντικές εξελίξεις PKI είναι περιορισμένες σε συστατικά από την πλευρά του server.

3.4. Security Assertion Markup Language (SAML)

Η SAML [22, 25] έχει αναπτυχθεί από την OASIS XML-Based Security Services Technical Committee (SSTC). Είναι ένα πλαίσιο βασισμένο σε XML για την ανταλλαγή ασφαλούς πληροφορίας. Αυτή η ασφαλής πληροφορία εκφράζεται στη μορφή των δηλώσεων γύρω από

υποκείμενα, όπου ένα υποκείμενο είναι μια οντότητα (άνθρωπος ή υπολογιστής) η οποία έχει μια ταυτότητα σε μερικά ασφαλή πεδία. Ένα τυπικό παράδειγμα ενός υποκειμένου είναι ένα άτομο, ταυτοποιημένο από τη διεύθυνση του ηλεκτρονικού ταχυδρομείου του σε ένα ειδικό internet DNS πεδίο. Οι δηλώσεις μπορούν να μεταφέρουν πληροφορία σχετικά με ενέργειες αυθεντικοποίησης και θέματα εξουσιοδότησης σχετικά με το πότε τα υποκείμενα επιτρέπεται να έχουν πρόσβαση σε κάποιους πόρους.

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

Η ασφάλεια εντός των υπηρεσιών ιστού ακόμη δεν έχει οριστεί πλήρως, περισσότερη ανάλυση έχει γίνει στο πώς παρέχονται οι υπηρεσίες εμπιστευτικότητας και αυθεντικοποίησης, ταυτοποίησης σε μια από άκρο σε άκρο (end-to-end) θεμελίωση. Το πρότυπο SAML παρέχει τα μέσα με τα οποία αυθεντικοποιημένες και εξουσιοδοτημένες δηλώσεις μπορούν να ανταλλάσσονται μεταξύ των ομάδων που επικοινωνούν.

3.5. eXtensible Access Control Markup Language (XACML)

Η XACML [23, 24] ακολουθήθηκε για να ορίσει ένα βασικό σχήμα για τη δήλωση των πολιτικών εξουσιοδότησης σε XML έναντι αντικειμένων τα οποία ταυτοποιούνται από μόνα τους σε XML.

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

Πολλές από τις υπάρχουσες γλώσσες δεν υποστηρίζουν κατανεμημένες πολιτικές, δεν είναι εκτεταμένες ή δεν είναι εκτεταμένες αρκετά ώστε να υποστηρίξουν καινούργιες απαιτήσεις. Η XCAML επιτρέπει τη χρήση αυθαίρετων χαρακτηριστικών στις πολιτικές, τον έλεγχο προσπέλασης βασισμένο σε ρόλους (role based access control), τις πολιτικές ευρετηρίου, τις ετικέτες ασφάλειας, τις πολιτικές βασισμένες σε ώρα/ημέρα, δυναμικές πολιτικές και όλα αυτά χωρίς να απαιτούνται αλλαγές στις εφαρμογές οι οποίες χρησιμοποιούν XACML.

Μερικές βασικές απαιτήσεις πολιτικής της γλώσσας είναι [12]:

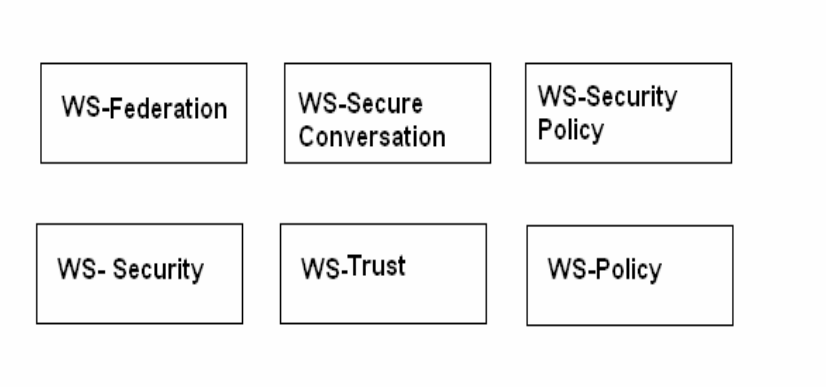
- Να παρέχει μια μέθοδο για να συνδυάζει ανεξάρτητους κανόνες και πολιτικές σε ένα ξεχωριστό σύνολο πολιτικής, το οποίο απευθύνεται σε ένα συγκεκριμένο αίτημα απόφασης.
- Να παρέχει μια μέθοδο για ευέλικτο ορισμό της διαδικασίας στην οποία κανόνες και πολιτικές συνδυάζονται.
- Να παρέχει μια μέθοδο για το χειρισμό ενός κατανεμημένου συνόλου στοιχείων πολιτικής ενώ συνοψίζει τη μέθοδο για εγκατάσταση, ανάκτηση και αυθεντικοποίηση της πολιτικής των στοιχείων.

