ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Π.Μ.Σ. «ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ & ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

« Αξιολόγηση των γλωσσών αποτύπωσης πολιτικών ασφάλειας (γλώσσα XACML) και υλοποίηση μιας πρότυπης πολιτικής ασφάλειας »

ΚΑΦΡΙΤΣΑ ΜΑΡΙΑ

Α.Μ.: 1111

Επιβλέπων:
Λαμπρινουδάκης Κωνσταντίνος, Καθηγητής

Ιούνιος 2013

Περίληψη

Θέμα της διπλωματικής εργασίας είναι η μελέτη και αξιολόγηση της γλώσσας αποτύπωσης πολιτικών ασφαλείας XACML, καθώς και η χρήση της για υλοποίηση μιας πρότυπης πολιτικής ασφάλειας, που ρυθμίζει τον έλεγχο πρόσβασης των χρηστών σε ένα Πληροφοριακό Σύστημα στον χώρο της Υγείας.

Δομή Εργασίας

Η εργασία ακολουθεί της εξής δόμηση:

- Το 1^{ο} κεφάλαιο παρέχει μια εισαγωγή στο επιστημονικό πεδίο του ελέγχου πρόσβασης και στο OASIS πρότυπο eXtensible Access Control Markup Language (XACML) V3.0. Παρουσιάζεται επίσης το μοντέλο Attribute Based Access Control (ABAC), που υποστηρίζεται από το πρότυπο XACML.
- Το 2^{ο} κεφάλαιο ασχολείται με τα βασικά στοιχεία που απαρτίζουν ένα Πληροφοριακό Σύστημα Υγείας, όπως οι διαφορετικού είδους χρήστες και η μορφή και ο τύπος των πόρων του συστήματος. Επιπρόσθετα, παρουσιάζεται το περιβάλλον WSO2 Identity Server, που χρησιμοποιήθηκε για την ανάπτυξη της πολιτικής ασφάλειας του συστήματος.
- Το 3^{ο} κεφάλαιο αναλύει την συνολική πολιτική ασφάλειας που αναπτύχθηκε, καθώς και τις επιμέρους πολιτικές ασφάλειας, που αυτή περιλαμβάνει, και τυγχάνουν εφαρμογής για αιτήματα συγκεκριμένων ρόλων χρηστών. Παρουσιάζεται, επίσης, η απόκριση του Πληροφοριακού Συστήματος σε διάφορα αιτήματα πρόσβασης και επαληθεύεται με αυτόν το τρόπο η ορθότητα της υλοποίησης.
- Το 4^{ο} κεφάλαιο ολοκληρώνει την εργασία αξιολογώντας την γλώσσα XACML και κατ' επέκταση το πρότυπο.

Summary

The subject of the present diploma thesis is the study and evaluation of XACML policy language. Furthermore, XACML is being utilized for expressing the security policy that regulates the access control function for users of an eHealthcare Information System.

Structure

The thesis is structured as follows:

- Chapter 1 provides an introduction to the field of access control and to OASIS standard, eXtensible Access Control Markup Language (XACML) V3.0. Also, Attribute Based Access Control (ABAC) model is being depicted as a supported mechanism by XACML.
- Chapter 2 describes the basic components that are being included in a Healthcare Information System, that is the different kind of users and the type of resources encountered. WSO2 Identity Server is also presented in this chapter, since it is the development environment for the security policy.
- Chapter 3 analyzes the whole policy set and the separate policies that constitute the policy set, which are applicable to decision requests from specific user roles. Also, different requests are being applied to the system and the corresponding responses are being presented for determining the correctness of the security policy implemented.
- Chapter 4 concludes the present diploma thesis with an evaluation of the XACML policy language and standard.

Πίνακας περιεχομένων

Πίνακας Εικόνων

1. Το Πρότυπο XACML

1.1 Η έννοια του Ελέγχου Πρόσβασης

Μία από τις σημαντικότερες απαιτήσεις οποιουδήποτε συστήματος διαχείρισης πληροφοριών, είναι η προστασία των δεδομένων και των πόρων του ενάντια στην μη επιτρεπόμενη γνωστοποίηση (μυστικότητα) και τις αναρμόδιες τροποποιήσεις (ακεραιότητα), εξασφαλίζοντας συγχρόνως την διαθεσιμότητά τους για τους νόμιμους χρήστες (καμία άρνηση υπηρεσίας).
Η επιβολή της προστασίας επομένως απαιτεί ότι κάθε πρόσβαση σε ένα σύστημα και στους πόρους του ελέγχεται και ότι μόνο οι εξουσιοδοτημένες προσβάσεις μπορούν να πραγματοποιηθούν. Η προαναφερόμενη διαδικασία ορίζει την έννοια *του* ***ελέγχου πρόσβασης***.
Η XACML είναι μια δηλωτική γλώσσα πολιτικών ελέγχου πρόσβασης, που υλοποιείται με XML, καθώς επίσης και ένα μοντέλο επεξεργασίας που περιγράφει πώς ερμηνεύονται οι πολιτικές.

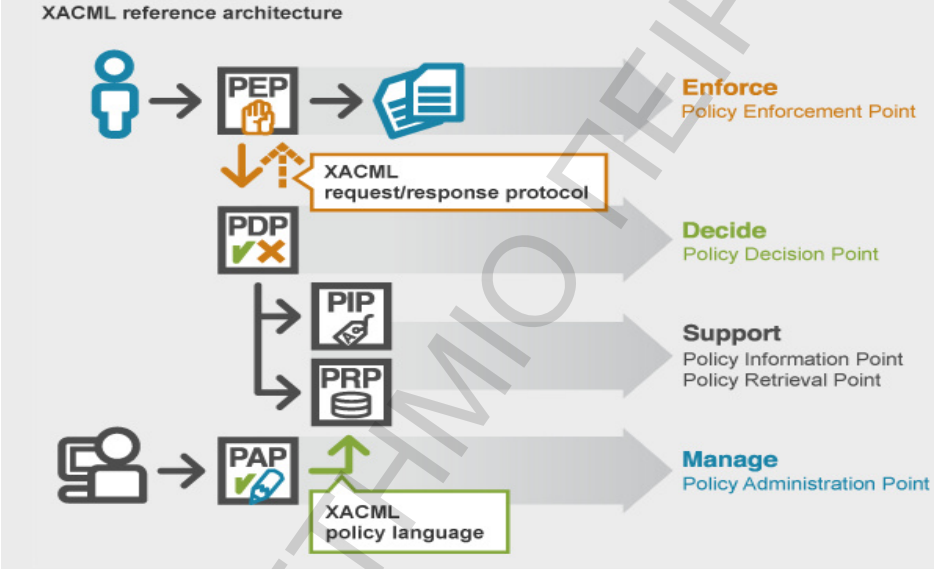
1.2 Η XACML ως ένα Ολοκληρωμένο Πρότυπο Ελέγχου Πρόσβασης

Η XACML είναι ένα OASIS πρότυπο που περιγράφει τόσο μια γλώσσα πολιτικών, η οποία υλοποιείται με XML, όσο και μια γλώσσα αιτήματος/απάντησης για την απόφαση του ελέγχου πρόσβασης. Αυτή η γλώσσα πολιτικής απαριθμεί τις γενικές απαιτήσεις ελέγχου πρόσβασης, και έχει τα τυποποιημένα σημεία επέκτασης για τον καθορισμό νέων συναρτήσεων, τύπων δεδομένων, συνδυαστικής λογικής, κ.λπ. Η γλώσσα αιτήματος/απάντησης επιτρέπει την διαμόρφωση ερωτήσεων για το εάν μια δεδομένη ενέργεια πρέπει ή όχι να επιτραπεί. Η απάντηση περιλαμβάνει πάντα μια από τις τέσσερις τιμές: Permit, Deny, Indeterminate (ένα λάθος εμφανίστηκε ή κάποια απαραίτητη τιμή έλειπε, έτσι μια απόφαση δεν μπορεί να ληφθεί) ή Not Applicable (το αίτημα δεν μπορεί να απαντηθεί από αυτήν την υπηρεσία).

Το πρότυπο XACML τυποποιεί τρεις ουσιαστικές πτυχές της διαδικασίας έγκρισης:

- XACML γλώσσα πολιτικών: μια πλούσια attribute-based γλώσσα πολιτικών με την οποία κανόνες ελέγχου πρόσβασης μπορούν να συνδυαστούν σε περίπλοκες και εξεζητημένες πολιτικές. Πολλές πολιτικές και σετ πολιτικών μπορούν να συνδυαστούν σε ακόμη μεγαλύτερα σύνολα πολιτικών. Ευέλικτοι συνδυαστικοί αλγόριθμοι καθορίζουν το πώς οι κανόνες ενώνονται για να αποδώσουν την ακριβή έννοια συλλογικών πολιτικών, όμοια με τον τρόπο που η γραμματική μιας φυσικής γλώσσας μας επιτρέπει να εκφράσουμε τις ακριβείς οδηγίες.

- XACML πρωτόκολλο αίτησης/απάντησης, το οποίο χρησιμοποιείται για ερωτήσεις σε μια μηχανή αποφάσεων που αξιολογεί αιτήσεις πρόσβασης του «πραγματικού» κόσμου με βάση υπάρχουσες XACML πολιτικές. Τα αποτέλεσμα, είτε είναι θετικό ή αρνητικό επιστρέφεται σαν μια XACML απάντηση.
- Αρχιτεκτονική αναφοράς XACML (Σχήμα 1), στον πυρήνα της οποίας, το Σημείο Απόφασης Πολιτικών (Policy Decision Point-PDP) εκτιμά τις αιτήσεις πρόσβασης που παρέχονται από το Σημείο Επιβολής Πολιτικών (Policy enforcement Point-PEP). Τα PDP/PEP μπορούν επίσης να θέσουν ερώτηση στο Σημείο Πληροφοριών Πολιτικών (Policy Information Point-PIP) για να συγκεντρώσει περιγραφικές ιδιότητες σχετικά με το υποκείμενο ή τον πόρο για τον οποίο ζητείται πρόσβαση. Όλες οι πολιτικές διατηρούνται μέσω του Σημείου Διαχείρισης Πολιτικών (Policy Administration Point-PAP).



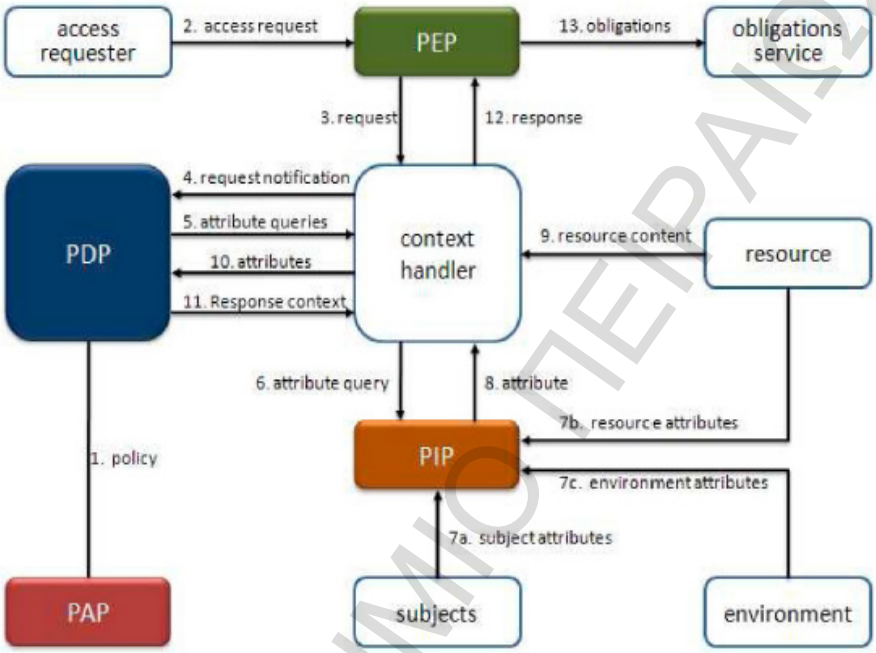
Σχήμα 1. Αρχιτεκτονική Αναφοράς XACML

1.3 Πλαίσιο Λειτουργίας της XACML

Το πρότυπο της XACML καθορίζει πέντε βασικά συστατικά που χειρίζονται τις αποφάσεις πρόσβασης:

- Policy Administration Point (PAP): το PAP αποτελεί την αποθήκη για τις πολιτικές και παρέχει τις πολιτικές στο PDP.
- Policy Enforcement Point (PEP): το PEP είναι η διεπαφή ολόκληρου του περιβάλλοντος με τον «έξω κόσμο». Λαμβάνει τα αιτήματα πρόσβασης, τα αξιολογεί και αναλόγως δίνει άδεια ή αρνείται την πρόσβαση στον πόρο.
- Policy Decision Point (PDP): το PDP είναι το κύριο σημείο των αποφάσεων όσον αφορά τα αιτήματα πρόσβασης. Αυτό είναι επιφορτισμένο με την συγκέντρωση όλης της απαραίτητης πληροφορίας από τις υπόλοιπες μονάδες και τελικά την εξαγωγή συμπερασμάτων-αποφάσεων.

- Policy Information Point (PIP): το PIP είναι το σημείο όπου ανακτώνται οι απαραίτητες ιδιότητες (attributes) για την εκτίμηση των πολιτικών, από διάφορες εξωτερικές ή εσωτερικές συνιστώσες. Οι ιδιότητες αυτές μπορούν να ανασυρθούν από τον πόρο που ζητείται για πρόσβαση, το περιβάλλον (π.χ. χρόνος ή τοποθεσία), τα υποκείμενα (subject) κλπ.



Σχήμα 2. Ροή Δεδομένων XACML

Το μοντέλο λειτουργεί ακολουθώντας τα παρακάτω βήματα:

1. Όπως φαίνεται στο Σχήμα 2, το PAP έχει αποθηκευμένα Policies και PolicySets, τα οποία είναι διαθέσιμα στο PDP. Αυτά τα Policies ή τα PolicySets αναπαριστούν ολόκληρη την πολιτική για ένα συγκεκριμένο στόχο (target).
2. Το PEP λαμβάνει τα αιτήματα πρόσβασης.
3. Το PEP προωθεί στον χειριστή πλαισίου (context handler) τα αιτήματα πρόσβασης σε φυσική μορφή (native format), η οποία προαιρετικά συμπεριλαμβάνει ιδιότητες των subjects, resource, action και environment.
4. Ο context handler κατασκευάζει ένα XACML request πλαίσιο, στο οποίο προαιρετικά προσθέτει attributes και το αποστέλλει στο PDP.
5. Το PDP αιτείται οποιαδήποτε πρόσθετη πληροφορία σχετική με τα ιδιότητες των subjects, resources, action κλπ. από τον χειριστή πλαισίου.
6. Ο context handler ζητά ακολούθως τα attributes από το PIP.
7. Το PIP αποκτά τα ζητούμενα attributes.
8. Το PIP επιστρέφει τις ζητούμενες ιδιότητες στον context handler.
9. Προαιρετικά ο context handler συμπεριλαμβάνει και το resource σε αυτό το πλαίσιο.

10. Ο context handler στέλνει τις ζητούμενες ιδιότητες (και ίσως το resource) στο PDP. Το PDP εκτιμά την πολιτική.
11. Το PDPεπιστρέφει το πλαίσιο της απάντησης (απόφαση έγκρισης πρόσβασης-authorization decision) στον context handler.
12. Ο context handler «μεταφράζει» αυτό το πλαίσιο απάντησης στην φυσική γλώσσα του PEP και σχεδόν ταυτόχρονα επιστρέφει την απάντηση στο PEP.
13. Το PEP εκπληρώνει τυχόν υποχρεώσεις (obligations).

Εάν το αποτέλεσμα είναι να επιτραπεί η πρόσβαση, τότε το PEP κάνει δεκτή την πρόσβαση στο συγκεκριμένο resource, σε αντίθετη περίπτωση αρνείται την πρόσβαση.

1.3.1 Μοντέλο ABAC και XACML

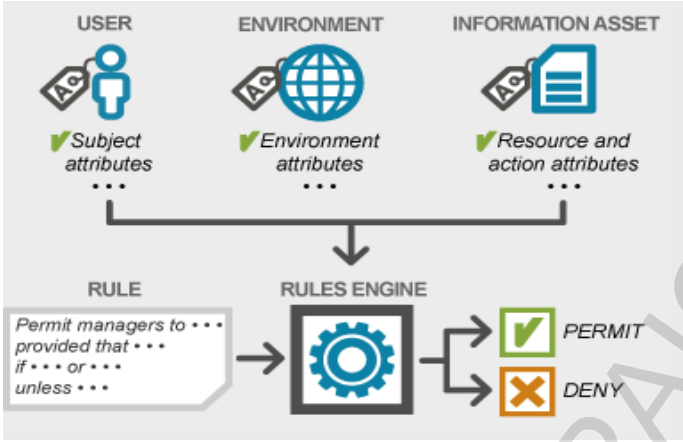
Ένα από τα βασικότερα χαρακτηριστικά γνωρίσματα της XACML, είναι το γεγονός ότι χρησιμοποιούνται ιδιότητες για να εκφράσουν πλούσιες και σύνθετες πολιτικές. Δηλαδή ακολουθείται το ABAC (Attribute-based Access Control), μοντέλο ελέγχου πρόσβασης βασισμένο σε ιδιότητες. Το ABAC χρησιμοποιεί ιδιότητες σαν δομικές μονάδες μέσα σε μία δομημένη γλώσσα που ορίζει κανόνες ελέγχου πρόσβασης και περιγράφει αιτήματα πρόσβασης. Τα attributes είναι σύνολα ετικετών ή ιδιοτήτων που μπορούν να χρησιμοποιηθούν για να περιγράψουν όλες τις οντότητες που πρέπει να εξεταστούν για λόγους έγκρισης. Κάθε ιδιότητα αποτελείται από ένα ζευγάρι μεταβλητής-τιμής όπως για παράδειγμα "Role=Manager".

1.4 Δομή της XACML

Η γλώσσα XACML είναι τόσο εκφραστική όσο και η φυσική γλώσσα. Για παράδειγμα, η έκφραση «ένας **χρήστης** θέλει να εφαρμόσει μια **πράξη** πάνω σε έναν **πόρο** πληροφορίας κάτω από ένα δεδομένο **πλαίσιο**», περιλαμβάνει τέσσερις γραμματικές δομικές μονάδες σύμφωνα με το Σχήμα 3, ένα υποκείμενο, μία πράξη, έναν πόρο και το περιβάλλον στο οποίο γίνεται η αίτηση αυτή.

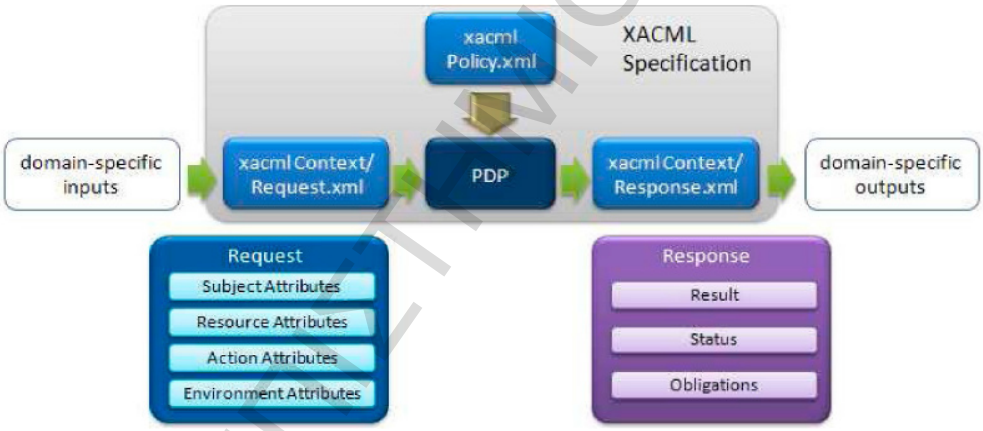
Κάθε ένα από τα παραπάνω μπορεί να περιγραφεί με χρήση ιδιοτήτων:

- Το υποκείμενο (subject) το οποίο ζητά πρόσβαση σε έναν πόρο πληροφορίας. Γενικές ιδιότητες που περιγράφουν το subject παραδείγματος χάριν ρόλοι, ιδιότητες μέλους ομάδας, τμήμα στο οποίο ανήκει ο χρήστης, πιστοποιήσεις και ικανότητες κλπ. μπορούν συχνά να ανακτηθούν από ένα σύστημα ανθρωπίνων πόρων ή από έναν κατάλογο (π.χ. LDAP).
- Η πράξη (action) που το υποκείμενο θέλει να πραγματοποιήσει. Κοινές ιδιότητες πράξεων σε αιτήσεις πρόσβασης είναι οι read και write.
- Ο πόρος (resource), που αναγνωρίζεται ως η πληροφορία ή το αντικείμενο στο οποίο έχει αντίκτυπο η πράξη.
- Το περιβάλλον (environment), το οποίο αναγνωρίζεται ως το πλαίσιο μέσα στο οποίο γίνεται η αίτηση πρόσβασης. Οι πιο συνήθεις ιδιότητες περιβάλλοντος σχετίζονται με την τρέχουσα ώρα και τοποθεσία όπου γίνεται η αίτηση πρόσβασης.



Σχήμα 3. Δομικές μονάδες της XACML

Η XACML στοχεύει στο να είναι κατάλληλη για ποικίλα περιβάλλοντα εφαρμογής. Το XACML πλαίσιο ορίζεται με XML Schema, περιγράφοντας μια κανονική αναπαράσταση για τις εισόδους και εξόδους του PDP.

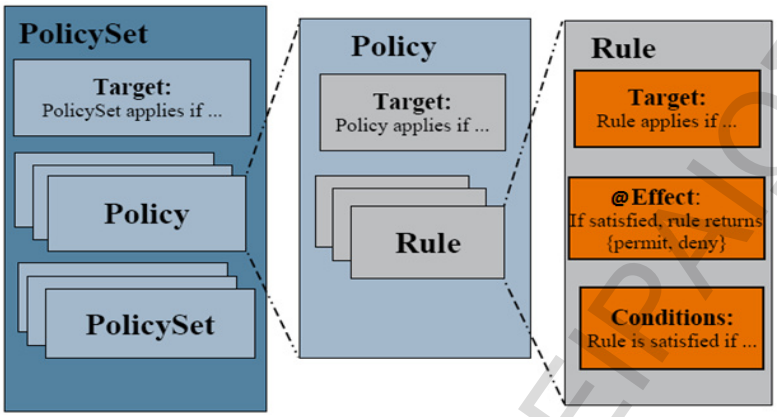


Σχήμα 4. Βασικό πλαίσιο της XACML

Ένα Request element, όπως φαίνεται στο Σχήμα 4, περιέχει τέσσερα συστατικά, τα Subject, Resource, Action, Environment. Ένα Request έχει μόνο μία συλλογή από resource και action ιδιότητες, και το πολύ μία συλλογή από environment ιδιότητες. Αλλά όσον αφορά τις Subject ιδιότητες, είναι δυνατόν να υπάρχουν πολλαπλές συλλογές.