3.6. Μοντέλο Ασφάλειας Υπηρεσιών Ιστού (Web Services Security Model)

Οι εταιρείες IBM και Microsoft συνεργάστηκαν για να αναπτύξουν ένα σύνολο από προδιαγραφές ασφάλειας, οι οποίες απευθύνονται στο πως παρέχεται η προστασία στα ανταλλασσόμενα μηνύματα σε ένα περιβάλλον υπηρεσίας ιστού.

Δημιούργησαν ένα μοντέλο ασφάλειας [12] το οποίο φέρνει μαζί τεχνολογίες όπως είναι υποδομή δημόσιου κλειδιού και ο Κέρβερος που άλλοτε θεωρούνταν ασύμβατες. Εν συντομία, αυτό δεν είναι ένα εξιδανικευμένο πλαίσιο αλλά ένα χρήσιμο πλαίσιο το οποίο επιτρέπει την μας οικοδόμηση μιας ασφαλούς υπηρεσίας ιστού.

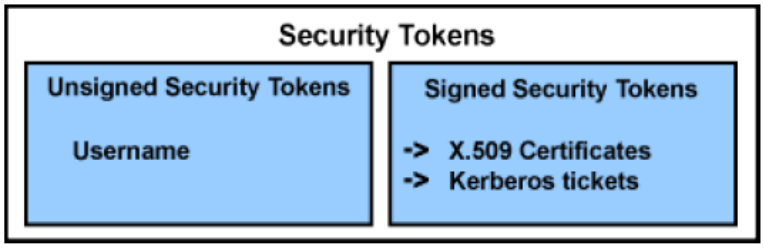
Ένα ευρύ σύνολο από προδιαγραφές ασφάλειας περιέχονται σ' αυτό το μοντέλο (εικόνα 5). Αυτές οι προδιαγραφές καλύπτουν τεχνολογίες ασφάλειας συμπεριλαμβανομένων της ακεραιότητας, της εμπιστευτικότητας, της αυθεντικοποίησης, της εξουσιοδότησης, των ασφαλών διαδρομών επικοινωνίας, της εμπιστοσύνης, των ασφαλών περιβαλλόντων και της πολιτικής ασφάλειας.



Εικόνα 5. Προδιαγραφές Ασφάλειας Υπηρεσιών Ιστού.

Η WS-Security, η WS-Trust και η WS-Policy είναι οι αρχικές προδιαγραφές, οι οποίες παρέχουν τη θεμελίωση σύμφωνα με την οποία μπορούμε να εργαστούμε ώστε να ιδρύσουμε ασφαλείς υπηρεσίες ιστού δια μέσου έμπιστων περιοχών.

Η WS-Security προδιαγραφή [12, 16] περιγράφει τον τρόπο με τον οποίο επισυνάπτονται οι υπογραφές και οι κρυπτογραφημένες κεφαλίδες στα SOAP μηνύματα. Επιπρόσθετα, περιγράφει πως επισυνάπτονται τα τεκμήρια ασφάλειας (εικόνα 6) στα μηνύματα. Τεκμήριο ασφάλειας ορίζουμε την αναπαράσταση της πληροφορίας που σχετίζεται με την ασφάλεια (π.χ. X.509 πιστοποιητικά, Κέρβερος ετικέτες, usernames, τεκμήρια ασφάλειας κινητών συσκευών από κάρτες SIM). Υπογεγραμμένο τεκμήριο ασφάλειας ορίζεται ένα τεκμήριο ασφάλειας που περιέχει ένα σύνολο σχετικών δηλώσεων κρυπτογραφικά επικυρωμένων από έναν εκδότη (π.χ. X.509 πιστοποιητικά, Κέρβερος ετικέτες).