Ένα Response element αναπαριστά την πληροφορία σχετικά με την απόφαση έγκρισης ή μη του Request, που γίνεται από το PDP. Αυτό περιλαμβάνει μία ή περισσότερες ιδιότητες αποτελέσματος (Result Attributes). Κάθε αποτέλεσμα περιέχει μια Απόφαση (Decision) όπως οι Permit, Deny, NotApplicable, Indeterminate. Επίσης, περιέχεται κάποια πληροφορία κατάστασης (Status information), η οποία δίνει τα λάθη που προκύπτουν κατά

την εκτίμηση του Request, καθώς και τυχόν μία ή περισσότερες υποχρεωτικές ενέργειες (Obligations), που προσδιορίζουν κάποιες πράξεις που πρέπει να εκτελεστούν πριν την χορήγηση ή την άρνηση πρόσβασης.



Σχήμα 5. Κύρια Συστατικά της XACML (PolicySet, Policy, Rule)

Το πρότυπο XACML, όπως φαίνεται στο Σχήμα 5, δομείται από τις παρακάτω κύριες μονάδες, οι οποίες αναλύονται λεπτομερώς σε επόμενες παραγράφους:

- Rule
- Policy
- PolicySet

Σε γενικές γραμμές, ένα Rule element καθορίζει τα target elements στα οποία εφαρμόζεται ο κανόνας και απαριθμεί τις συνθήκες για την εφαρμογή του κανόνα. Έχει τρία συστατικά στοιχεία, τα *target*, *effect* και *condition.*
Ένα target element προσδιορίζει τα στοιχεία subjects, resource, actions, environment στα οποία εφαρμόζεται ο κανόνας. Ένα condition element δείχνει υπό ποιες συνθήκες εφαρμόζεται ο κανόνας ενώ το effect attribute ορίζει τις συνέπειες του κανόνα, δηλαδή το αν το αποτέλεσμα είναι permit ή deny.
Ένα Policy είναι ένα σύνολο κανόνων οι οποίοι συνδυάζονται με κάποιους αλγορίθμους. Αυτοί οι αλγόριθμοι αποκαλούνται Rule-Combining-Algorithms.
Ένα PolicySet είναι ένα σύνολο από Policies και PolicySets που συνδυάζονται με Policy-Combining αλγορίθμους. Περιλαμβάνει επίσης target, όπως το Policy.

2. XACML και Πληροφοριακά Συστήματα Υγείας

2.1 Ηλεκτρονικό Αρχείο Υγείας - Εισαγωγή

Οι στρατηγικές ασφάλειας πληροφοριών αναπτύσσουν τρεις βασικές και αλληλένδετες έννοιες:

- Διαθεσιμότητα (Availability)
- Ακεραιότητα (Integrity)
- Εμπιστευτικότητα (Confidentiality)

Τα τελευταία χρόνια, ως αποτέλεσμα των τεχνολογικών επιτευγμάτων, έχουν αναδειχθεί νέες ιδέες σχετικά με την ιδιωτικότητα στην υγειονομική περίθαλψη, οι οποίες αλλάζουν τον τρόπο συσχετισμού των παραπάνω τριών εννοιών. Πριν την ψηφιοποίηση, τα αρχεία υγείας δεν ήταν άμεσα διαθέσιμα, και προκειμένου να είναι σε θέση να κατανοηθούν, απαιτούνταν διάφορα επίπεδα ιατρικής κατάρτισης.
Αντίθετα, σήμερα μέσα στα ηλεκτρονικά αρχεία υγείας ένα πλήθος σημαντικών πληροφοριών είναι δυνατόν να συνδυαστούν και μαζί με ένα πλούσιο σύνολο αναλυτικών επεξηγήσεων, βοηθούν τον χρήστη να τα κατανοήσει ευκολότερα.
Τα Ηλεκτρονικά Αρχεία Υγείας (Electronic Health record - EHR) είναι επομένως εύκολα διαθέσιμα σε νέα ακροατήρια, διευκολύνοντας την συνεργασία μεταξύ παρόχων υγειονομικής περίθαλψης και άλλων συμμετεχόντων σε αυτή την διαδικασία.
Αυτό έχει σαν αποτέλεσμα μεγάλα κέρδη σε αποδοτικότητα. Μια βασική παρενέργεια εντούτοις αποτελεί το γεγονός ότι οι ακεραιότητα και η εμπιστευτικότητα αναδεικνύονται σε κρίσιμα θέματα.
Οι ικανότητες των κυρίαρχων προτύπων για την επεξεργασία πληροφοριών ενός EHR και τα μοντέλα ελέγχου πρόσβασης που μπορούν να χρησιμοποιηθούν αναλύονται υπό το πρίσμα υψηλού επιπέδου απαιτήσεων. Η ιδανική προσέγγιση για αυτό αποτελεί ο Έλεγχος Πρόσβασης Βασισμένος σε Attributes (Attribute Based Access Control - ABAC), που υλοποιείται στα πλαίσια του XACML προτύπου.
Οι προσωπικές πληροφορίες του ασθενούς (Personal Health Information - PHI) διατηρούνται ολοένα και περισσότερο σε ηλεκτρονικά αρχεία. Αυτό σημαίνει ότι τα PHI δεδομένα μπορούν να παρασχεθούν, να αναπαραχθούν και να μεταφερθούν με μεγαλύτερη ευκολία από πριν.
Το επίπεδο ελέγχου πάνω στα EHRs που χορηγείται στο άτομο/ασθενή εναντίον των αντιπροσώπων των κέντρων περίθαλψης μπορεί να σταθμιστεί διαφορετικά ανάλογα με τις πολιτιστικές και δικαστικές παραδόσεις και αξίες. Εντούτοις, γενικά η νομοθεσία στις περισσότερες χώρες έχει προσπαθήσει να εξουσιοδοτήσει το άτομο σε μεγαλύτερη ή μικρότερη έκταση. Στον ασθενή χορηγούνται ρητά δικαιώματα, που ήταν προηγουμένως είτε κακώς καθορισμένα ή μη εφαρμόσιμα, σε σχέση με τα αρχεία υγείας που διατηρούνται από τους παρόχους περίθαλψης.
Επιπροσθέτως, οι νομοθέτες προσπαθούν να ελέγξουν κάτω από ποιες περιστάσεις οι πάροχοι περίθαλψης θα έπρεπε να έχουν την άδεια διαμοιρασμού στοιχείων ασθενών με τρίτα πρόσωπα που μπορούν να είναι λιγότερο ή περισσότερο εμπλεκόμενα στην διαδικασία περίθαλψης που παρέχεται.

2.2 Το περιβάλλον Ανάπτυξης - WSO2 Identity Server

Ο WSO2 Identity Server είναι ένας πλήρως ανοικτού κώδικα, βασισμένος σε components server οποίος εκτελεί τις λειτουργίες ελέγχου πρόσβασης και αναγνώρισης ταυτότητας.
Διευκολύνει τη διαχείριση ασφάλειας και αναγνώρισης ταυτότητας των διαφόρων web εφαρμογών των επιχειρήσεων και υπηρεσιών, υποστηρίζοντας ταυτόχρονα και τα OpenID, Information Cards, XACML και SAML 2.0 πρότυπα.
Βασισμένος στην βραβευμένη πλατφόρμα WSO2 Carbon, ο WSO2 Identity Server αποτελείται μόνο από τα απαιτούμενα εκείνα συστατικά απαραίτητα για την αποδοτική του λειτουργία.

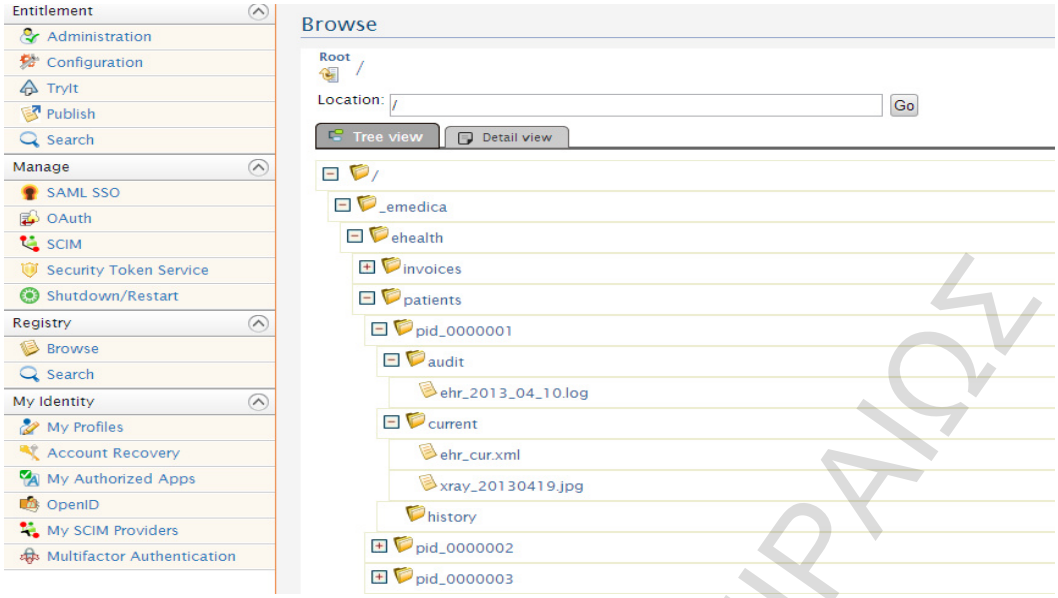
Στα βασικότερα πλεονεκτήματα του WSO2 Identity Server συγκαταλέγονται τα εξής:

- Συμβάλει στην βελτίωση της «εμπειρίας του πελάτη», μειώνοντας την διάρκεια του χρόνου παροχής ταυτότητας (identity provisioning time).
- Εγγυάται ασφαλείς online αλληλεπιδράσεις.
- Επιδρά στην παράδοση ενός «reduced» single sign-on περιβάλλοντος (delivering a reduced single sign-on environment).
- Μειώνει τον φόρτο για διαχείριση ταυτοτήτων και εξουσιοδοτήσεων, με την χρήση ελέγχου πρόσβασης βασισμένου σε ρόλους (RBAC-Role-based access control) και fine-grained ελέγχου πρόσβασης βασισμένου σε πολιτικές (policy-based access control)