Εικόνα 6. Τεκμήρια ασφάλειας [12].

Η WS-Security προδιαγραφή αποτελεί έναν οικοδομικό λίθο, ο οποίος μπορεί να χρησιμοποιηθεί σε συνδυασμό με άλλα πρωτόκολλα υπηρεσιών ιστού για να διευθύνει μια μεγάλη ποικιλία απαιτήσεων ασφάλειας των εφαρμογών. Η ακεραιότητα μηνύματος παρέχεται από την ισχύ της XML υπογραφής και τα τεκμήρια ασφάλειας, για να εγγυηθούν ότι τα μηνύματα έχουν δημιουργηθεί από τον κατάλληλο αποστολέα και δεν έχουν μεταβληθεί κατά την μεταφορά. Ομοίως την εμπιστευτικότητα του μηνύματος παρέχει η XML κρυπτογράφηση και τα τεκμήρια ασφάλειας για να διατηρούνται τα τμήματα ενός SOAP μηνύματος εμπιστευτικά.

Η WS-Trust προδιαγραφή [18, 25] περιγράφει ένα μηχανισμό, ο οποίος λαμβάνει ένα τεκμήριο ασφάλειας και εγκαθιστά μια έμπιστη σχέση μεταξύ ομάδων. Ο αιτούμενος στέλνει μια αίτηση και εφόσον η πολιτική του το επιτρέπει, τότε οι απαιτήσεις του ικανοποιούνται. Ο αιτούμενος λαμβάνει ένα τεκμήριο ασφάλειας για την αποστολή. Αφού το τεκμήριο ασφάλειας ληφθεί επιτυχώς και χρησιμοποιηθεί σε μια αίτηση, τα μηνύματα SOAP της χρησιμοποιούμενης ομάδας είναι έμπιστα. Η WS-Trust θεωρείται ως ανεπαρκές εργαλείο για τη δημιουργία ενός περιβάλλοντος εμπιστοσύνης, εφόσον απαιτούνται κλιμακωτά επίπεδα εμπιστοσύνης.

Η τελευταία ενημερωμένη WS-Trust προδιαγραφή χρησιμοποιεί ασφαλείς μηχανισμούς αποστολής μηνυμάτων της WS-Security για να ορίσει πρόσθετα στοιχεία και προεκτάσεις με σκοπό την ανταλλαγή του τεκμήριου ασφάλειας, ώστε να επιτρέψει την έκδοση και την διασπορά των διαπιστευμένων μηνυμάτων εντός των έμπιστων περιοχών.

Για να επιτύχουμε μια ασφαλή επικοινωνία μεταξύ δύο ομάδων, οι ομάδες πρέπει να ανταλλάσουν διαπιστευτήρια ασφάλειας (έμμεσα ή άμεσα). Ωστόσο, κάθε ομάδα χρειάζεται να προσδιορίσει αν μπορεί να εμπιστευτεί τα ισχυριζόμενα διαπιστευτήρια της άλλης ομάδας. Αυτή η προδιαγραφή ορίζει προεκτάσεις της WS-Security για την εκπομπή και την ανταλλαγή τεκμηρίων ασφάλειας και τρόπους ώστε να προσπελαύνουν στο χώρο των έμπιστων συσχετίσεων.

Η WS-Policy προδιαγραφή [14] παρέχει ένα μοντέλο γενικού σκοπού και συντακτική για να περιγράφει και να επικοινωνεί με τις πολιτικές των υπηρεσιών ιστού. Η WS-Policy ορίζει ένα βασικό σύνολο σχεδίων τα οποία μπορούν να χρησιμοποιηθούν και να επεκταθούν από άλλες προδιαγραφές υπηρεσιών ιστού για να περιγράψουν γενικής κλίμακας απαιτήσεις υπηρεσίας, αναφορές και δυνατότητες. Άλλες προδιαγραφές είναι ελεύθερες να ορίσουν τεχνολογικά ειδικούς μηχανισμούς για να συνδέσουν την πολιτική με διάφορες οντότητες και πόρους. Διαδοχικές προδιαγραφές παρέχουν το προφίλ της χρήσης του WS-Policy μέσα σε άλλες γενικές τεχνολογίες υπηρεσίας ιστού.

Η WS-Federation προδιαγραφή [13, 27] ορίζει μηχανισμούς, οι οποίοι επιτρέπουν διαφορετικά «βασίλεια» ασφάλειας να συνδέονται ομοσπονδιακά χρησιμοποιώντας διαφορετικούς ή παρόμοιους μηχανισμούς. Σε μια ομοσπονδία μοναδικά υπογεγραμμένη, ένας χρήστης αυθεντικοποιείται σε ένα μια πύλη εσωτερικά της ομοσπονδίας των υπηρεσιών ιστού. Αφού έχει επιτυχώς αυθεντικοποιηθεί μπορεί να χρησιμοποιήσει άλλες πύλες χωρίς να αυθεντικοποιηθεί επειδή οι πύλες έχουν συνδεθεί μέσω των παροχέων πιστοποίησης. Με αυτό τον τρόπο τα δεδομένα περνούν από μια πύλη σε άλλη.

Η WS-SecureConversation προδιαγραφή [15] ορίζει μηχανισμούς για την εγκατάσταση και την διαμοίραση ασφαλών περιβαλλόντων και παραγωγής κλειδιών, ώστε να καθιστούν ικανή μια ασφαλή επικοινωνία. Σε αντίθεση με την WS-security προδιαγραφή, η οποία εστιάζεται στο μοντέλο της αυθεντικοποίησης του μηνύματος, αλλά όχι σε ένα ασφαλή περιβάλλον και συνεπώς είναι αντικείμενο πολλών τύπων επιθέσεων ασφάλειας.

Η WS-SecurityPolicy προδιαγραφή [17] ορίζει ένα σύνολο δηλώσεων πολιτικής ασφάλειας, οι οποίες απευθύνονται στην ασφάλεια υπηρεσιών ιστού, όπως είναι ασφάλεια SOAP μηνυμάτων, η WS-Trust και η WS-SecureConversation προδιαγραφή. Ορίζει ένα σύνολο από δηλώσεις οι οποίες περιγράφουν πως τα μηνύματα μπορεί να είναι ασφαλή. Αλγόριθμοι

κρυπτογράφησης και μηχανισμοί χρησιμοποιούνται για να επιτύχουν ασφάλεια σε επίπεδο μεταφοράς.

4. Συμπεράσματα

Η XML θεωρείται ένας πολύτιμος μηχανισμός για την ανταλλαγή δεδομένων μέσω του διαδικτύου. Το SOAP, ένα πρωτόκολλο για αποστολή μηνυμάτων XML, διευκολύνει τη διαδικασία ενδοεπικοινωνίας με τρόπους που δεν ήταν δυνατοί πιο πριν, ενώ το UDDI φαίνεται να γίνεται γρήγορα το πρότυπο για τη συγκέντρωση των υπηρεσιών του ιστού. Οι ίδιες οι υπηρεσίες περιγράφονται από την XML σε WSDL έγγραφα. Χωρίς την XML, αυτή η ευελιξία δεν θα ήταν εφικτή.

Ένας άλλος τομέας ταχείας ανάπτυξης είναι αυτός της ασφάλειας. Οι παραδοσιακές μέθοδοι εγκαθίδρυσης εμπιστοσύνης μεταξύ των συμβαλλόμενων μερών δεν είναι κατάλληλες στο διαδίκτυο ή σε μεγάλα δίκτυα LAN ή WAN.

Τεχνολογίες ασφάλειας υπάρχουν για πιστοποίηση και εξουσιοδότηση (SAML), για διαχείριση δημόσιου κλειδιού (XKMS), για επικύρωση της προέλευσης των μηνυμάτων (XML ψηφιακές υπογραφές), για τη δήλωση πολιτικών εξουσιοδότησης (XACML) και για την εμπιστευτικότητα (XML κρυπτογράφηση). Πέρα από αυτές τις τεχνολογίες η Microsoft και η IBM ανέπτυξαν ένα σύνολο από προδιαγραφές ασφάλειας για να παρέχουν προστασία σε ένα περιβάλλον υπηρεσίας ιστού.

5. Αναφορές

[1] C. Albrecht, “How clean is the future of SOAP”, *Communications of the ACM*, Vol. 47, No. 2, February 2004.