2.3 Πληροφοριακό Σύστημα Υγείας EMEDICA - Δομή

Το Πληροφοριακό Σύστημα για το οποίο υλοποιήθηκε η Πρότυπη Πολιτική Ελέγχου Πρόσβασης, ακολουθεί το XACML πρότυπο, έχοντας ως βασικές δομικές μονάδες τα Subjects, Resources, Actions, Environment.
Τα Resources, τα οποία καθορίζονται ως τα στοιχεία που πρέπει να προστατευθούν, όπως φαίνεται και στην εικόνα 1, αποθηκεύονται στον WSO2 Identity Server σε δενδρική δομή, έχοντας ως root στοιχείο το _emedica, το οποίο είναι και το όνομα του πληροφοριακού συστήματος. Κάτω από το _emedica αναπτύσσονται εμφωλευμένα όλα τα resources στα αντίστοιχα μονοπάτια:

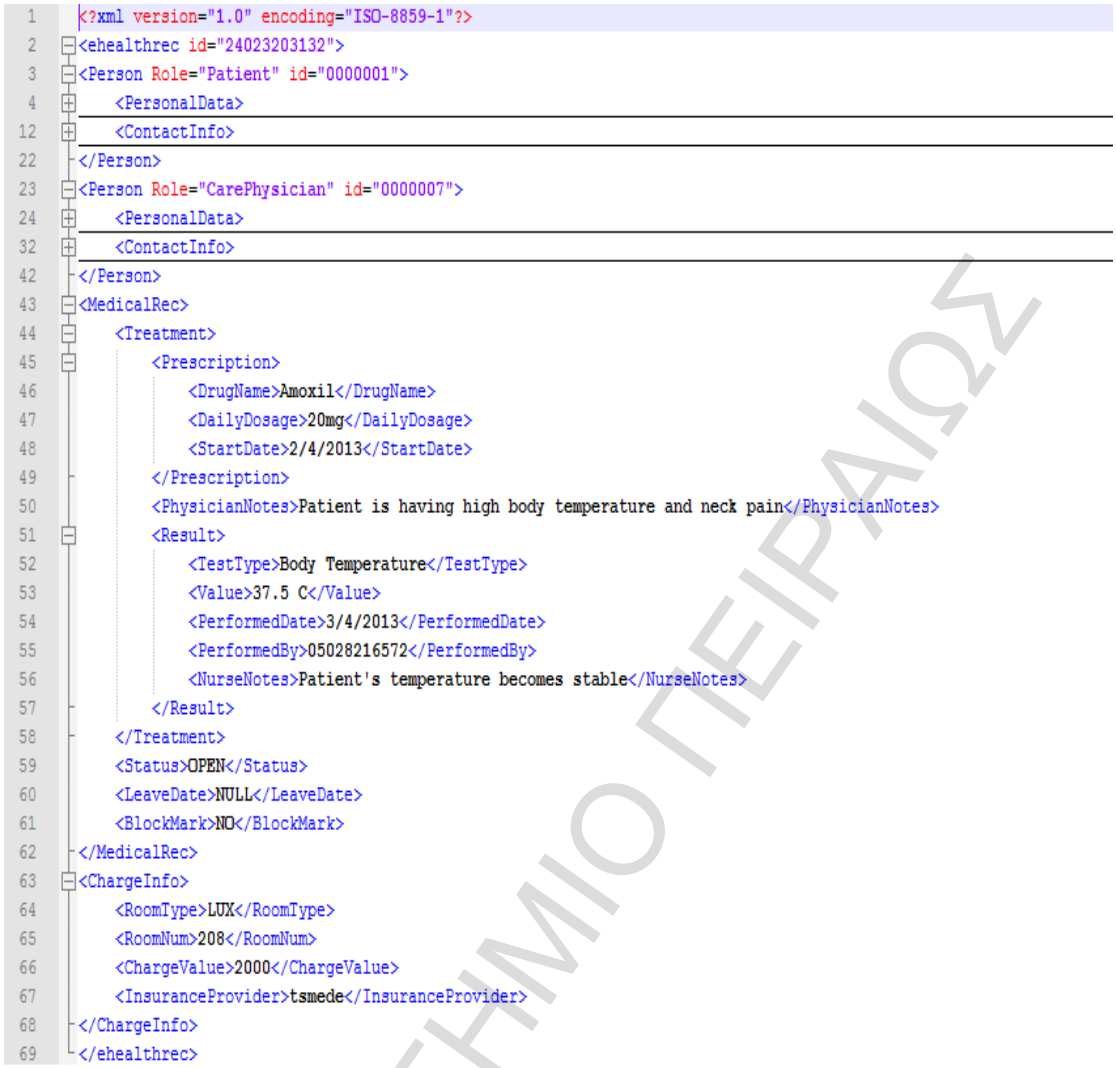
- /_emedica/ehealth/invoices/2013/ όπου υπάρχουν όλες οι αποδείξεις για όλους τους ασθενείς για το τρέχον έτος. Οι αποδείξεις έχουν την μορφή Invoice_1.txt.
- /_emedica/ehealth/patients/pid_0000001/audit όπου υπάρχουν όλα τα log files που αντιστοιχούν σε κάθε ενέργεια-κίνηση στο αρχείο του ασθενούς με το pid_0000001. Τα log files είναι της μορφής ehr_2013_4_10.log



Εικόνα 1. Δενδρική Δομή Πόρων Συστήματος

- /_emedica/ehealth/patients/pid_0000001/current/, όπου βρίσκονται τα ηλεκτρονικά αρχεία υγείας (EHR) και οι ακτινογραφίες του ασθενή με pid_0000001 και έχουν την μορφή ehr_cur.xml και xray_20130419.jpg αντίστοιχα.

Το βασικότερο resource (το EHR) είναι ένα έγγραφο xml και απεικονίζεται στην παρακάτω εικόνα (Εικόνα 2).



```xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<ehealthrec id="24023203132">
<Person Role="Patient" id="0000001">
    <PersonalData>
    <ContactInfo>
</Person>
<Person Role="CarePhysician" id="0000007">
    <PersonalData>
    <ContactInfo>
</Person>
<MedicalRec>
    <Treatment>
        <Prescription>
            <DrugName>Amoxil</DrugName>
            <DailyDosage>20mg</DailyDosage>
            <StartDate>2/4/2013</StartDate>
        </Prescription>
        <PhysicianNotes>Patient is having high body temperature and neck pain</PhysicianNotes>
        <Result>
            <TestType>Body Temperature</TestType>
            <Value>37.5 C</Value>
            <PerformedDate>3/4/2013</PerformedDate>
            <PerformedBy>05028216572</PerformedBy>
            <NurseNotes>Patient's temperature becomes stable</NurseNotes>
        </Result>
    </Treatment>
    <Status>OPEN</Status>
    <LeaveDate>NULL</LeaveDate>
    <BlockMark>NO</BlockMark>
</MedicalRec>
<ChargeInfo>
    <RoomType>LUX</RoomType>
    <RoomNum>208</RoomNum>
    <ChargeValue>2000</ChargeValue>
    <InsuranceProvider>tsmede</InsuranceProvider>
</ChargeInfo>
</ehealthrec>
```

Εικόνα 2. Ηλεκτρονικό Αρχείο Υγείας (EHR)

Το Electronic Health record που είναι το root element <ehealthrec>, αποτελείται από τα elements <Person> με Role="Patient", <Person> με Role="CarePhysician", <MedicalRec> και <ChargeInfo>. Τα δύο πρώτα στοιχεία περιέχουν πληροφορίες σχετικά με τον ασθενή και τον γιατρό που τον παρακολουθεί (όνομα, τηλέφωνο, διεύθυνση, αρ. ασφάλισης κλπ.). Στο στοιχείο <MedicalRec> περιλαμβάνονται ιατρικά δεδομένα για την εξέλιξη της θεραπείας και της νοσηλείας του ασθενούς (στοιχεία φαρμάκων, συμπτώματα, κλπ.), ενώ στο στοιχείο <ChargeInfo> περιέχονται δεδομένα σχετικά με χρεώσεις (τιμή δωματίου, ασφαλιστικός φορέας κλπ.).
Στο Εικόνα 3 απεικονίζεται με μεγαλύτερη λεπτομέρεια το μέρος του EHR που σχετίζεται με τα πλήρη στοιχεία του ασθενούς.

ehr_cur#1.xml

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<ehealthrec id="24023203132">
<Person Role="Patient" id="0000001">
    <PersonalData>
        <Name>George</Name>
        <Surname>Smith</Surname>
        <Fathers>Peter</Fathers>
        <DateOfBirth>1932-02-24</DateOfBirth>
        <SSN_ID>24023203132</SSN_ID>
        <VAT_NUM>125627382</VAT_NUM>
    </PersonalData>
    <ContactInfo>
        <Street>ermou 2</Street>
        <City>athens</City>
        <Country>greece</Country>
        <PostalCode>11242</PostalCode>
        <Phone>2106721224</Phone>
        <Mobile>6976780972</Mobile>
        <Fax>NULL</Fax>
        <Email>g.smith@gmail.com</Email>
    </ContactInfo>
</Person>
<Person Role="CarePhysician" id="0000007">
<MedicalRec>
<ChargeInfo>
</ehealthrec>
```

Εικόνα 3. Στοιχεία του Ασθενή στο EHR

2.3.1 Υποκείμενα Πληροφοριακού Συστήματος Υγείας EMEDICA (Subjects)

Στο πληροφοριακό Σύστημα Υγείας που υλοποιήθηκε (EMEDICA) έχουν καταχωρηθεί συνολικά δεκαπέντε χρήστες (Subjects) οι οποίοι φαίνονται στην παρακάτω εικόνα (Εικόνα 4).

Users

Search

Enter user name pattern (* for all) or User claim value * Search

Select Claim Uri Select

<< first <prev 1 2 next > last >>

Name	Actions
a.bendon	Change Password Roles Delete User Profile
a.moon	Change Password Roles Delete User Profile
admin	Change Password Roles User Profile
g.smith	Change Password Roles Delete User Profile
ika	Change Password Roles Delete User Profile
m.resting	Change Password Roles Delete User Profile
m.white	Change Password Roles Delete User Profile
n.karter	Change Password Roles Delete User Profile
p.frank	Change Password Roles Delete User Profile
r.resting	Change Password Roles Delete User Profile
s.jacson	Change Password Roles Delete User Profile
s.molder	Change Password Roles Delete User Profile
tsmede	Change Password Roles Delete User Profile
v.sting	Change Password Roles Delete User Profile
w.molder	Change Password Roles Delete User Profile

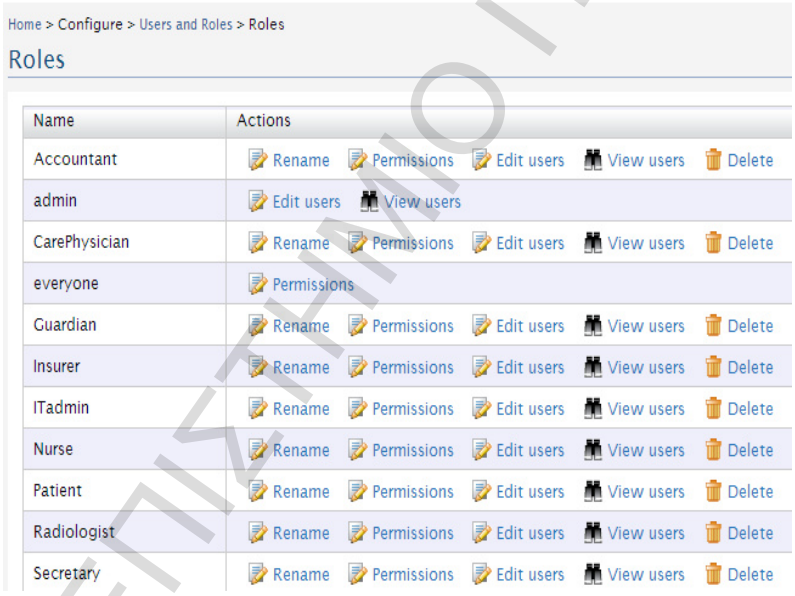
Εικόνα 4. Τα Subjects του Συστήματος

Κάθε Subject έχει έναν συγκεκριμένο ρόλο (Role) και ένα καθορισμένο προφίλ στο οποίο είναι καταχωρημένα όλα τα χαρακτηριστικά τους.

Όσον αφορά τους ρόλους, στο σύστημα υπάρχουν εννέα διαφορετικοί ρόλοι πάνω στους οποίους βασίζονται όλες οι πολιτικές ασφάλειας του πρότυπου πληροφοριακού συστήματος υγείας EMEDICA:

- Accountants (Λογιστές)
- CarePhysicians (Γιατροί)
- Guardians (Κηδεμόνες)
- Patients (Ασθενείς)
- ITadmins (Διαχειριστές Πληροφορικού Συστήματος)
- Insurers (ασφαλιστικοί Φορείς)
- Secretaries (Γραμματείς)
- Nurses (Νοσοκόμες)
- Radiologists (Ραδιολόγοι)

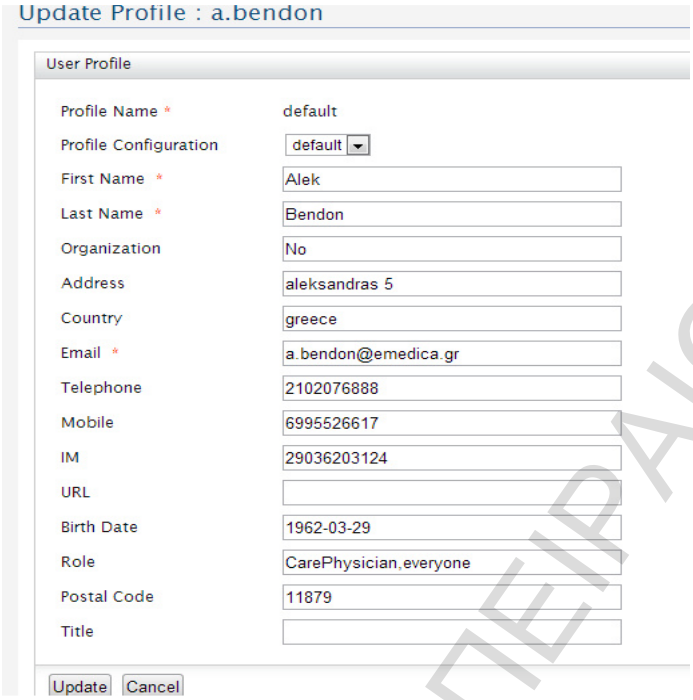
Σε αυτούς τους ρόλους, όπως φαίνεται και στην εικόνα 5, υπάρχουν και δύο ακόμα ρόλοι, οι ADMIN και EVERYONE. Αυτοί οι ρόλοι υπάρχουν by default στο σύστημα, ανεξαρτήτως αν το σύστημα που κατασκευάστηκε σχετίζεται με την υγεία ή με κάποιον άλλο τομέα δραστηριότητας και συνεπώς δεν έχουν σχέση με το πρότυπο σύστημα που υλοποιήθηκε στην παρούσα εργασία.



Εικόνα 5. Ρόλοι Χρηστών Συστήματος

Στην Εικόνα 6 απεικονίζεται με μεγαλύτερη λεπτομέρεια το πλήρες προφίλ που έχει αποθηκευτεί στον WSO2 Server για ένα subject, συγκεκριμένα για τον Alek Bendon. Στο προφίλ εμφανίζονται διάφορες πληροφορίες για το άτομο όπως ονοματεπώνυμο, διεύθυνση, τηλέφωνο, ημερομηνία γέννησης κλπ. Τα σημαντικότερα στοιχεία όμως που παίζουν ιδιαίτερο ρόλο στις πολιτικές που υλοποιήθηκαν είναι τα ακόλουθα:

- Role
- IM (το οποίο επιλέχθηκε να παριστάνει τον Αρ. Κοινωνικής Ασφάλισης – Social Security Number SSN)
- Email



Εικόνα 6. Πλήρες Προφίλ Υποκειμένου

3. Πρότυπη Πολιτική Ασφάλειας Πληροφοριακού Συστήματος Υγείας EMEDICA

3.1 Γενική Περιγραφή Πολιτικών Ασφάλειας (Ανάλυση PolicySet)

Το **<PolicySet>** xacml element είναι αυτό που αναπαριστά την πολιτική ασφαλείας που εφαρμόζεται συνολικά στο υπο-μελέτη πληροφοριακό σύστημα υγείας, ενώ το αναγνωριστικό του καθορίζεται με βάση το XACML attribute **@PolicySetId**, όπου στην περίπτωση μας έχει την τιμή «**EMEDICA_POLICYSET**». Σημαντικά elements που περιέχονται στο **<PolicySet>** element είναι το **<Target>** και τα **<PolicyIdReference>**.

Το **<Target>** element καθορίζει την εφαρμοσιμότητα της συνολικής πολιτικής ασφάλειας στο δυνατό σύνολο των αιτημάτων για πρόσβαση στους πόρους του συστήματος. Στην περίπτωσή μας, εξετάζεται η ιδιότητα «**role**» του **access-subject** που ζητεί κάποιον πόρο του συστήματος και αν αυτό έχει τουλάχιστον μια από τις αναγνωρίσιμες τιμές:

- Patient ή
- Guardian ή
- CarePhysician ή
- Nurse ή
- Secretary ή
- ITadmin ή
- Accountant ή
- Radiologist ή
- Insurer,

τότε πληρείται η έκφραση Target-Match, συνεπώς εξετάζονται οι επιμέρους πολιτικές που εσωκλείονται μέσα στην συνολική πολιτική ασφαλείας καθώς και το πολύ σημαντικό xacml attribute **@PolicyCombiningAlgId**, το οποίο καθορίζει τον τρόπο με τον οποίο συνδυάζονται οι αποφάσεις των επιμέρους πολιτικών, στην αρμοδιότητα των οποίων υπάγεται το αίτημα πρόσβασης (request).
Ο υπολογισμός της έκφρασης του **<Target>** element μπορεί να καταλήξει σε μία εκ των τριών τιμών:

- Target-**Match**
- Target-**No Match**
- Target-**Indeterminate**

Η τελική τιμή που παίρνει αποτελεί μια σύνθεση με **Λογικό AND** όλων των τιμών των εκφράσεων που προκύπτουν από τα περιεχόμενα **<AnyOf>** elements. Ο υπολογισμός της έκφρασης ενός **<AnyOf>** element μπορεί επίσης να καταλήξει σε μια εκ των τριών τιμών:

- AnyOf-**Match**
- AnyOf-**No Match**
- AnyOf-**Indeterminate**

Η τελική τιμή που παίρνει αποτελεί μια σύνθεση με **Λογικό OR** όλων των τιμών των εκφράσεων που προκύπτουν από τα περιεχόμενα **<AllOf>** elements.
Ο υπολογισμός της έκφρασης ενός **<AllOf>** element μπορεί επίσης να καταλήξει σε μια εκ των τριών τιμών που προαναφέρθηκαν:

- AllOf-**Match**
- AllOf-**No Match**
- AllOf-**Indeterminate**

Η τελική τιμή που παίρνει αποτελεί μια σύνθεση με **Λογικό AND** όλων των τιμών που προκύπτουν από τον υπολογισμό των εκφράσεων των περιεχόμενων **<Match>** elements.
Ο υπολογισμός του **<Match>** element μπορεί να καταλήξει είτε σε μια εκ των Boolean τιμών «**True**» ή«**False**», είτε στην τιμή «**Indeterminate**». Η τιμή «**Indeterminate**» παριστάνει την δημιουργία κάποιου λειτουργικού λάθους κατά τη φάση υπολογισμού των xacml εκφράσεων.
Σε περίπτωση που όλα τα **<Match>** elements παίρνουν τιμές «**True**», πλην ενός ή περισσοτέρων που έχουν τιμή «**Indeterminate**», τότε το εξωτερικό **<AllOf>** element παίρνει την τιμή «**Indeterminate**», και αυτή δύναται να μεταφερθεί στους υπολογισμούς των εξωτερικών εκφράσεων.
Στην περίπτωσή μας και έχοντας εξασφαλίσει ότι οι πολιτικές δεν δημιουργούν λάθη εκφράσεων (και συνεπώς παραγωγή τιμών Indeterminate), το **<Target>** element της συνολικής πολιτικής ασφαλείας αποτελείται από ένα **<AnyOf>** element, το οποίο με τη σειρά του εσωκλείει εννέα **<AllOf>** elements. Κάθε **<AllOf>** element αποτελείται από ένα **<Match>** element, συνεπώς το **<Target>** element υπολογίζεται στην τιμή «**Match**», εάν οποιοδήποτε από τα περιεχόμενα **<AllOf>** elements παίρνει την τιμή «**Match**», ή ισοδύναμα οποιοδήποτε **<Match>** element παίρνει την τιμή «**True**».

Καθένα από τα **<Match>** elements αποτελείται από τρία βασικά συστατικά:

- Το attribute **@MatchId**, το οποίο παριστάνει τη συνάρτηση σύγκρισης που θα επενεργήσει στα επόμενα δύο ορίσματα. Στην περίπτωση που εξετάζουμε χρησιμοποιείται η συνάρτηση «**string-equal**», δηλ. συνάρτηση ισότητας μεταξύ δύο συμβολοσειρών χαρακτήρων (string).
- Το element **<AttributeValue>**, το οποίο είναι μια σταθερά τύπου string και παίρνει την τιμή ενός απ' τους ρόλους των χρηστών που είναι δυνατό να αιτηθούν πρόσβαση στους πόρους του συστήματος πχ. **Patient**.
- Το element **<AttributeDesignator>**, το οποίο επιλέγει μια σακούλα (bag) τιμών για συγκεκριμένη ιδιότητα, προερχόμενη άμεσα ή έμμεσα από το αίτημα πρόσβασης. Στην περίπτωσή μας ζητείται η ιδιότητα «**role**» του χρήστη που ζητά πρόσβαση, δηλαδή του **access-subject**, και αυτό παρέχεται αυτόματα στο module που παράγει τις αποφάσεις (PDP) από το Profile που έχουμε καθορίσει για τους χρήστες του

συστήματος, λαμβάνοντας υπόψιν την ιδιότητα «subject-id», η οποία αποτελεί αναγνωριστικό του χρήστη στο αίτημα πρόσβασης.

Τα xacml elements **<Policy>** περιέχουν τις επιμέρους πολιτικές, που απαρτίζουν την συνολική πολιτική ασφάλειας του συστήματος και παίρνουν τιμές αντίστοιχες με το όνομα κάθε πολιτικής (π.χ. το xacml attribute **@PolicyId = "Policy_Patients"**). Η κάθε πολιτική, όπως δείχνει και το όνομά της, είναι αρμόδια για την παραγωγή αποφάσεων σε αιτήματα πρόσβασης που αφορούν συγκεκριμένους ρόλους χρηστών του συστήματος, συνεπώς για κάποιον χρήστη που έχει τον πρωτεύον ρόλο «**CarePhysician**», η αντίστοιχη πολιτική που είναι αρμόδια να απαντήσει στο αίτημά του θα είναι η «Policy_Physicians», χωρίς να αποκλείεται ότι και κάποια άλλη πολιτική μπορεί να δώσει κάποια απόφαση εάν ο χρήστης κατέχει και δεύτερο υπαρκτό ρόλο.
Σημειώνεται ότι οι επιμέρους πολιτικές συνδυάζονται με τον αλγόριθμο συνδυασμού πολιτικών «**permit-overides**», ο οποίος χρησιμοποιείται για να δοθεί προτεραιότητα στην πολιτική της οποίας η απόφαση καταλήγει σε τιμή «**Permit**». Ο κύριος λόγος για τον οποίο χρησιμοποιούμε τον αλγόριθμο αυτό, είναι για τις περιπτώσεις όπου κάποιος χρήστης μπορεί να έχει ταυτόχρονα 2 ρόλους, δηλ. είναι **CarePhysician** και ταυτόχρονα **Guardian** (πχ. για κάποιο μέλος της οικογένειάς του). Σε αυτήν την περίπτωση δύο από τις πολιτικές θα καταλήξουν σε αποφάσεις, η μια μπορεί να έχει τιμή «Permit» από την πλευρά του **Guardian** και η άλλη τιμή «**Deny**» από την πλευρά του **CarePhysician**, εάν δεν είναι ο θεράπων ιατρός για τον συγκεκριμένο ασθενή. Σε αυτές τις περιπτώσεις ορθά προτιμούμε την συνολική απόφαση της πολιτικής ασφαλείας του συστήματος να είναι «**Permit**».
Επισημαίνεται ότι εάν δεν έχουμε Target-**Match** για την συνολική πολιτική ασφαλείας (δηλ. δεν αναγνωρίζεται ο χρήστης ή το σύνολο των ρόλων που μπορεί να κατέχει), τότε η συνολική πολιτική ασφαλείας αποκρίνεται με την απόφαση «**Not Applicable**», ανεξαρτήτως του αλγορίθμου συνδυασμού πολιτικών.