[2] T. Bray, J. Paoli, C. M. Sperberg-McQueen, F. Yergeau, “Extensible Markup Language (XML) 1.0 (Third Edition)”, W3C Recommendation, February 2004.

[3] E. Cerami, *“Web Services Essentials”*, O’ Reilly publications, First edition, February 2002.

[4] D. Chappell and T. Jewell, *“JAVA Web Services”*, O’ Reilly publications, First edition, March 2002.

[5] D. Eastlake, J. Reagle, D. Solo, “XML-Signature Syntax and Processing”, IETF RFC 3275, March 2002, http://www.ietf.org/rfc/rfc3275.txt.

[6] M. Gudgin, M. Hadley, N. Mendelsohn, J. Moreau, H. F. Nielsen, "SOAP Version 1.2 Part 1: Messaging Framework", W3C Recommendation, June 2003.

[7] M. Gudgin, M. Hadley, N. Mendelsohn, J. Moreau, H. F. Nielsen, "SOAP Version 1.2 Part 2: Adjuncts", W3C Recommendation, June 2003.

[8] P. Hallam-Baker, S. H. Mysore, "XML Key Management Specification (XKMS 2.0)", W3C Recommendation 28 June 2005, http://www.w3.org/TR/xkms2/.

[9] P. Hallam-Baker, S. H. Mysore, "XML Key Management Specification (XKMS 2.0) Bindings", W3C Recommendation 28 June 2005, http://www.w3.org/TR/xkms2-bindings/.

[10] M. Hondo, N. Nagaratnam, A. Nadalin, "Securing Web services", *IBM Systems Journal*, Vol 41, 228 No 2, 2002.

[11] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF RFC 2459, January 1999, http://www.ietf.org/rfc/rfc2459.txt.

[12] IBM, "Security in a Web Services World: A Proposed Architecture and Roadmap", April 2002, http://www.128.ibm.com/developerworks/webservices/library/specification/ws-secmap/.

[13] IBM, "Web Services Federation Language (WS-Federation)", July 2003, http://www-128.ibm.com/developerworks/library/specification/ws-fed/.

[14] IBM, "Web Services Policy Framework (WS-Policy)", September 2004, http://www-128.ibm.com/developerworks/webservices/library/specification/ws-polfram/.

[15] IBM, "Web Services Secure Conversation Language (WS-SecureConversation)", February 2005, http://www.128.ibm.com/developerworks/webservices/library/specification/ws-secon/.

[16] IBM, "Web Services Security (WS-Security)", April 2002, http://www-128.ibm.com/developerworks/webservices/library/specification/ws-secure/.

[17] IBM, "Web Services Security Policy Language (WS-SecurityPolicy)", July 2005, http://www-128.ibm.com/developerworks/webservices/library/specification/ws-secpol/.

[18] IBM, "Web Services Trust Language (WS-Trust)", February 2005, http://www-128.ibm.com/developerworks/library/specification/ws-trust/.

[19] N. Mitra, "SOAP Version 1.2 Part 0: Primer", W3C Recommendation, June 2003.

[20] E. Newcomer, "*Understanding Web Services XML, WSDL, SOAP, and UDDI*", Addison-Wesley publications, September 2002.

[21] M. O'Neill, "*Web Services Security*", McGraw-Hill Osborne Media, January 2003.

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

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

[24] OASIS, "eXtensible Access Control Markup Language (XACML) Version 1.0," February 2003, http://www.oasis-open.org/committees/xacml/repository/.

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

[26] N. Park, K. Moon, S. Sohn, "Certificate Validation Service using XKMS for Computational Grid", *ACM Workshop on XML Security 2003*,Washington., USA 2003.

[27] C. Platzer, *"Trust-based Security in Web Services''*, Master's Thesis, Technical University of Vienna, May 2004.

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

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

[30] A. Skonnard, "SOAP: The Simple Object Access Protocol", Technical report, Microsoft, 2001, http://www.microsoft.com/mind/0100/soap/soap.asp.

[31] UDDI, "UDDI Spec Technical Committee Draft 20041019", 2004, http://uddi.org/pus/uddi-v3.0.2.-20040109.htm

[32] World Wide Web Consortium (W3C), "Web Services Description Language (WSDL) 1.1", 2001, http://www.w3.org/TR/wsdl/.