3.2 Περιγραφή Επιμέρους Πολιτικής - Policy_Physicians

Η πρώτη πολιτική που θα αναλυθεί είναι η Πολιτική Ασφάλειας για τους γιατρούς (Policy_Physicians). Η πολιτική αποτελείται από τρείς διακριτούς κανόνες:

- Rule_1: Ο Γιατρός μπορεί να διαβάσει το στοιχείο <MedicalRec> από το EHR ενός ασθενούς, δεδομένου ότι είναι ο θεράπων ιατρός του.
- Rule_2: Ο Γιατρός μπορεί να γράψει στο στοιχείο <MedicalRec> από το EHR ενός ασθενούς δεδομένου ότι είναι ο θεράπων ιατρός του και σαν αποτέλεσμα αποστέλλεται e-mail ειδοποίηση στον ασθενή για αυτή την πράξη.
- Rule_3: Ο Ραδιολόγος μπορεί να διαβάσει οποιαδήποτε ακτινογραφία στα αρχεία των ασθενών, δεδομένου ότι το e-mail του ανήκει στο e-medica domain.

3.2.1 Ανάλυση Επιμέρους Πολιτικής - Policy_Physicians

Το **<Policy>** element που έχει για αναγνωριστικό το xacml attribute **@PolicyId** ίσο με «**Policy_Physicians**», αναπαριστά την επιμέρους πολιτική που καθορίζει τις προσβάσεις που μπορούν να έχουν οι χρήστες, των οποίων ο ρόλος είναι γιατροί γενικά (**CarePhysician** ή και **Radiologist**).

Σημαντικά elements που περιέχονται στο προαναφερόμενο **<Policy>** element είναι το **<Target>** element και τα **<Rule>** elements. Το **<Target>** element καθορίζει την εφαρμοσιμότητα της επιμέρους πολιτικής ασφάλειας στο πεδίο των αιτημάτων πρόσβασης για χρήστες, των οποίων η ιδιότητα **«role»** είναι είτε «**CarePhysician**», είτε «**Radiologist**».

Τα δύο πρώτα **<Rule>** elements έχουν φτιαχτεί γενικά για χρήστες των οποίων ο ρόλος είναι γιατρός, ενώ το τρίτο για χρήστες τον οποίων ο ρόλος μπορεί να πάρει και την τιμή «**Radiologist**». Βασικό στοιχείο της πολιτικής αποτελεί και το xacml attribute **@RuleCombiningAlgId** του οποίου η τιμή είναι «**deny-unless-permit**». Αυτό το στοιχείο καθορίζει τον τρόπο με τον οποίο οι αποφάσεις που προκύπτουν από τον υπολογισμό των περιεχόμενων κανόνων θα συνδυαστούν για να δοθεί η συνολική απόφαση της πολιτικής.

Ο συγκεκριμένος αλγόριθμος που χρησιμοποιήθηκε στην πολιτική αυτή έχει το πλεονέκτημα ότι δίνει προτεραιότητα στις αποφάσεις κανόνων που υπολογίζουν σε τιμή «**Permit** έναντι αυτών των οποίων οι αποφάσεις είναι «**Deny**». Επιπροσθέτως, δεν αφήνει να επιστραφεί ως αποτέλεσμα απόφασης της πολιτικής κάποια από τις τιμές «**Not Applicable**» ή «**Indeterminate**». Συνεπώς, η πολιτική για χρήστες των οποίων ο ρόλος είναι γιατροί θα καταλήγει πάντα είτε σε απόφαση **Permit**, είτε σε **Deny**.
Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule_PHY1**», αναπαριστά τον πρώτο κανόνα της πολιτικής για τους γιατρούς. Σημαντικά στοιχεία του **<Rule>** element αποτελούν τα **<Target>** και **<Condition>** elements, καθώς και το attribute **@Effect**.
Στον συγκεκριμένο κανόνα εκτός από τα elements **<Target>**, **<AnyOf>**, **<AllOf>** υπάρχει και ένα **<Match>** element το οποίο γίνεται **True** όταν το χαρακτηριστικό «**action-id**» της κατηγορίας **action,** στο αίτημα πρόσβασης, είναι ίσο με την τιμή **read**. Συνεπώς ο κανόνας αυτός βρίσκει εφαρμογή όταν κάποιος χρήστης του συστήματος (access-subject) , του οποίου ο ρόλος είναι γιατρός γενικά, προσπαθεί να εκτελέσει την ενέργεια (action) read σε κάποιον πόρο (resource) του συστήματος.
Το xacml attribute **@Effect**, που στην περίπτωσή μας έχει την τιμή «**Permit**», παριστάνει την επίδραση του κανόνα στην απόφαση της πολιτικής, όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**». Το **<Condition>** element αποτελεί ένα δευτέρου επιπέδου φίλτρο πάνω στα αιτήματα πρόσβασης, για τα οποία ο συγκεκριμένος κανόνας μπορεί να εφαρμοστεί. Στο element αυτό έχουμε την δυνατότητα να κατασκευάσουμε πολυπλοκότερες εκφράσεις από ότι στο **<Target>** element και να χρησιμοποιήσουμε συναρτήσεις με πολλά επίπεδα ένθεσης, ενώ συναντάται πάντα εσωτερικά κάποιου **<Rule>** element.

Εσωτερικά του **<Condition>** εφαρμόζεται ένα **<Apply>** element, το οποίο υποδηλώνει το κάλεσμα μιας συνάρτησης με αναγνωριστικό το xacml attribute **@FunctionId**. Στην περίπτωσή μας χρησιμοποιήσαμε την Λογική συνάρτηση **AND**, ώστε η συνολική έκφραση στο **<Condition>** να γίνεται **True**, όταν όλες οι επιμέρους εκφράσεις υπολογίζονται σε «**True**». Με αυτόν τον τρόπο συμπεριλαμβάνουμε συνολικά 3 υπο-εκφράσεις (συνθήκες), οι οποίες θα πρέπει και οι τρεις να δίνουν τιμή «**True**», για να γίνεται το **<Condition>** element αληθές:

- **1η συνθήκη**

Το στοιχείο ταυτοποίησης SSN_ID (Social Security Number) του χρήστη, που αιτείται τον πόρο του συστήματος (που είναι το ηλεκτρονικό αρχείο υγείας - EHR), θα πρέπει να είναι ίδιο με αυτό που αναγράφεται στα στοιχεία του θεράποντος ιατρού εσωτερικά του EHR.

- **2η συνθήκη**

Ο πόρος του συστήματος που ζητείται να διαβαστεί από τον χρήστη θα πρέπει να έχει το όνομα ehr_cur.xml, ενώ το μονοπάτι εύρεσης του πόρου αυτού θα ταιριάζει με αυτό που έχει ήδη προκαθοριστεί για τους ασθενείς στο Πληροφοριακό Σύστημα Υγείας **E-MEDICA**, δηλ. θα ακολουθεί το μοτίβο /_emedica/ehealth/patients/pid_[επταψήφιος αριθμός]/current/.

- **3η συνθήκη**

Το συγκεκριμένο υπο-στοιχείο εσωτερικά του πόρου που ο χρήστης ζητεί να διαβάσει είναι το **<MedicalRec>** element, με βάση την θεώρηση ότι τα ηλεκτρονικά αρχεία υγείας των ασθενών (EHR) αναπαρίστανται στο σύστημα ως xml έγγραφα.

Ανάλυση 1ης Συνθήκης

Για την κατασκευή της πρώτης συνθήκης χρησιμοποιούμε το **<Apply>** element με αναγνωριστικό συνάρτησης το xacml attribute **@FunctionId** ίσο με «**all-of-any**». Η συνάρτηση αυτή ανήκει στις συναρτήσεις υψηλότερης τάξης που χειρίζονται σακούλες (higher order bag functions). Δέχεται τρία ορίσματα με πρώτο το **<Function>** element, το οποίο υποδηλώνει την συνάρτηση σύγκρισης που χρησιμοποιείται. Τα επόμενα δύο ορίσματα είναι σακούλες από τιμές, ενώ η συνολική έκφραση γίνεται αληθής εάν η συνάρτηση σύγκρισης είναι αληθής μεταξύ κάθε τιμής της πρώτης σακούλας με οποιαδήποτε τιμή από την δεύτερη σακούλα.

Η πρώτη σακούλα τιμών προκύπτει λόγω της χρήσης του **<AttributeDesignator>** element, το οποίο στην περίπτωσή μας ανευρίσκει έμμεσα την τιμή της ιδιότητας «**im**», που ανήκει στην κατηγορία χρηστών access-subject, και το οποίο δεν έχει συμπεριληφθεί στο αρχικό request προς το PDP. Αντί αυτού το σύστημα αναζητεί στο Profile των δηλωμένων χρηστών την συγκεκριμένη ιδιότητα, με βάση το αναγνωριστικό «**subject-id**» του χρήστη.

Η δεύτερη σακούλα τιμών προκύπτει από την χρήση του **<AttributeSelector>** element, το οποίο ανευρίσκει τις τιμές των xml κόμβων που επιλέγονται κατά την εφαρμογή της XPath

έκφρασης (δηλώνεται στο xacml attribute @Path) πάνω στο περιεχόμενο του EHR του ασθενούς. Σημειώνεται ότι για δομημένα resources τύπου xml, υπάρχει η δυνατότητα να συμπεριληφθεί το resource εσωτερικά του request που παραλαμβάνεται από το PDP, μέσα στο **<Content>** element της κατηγορίας ιδιοτήτων «**resource**».

Η XPath έκφραση:

«//xacml:**ehealthrec**/xacml:**Person**[**@Role**='**CarePhysician**']/xacml:**PersonalData**/
xacml:**SSN_ID**/**text()**»

, που χρησιμοποιήθηκε στην τρέχουσα συνθήκη λειτουργεί με τον εξής τρόπο: Αρχικά εντοπίζουμε εσωτερικά στο EHR αρχείο έναν κόμβο με element το **<ehealthrec>.** Κατόπιν επιλέγονται όλοι οι απόγονοι κόμβοι του αρχικού που διαθέτουν elements **<Person>,** των οποίων το xml attribute **@Role** είναι ίσο με «**CarePhysician**». Μετά επιλέγονται οι απόγονοι κόμβοι με element **<PersonalData>.** Τέλος, επιλέγονται οι text τιμές των elements **<SSN_ID>**, απόγονων κόμβων των προηγούμενων. Σημειώνεται ότι η τιμή του element **<SSN_ID>**, χρησιμοποιείται ως στοιχείο ταυτοποίησης του subject. Συνεπώς, οποιοσδήποτε γιατρός (access-subject) εμφανίζεται στο EHR του ασθενούς, έχοντας στα προσωπικά στοιχεία του θεράποντος ιατρού τον Αριθμό Κοινωνικής Ασφάλισής του (όμοιος με αυτόν που έχει δηλωθεί στο Profile του subject), έχει το δικαίωμα να διαβάσει τις ιατρικές πληροφορίες εσωτερικά του EHR του ασθενούς.

Ανάλυση 2ης Συνθήκης

Για την κατασκευή της δεύτερης συνθήκης χρησιμοποιούμε το **<Apply>** element με αναγνωριστικό συνάρτησης το xacml attribute **@FunctionId** ίσο με **«any-of»**. Η προαναφερόμενη συνάρτηση επίσης ανήκει στις συναρτήσεις που χειρίζονται σακούλες τιμών και είναι υψηλότερης τάξης. Δέχεται τρία ορίσματα, με πρώτο το **<Function>** element, το οποίο υποδηλώνει την συνάρτηση σύγκρισης που χρησιμοποιείται, για την περίπτωση που εξετάζουμε αυτή είναι η **«string-regexp-match»**. Το επόμενο όρισμα είναι η τιμή του μοτίβου μιας συμβολοσειράς χαρακτήρων (string), η οποία παριστάνει το πλήρες μονοπάτι και το όνομα του πόρου, που αντιστοιχεί στα EHRs των ασθενών. Το τρίτο όρισμα είναι μια σακούλα τιμών, ενώ η συνολική έκφραση καταλήγει σε τιμή «**True**», εάν η συνάρτηση σύγκρισης είναι αληθής μεταξύ του 2ου ορίσματος και οποιασδήποτε τιμής που περιέχεται στην σακούλα του 3ου ορίσματος. Η σακούλα (bag) τιμών προκύπτει λόγω της χρήσης του **<AttributeDesignator>** element, το οποίο ανευρίσκει την ιδιότητα **«resource-id»**, για τον πόρο που έχει κατηγορία **«resource»**, συνεπώς αυτό είναι το πλήρες όνομα του πόρου στο request.

Ανάλυση 3ης Συνθήκης

Για την κατασκευή της 3ης συνθήκης χρησιμοποιούμε το **<Apply>** element με αναγνωριστικό συνάρτησης το xacml attribute **@FunctionId** ίσο με **«any-of»**. Όπως προηγουμένως, συγκρίνουμε την τιμή ενός string, το **«MedicalRec»**, με μια σακούλα τιμών που προκύπτουν για την καθορισμένη από τον χρήστη (user-defined) ιδιότητα **«resource-name»**, για τον πόρο κατηγορίας **«resource».** Η προαναφερόμενη ιδιότητα χρησιμοποιήθηκε για να

δείξουμε το όνομα του υπο-στοιχείου εσωτερικά του EHR (αρχείο τύπου xml), που το subject ζητεί να διαβάσει.
Κανονικά, επειδή το subject που ζητεί να διαβάσει κάποιο element του EHR του ασθενούς θα πρέπει σε θετική περίπτωση να είναι σε θέση να διαβάσει και μεμονωμένα οποιοδήποτε sub-element, θα έπρεπε η 3η συνθήκη να γραφτεί σύμφωνα με το OASIS πρότυπο XACML v3.0, κάνοντας χρήση της συνάρτησης **«xpath-node-match»** και ορίσματα τύπου **«xpathExpression»**. Παρακάτω, φαίνεται ο εναλλακτικός τρόπος γραφής της συνθήκης:

```
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
  <Function FunctionId="urn:oasis:names:tc:xacml:3.0:function:xpath-node-match"></Function>
  <AttributeValue DataType="urn:oasis:names:tc:xacml:3.0:data-type:xpathExpression"
                  XPathCategory="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">xacml:MedicalRec</AttributeValue>
  <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:3.0:content-selector" Category="urn:oasis:names:tc:xacml:3.0:
        attribute-category:resource" DataType="urn:oasis:names:tc:xacml:3.0:data-type:xpathExpression" MustBePresent="true"/>
</Apply>
```

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule_PHY2**», αναπαριστά τον δεύτερο κανόνα της πολιτικής για τους γιατρούς.

Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι γιατρός γενικά, προσπαθεί να εκτελέσει την ενέργεια **write** σε κάποιον πόρο του συστήματος ή ισοδύναμα στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας **action** συμπίπτει με την συμβολοσειρά χαρακτήρων **write**.
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».
Οι συνθήκες που έχουν συμπεριληφθεί στο **<Condition>** element είναι πανομοιότυπες με αυτές του προηγούμενου κανόνα για τους γιατρούς. Συνεπώς, ο κανόνας αυτός δεν διαφέρει και πολύ από τον προηγούμενο κανόνα ως προς την λειτουργικότητα των **<Target>** και **<Condition>** elements.
Παρατηρούμε όμως την εξής σημαντική διαφορά, στο τέλος του κανόνα έχει συμπεριληφθεί το element **<ObligationExpressions>**, το οποίο περιέχει εκφράσεις που θα πρέπει υποχρεωτικά να ληφθούν υπόψη εάν ο κανόνας καταλήξει στην απόφαση «**Permit**» (xacml attribute **@FulfillOn**). Το προαναφερόμενο element περιέχει εσωτερικά μια υποχρεωτική ενέργεια για το PEP, αυτή της αποστολής e-mail στον ασθενή, του οποίου το EHR έχει τροποποιηθεί (xacml attribute **@ObligationId = «EMAIL-TO-PATIENT»**). Για την διεκπεραίωση της υποχρεωτικής ενέργειας συμπεριλαμβάνονται τα παρακάτω ορίσματα.
Συνολικά έχουμε δύο ορίσματα τα οποία υπολογίζονται από τα xacml elements **<AttributeAssignmentExpression>**, με το πρώτο να είναι το e-mail του ασθενούς ενώ το δεύτερο είναι μια πρόταση που δείχνει το όνομα του γιατρού που έκανε τροποποίηση του EHR του ασθενούς.
Για την εύρεση του e-mail του ασθενούς χρησιμοποιήθηκε το element **<AttributeSelector>**, το οποίο εφαρμόζοντας κατάλληλη έκφραση XPath, εσωτερικά του EHR, ανευρίσκει το

ανωτέρω στοιχείο, και συγκεκριμένα στα στοιχεία επαφής του ατόμου, που δηλώνεται ως ασθενής. Παρακάτω δίνεται το xacml attribute @Path, το οποίο χρησιμοποιήθηκε για την επίτευξη της εύρεσης του στοιχείου e-mail:
//xacml:**ehealthrec**/xacml:**Person**[**@Role**='**Patient**']/xacml:**ContactInfo**/xacml:**Email**/text()

Για την κατασκευή του δεύτερου ορίσματος χρησιμοποιήθηκε η συνάρτηση «**string-concatenate**», η οποία συνενώνει δύο ή περισσότερες συμβολοσειρές χαρακτήρων. Το πρώτο string είναι μια σταθερά της μορφής: «**Your Medical Record has been updated by Care Physician:**», ενώ το δεύτερο string προέρχεται από την σακούλα τιμών που επιστρέφει το element **<AttributeDesignator>** και παριστάνει το όνομα του γιατρού (ιδιότητα **subject-id**), που αιτήθηκε της πρόσβασης (κατηγορίας access-subject) στο request. Σημειώνεται ότι, για την μετατροπή της σακούλας σε string χρησιμοποιήθηκε η συνάρτηση «**string-one-and-only**», η οποία λειτουργεί σωστά μόνο όταν η σακούλα διαθέτει μια και μοναδική τιμή.
Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-RAD1**», αναπαριστά τον τρίτο κανόνα της πολιτικής για τους γιατρούς.
Ο ανωτέρω κανόνας εφαρμόζεται ειδικά για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**» διαθέτει τον ρόλο του ραδιολόγου-ακτινολόγου και προσπαθεί να εκτελέσει την ενέργεια **read** σε συγκεκριμένους πόρους του συστήματος ή ισοδύναμα στο **<Target>** element η ιδιότητα «**action-id**» της κατηγορίας **action** συμπίπτει με την συμβολοσειρά χαρακτήρων **read** ΚΑΙ η ιδιότητα «**role**» της κατηγορίας «**access-subject**» ταιριάζει με την συμβολοσειρά χαρακτήρων **Radiologist.**
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».
Στο **<Condition>** element έχουν συμπεριληφθεί 2 υπο-εκφράσεις, οι οποίες θα πρέπει να δίνουν και οι δύο τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**».

- 1η συνθήκη

Ο πόρος του συστήματος που ζητείται να διαβαστεί από τον χρήστη (ακτινογραφία - xray) θα πρέπει να ακολουθεί το μοτίβο τόσο για το όνομα όσο και για το πλήρες μονοπάτι που έχει προκαθοριστεί για τους ασθενείς στο Πληροφοριακό Σύστημα **E-MEDICA**:

Μονοπάτι ⇔ /_emedica/ehealth/patients/pid_[επταψήφιος αριθμός]/current/

Όνομα πόρου ⇔ xray_[οχταψήφιος αριθμός].jpg

- 2η συνθήκη

Το e-mail του γιατρού-ραδιολόγου θα πρέπει να ανήκει στο **E-MEDICA** domain, δηλ να είναι της μορφής <user_name>@**emedica.gr.** Συνεπώς, στην συνθήκη συγκρίνεται η ιδιότητα «**emailaddress**» του χρήστη κατηγορίας «**access-subject**» με την συμβολοσειρά χαρακτήρων «**emedica.gr**». Η συνάρτηση που χρησιμοποιήθηκε είναι η «**rfc822Name-match**», η οποία δέχεται δύο ορίσματα, ένα με τύπο δεδομένων string και ένα τύπου

rfc822Name. Σημειώνεται ότι το δεύτερο όρισμα συμβολίζει μια ηλεκτρονική διεύθυνση ταχυδρομείου με το μέρος που ακολουθεί του χαρακτήρα «@», ή αλλιώς το domain μέρος, να παριστάνεται είτε με κεφαλαία είτε με μικρά γράμματα (NOT case-sensitive). Χρησιμοποιήθηκε επίσης η συνάρτηση μετατροπής «**rfc822Name-from-string**», διότι το δεύτερο όρισμα αρχικά ήταν τύπου string. Συνεπώς για κάθε ηλεκτρονική διεύθυνση γιατρού, που το domain μέρος της ταιριάζει με το string «emedica.gr», θα έχει ως αποτέλεσμα να υπολογίζεται η έκφραση σε τιμή True.

3.2.2 Αξιολόγηση και Επαλήθευση Πολιτικής - Policy_Physicians

Ο WSO2 Identity Server μας δίνει την δυνατότητα να δοκιμάσουμε την ορθή λειτουργία των πολιτικών. Μέσω της επιλογής **Try It**, εξομοιώνεται το κάθε αίτημα (Request) προς τον server. Στην ακόλουθη εικόνα (Εικόνα 7) απεικονίζεται το Request μαζί με το αντίστοιχο Response, που αντιστοιχούν στον πρώτο κανόνα της πολιτικής για τους χρήστες με ρόλο **Physician** (γιατρός).
Το σύστημα (δηλ. ο Server) δεν έχει την δυνατότητα στα Requests να ενσωματώνει και τον xml πόρο, που ο χρήστης μπορεί να ζητήσει. Ο πόρος όμως εσωτερικά διαθέτει μια πληθώρα από attributes που μπορούν να είναι σημαντικά στην απόφαση μιας πολιτικής. Σε κάποια Requests, οι αρμόδιες πολιτικές αποτελούνται από κανόνες, οι οποίοι δεν απαιτούν επιπρόσθετα attributes στην διαδικασία της απόφασης για το authorization.
Εντούτοις, στην πολιτική για τους γιατρούς οι δύο πρώτοι κανόνες απαιτούν την εμπλοκή συγκεκριμένων attributes από το resource για την διαδικασία λήψης απόφασης, οπότε σε αυτή την περίπτωση, γίνεται χειροκίνητη ενσωμάτωση του xml resource εσωτερικά του <**Content**> element του Request. Οπότε το συγκεκριμένο Request δεν αποδίδεται με παραθυρικό τρόπο (form).

Request_Physicians.xml

```
1  <Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
2  <!--Action Category-->
3  <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
4  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
5  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
6  </Attribute>
7  </Attributes>
8  <!--Subject Category-->
9  <Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
10 <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
11 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">n.karter</AttributeValue>
12 </Attribute>
13 </Attributes>
14 <!--Resource Category-->
15 <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
16 <Content>
17 <ehealthrec id="01060003133">
85 </Content>
86 <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
87 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
88                     /_emedica/ehealth/patients/pid_0000002/current/ehr_cur.xml</AttributeValue>
89 </Attribute>
90 <Attribute AttributeId="http:://wso2.org/my_attributes/resource-name" IncludeInResult="false">
91 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">MedicalRec</AttributeValue>
92 </Attribute>
93 </Attributes>
94 <!-- -->
95 </Request>
```

Εικόνα 7. Request_1 για Physician

Το Request απεικονίζει τον χρήστη με ρόλο «γιατρός» n.karter να αιτείται ανάγνωσης του element <MedicalRec> από το EHR του ασθενούς με pid_0000002 (s.molder). Εφόσον μέσα στο Content element αναφέρεται ότι θεράπων ιατρός του χρήστη με ρόλο «ασθενή» s.molder είναι ο χρήστης n.karter, το αποτέλεσμα της αίτησης είναι Permit.
Όσον αφορά τον δεύτερο κανόνα, αν ο ίδιος χρήστης με ρόλο «Physician» κάνει αίτηση εγγραφής (update) μέσα στο element **<MedicalRec>** του EHR του ίδιου ασθενή, τότε εφόσον πάλι ο χρήστης αποτελεί θεράπων ιατρό του ασθενούς, το αποτέλεσμα θα είναι Permit. Σε αυτήν την περίπτωση όμως ο κανόνας εξασφαλίζει ότι θα σταλεί στον χρήστη-ασθενή email με σκοπό την ενημέρωσή του για την πράξη του χρήστη-γιατρού του. Αυτό απεικονίζεται στις εικόνες 8 και 9.

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<!--Action Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
</Attribute>
</Attributes>
<!--Subject Category-->
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">n.karter</AttributeValue>
</Attribute>
</Attributes>
<!--Resource Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Content>
<ehealthrec id="01060003133">
</Content>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000002/current/ehr_cur.xml</AttributeValue>
</Attribute>
<Attribute AttributeId="http:://wso2.org/my_attributes/resource-name" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">MedicalRec</AttributeValue>
</Attribute>
</Attributes>
<!-- -->
</Request>
```

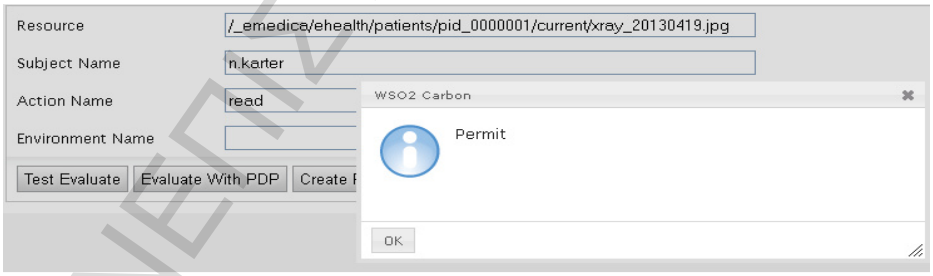
Εικόνα 8. Request_2 για Physician

```
<Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
<Result>
<Decision>Permit</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
<Obligations>
<Obligation ObligationId="EMAIL-TO-PATIENT">
<AttributeAssignment  AttributeId="obligation-attribute:mailto"
DataType="http://www.w3.org/2001/XMLSchema#string">s.molder@hotmail.com</AttributeAssignment>
<AttributeAssignment  AttributeId="obligation-attribute:note"
DataType="http://www.w3.org/2001/XMLSchema#string">Your Medical Record has been updated by Care Physician:n.karter-
</Obligation>
</Obligations>
</Result>
</Response>
```

Εικόνα 9. Response_2 για Physician

Μέσω της επιλογής **Try It**, εξομοιώνεται το κάθε αίτημα (Request) προς τον server ως εξής: Σε κάθε πεδίο του Server συμπληρώνεται η αντίστοιχη πληροφορία που αφορά το συγκεκριμένο Request, δηλ. στο πεδίο *Resource* συμπληρώνεται ο πόρος στον οποίον γίνεται η αίτηση για πρόσβαση, στο πεδίο *Subject Name* το υποκείμενο που αιτείται πρόσβασης, στο *Action Name* το είδος της πρόσβασης που ζητείται (read, write κλπ.) και τέλος στο πεδίο *Environment Name* συμπληρώνεται πληροφορία που σχετίζεται με περιβαλλοντικούς παράγοντες κατά την πρόσβαση (χρόνος κλπ.).

Για την αξιολόγηση του τρίτου και τελευταίου κανόνα της πολιτικής, ένα ενδεικτικό Request είναι το ακόλουθο: ο χρήστης με ρόλο ραδιολόγου, n.karter, επιθυμεί ανάγνωση ακτινογραφίας από το αρχείο του ασθενή g.smith (pid_0000001). Σε αυτήν την περίπτωση το σύστημα, ανασύρει από το αποθηκευμένο προφίλ του n.karter την ηλεκτρονική διεύθυνσή του και εφ'όσον αυτή ανήκει στο domain του πληροφοριακού συστήματος EMEDICA, τότε επιτρέπει την πρόσβαση, όπως φαίνεται και στην εικόνα 10.



Εικόνα 10. Request_3 για Physician

3.3 Περιγραφή Επιμέρους Πολιτικής - Policy_Patients

Η πολιτική ασφάλειας που αφορά τους ασθενείς (Policy_Patients) αποτελείται από 2 επιμέρους κανόνες:

- ❖ Rule_1: Ο ασθενής έχει πρόσβαση για ανάγνωση μόνο στο δικό του EHR
- ❖ Rule_2: Ο ασθενής μπορεί να κάνει update μόνο στο δικό του EHR και μόνο από local IPs του EMEDICA Clinic (192.168.1.1-192.168.1.255).

3.3.1 Ανάλυση Επιμέρους Πολιτικής - Policy_Patients

Το **<Policy>** element που έχει για αναγνωριστικό το xacml attribute **@PolicyId** ίσο με «**Policy_Patients**», αναπαριστά την επιμέρους πολιτική που καθορίζει τις προσβάσεις που μπορούν να έχουν οι χρήστες, των οποίων ο ρόλος είναι ασθενείς (**Patient**). Σημαντικά elements που περιέχονται στο προαναφερόμενο **<Policy>** element είναι το **<Target>** element και τα δύο **<Rule>** elements.

Το **<Target>** element καθορίζει την εφαρμοσιμότητα της επιμέρους πολιτικής ασφάλειας στο πεδίο των αιτημάτων πρόσβασης για χρήστες, των οποίων το χαρακτηριστικό **«role»** είναι «**Patient**». Συγκεκριμένα, χρησιμοποιείται ένα **<Match>** element που συγκρίνει μέσω της συνάρτησης «**string-regexp-match**» την συμβολοσειρά χαρακτήρων «**Patient**» με κάθε μια από τις δυνατές επιστρεφόμενες τιμές της σακούλας, που προκύπτει κατά την εφαρμογή του **<AttributeDesignator>** element στην ιδιότητα «**role**» της κατηγορίας **access-subject.** Σημειώνεται ότι, οι τιμές για το ανωτέρω χαρακτηριστικό προέρχονται από το Profile του χρήστη με βάση το αναγνωριστικό, χαρακτηριστικό «**subject-id**», που περιέχεται στο αίτημα πρόσβασης.

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule_PAT1**», αναπαριστά τον πρώτο κανόνα της πολιτικής για τους ασθενείς. Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι ασθενής, προσπαθεί να εκτελέσει την ενέργεια **read** σε κάποιον πόρο του συστήματος ή ισοδύναμα στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας **action** συμπίπτει με την συμβολοσειρά χαρακτήρων **read**.
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».
Στο **<Condition>** element έχει συμπεριληφθεί μόνο μια έκφραση, οι οποία θα πρέπει να δίνει την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**». Στην έκφραση αυτή συγκρίνουμε μέσω της συνάρτησης «**string-regexp-match**» την τιμή του χαρακτηριστικού «**url**» του χρήστη κατηγορίας «**access-subject**», με το πλήρες όνομα του πόρου, δηλ το χαρακτηριστικό «**resource-id**» της κατηγορίας «**resource**». Σημειώνεται ότι, το χαρακτηριστικό «**url**» για κάθε χρήστη με ρόλο ασθενή παριστάνει το μονοπάτι της διαδρομής που είναι αποθηκευμένα τα ιατρικά του αρχεία, ανεξαρτήτως εάν ο χρήστης κατέχει ταυτόχρονα και άλλους ρόλους. Το χαρακτηριστικό αυτό παίρνει την εξής μορφή:
«**/_emedica/ehealth/patients/pid_000000?/»** όπου ο χαρακτήρας «?» υποδηλώνει τον αύξων αριθμό του χρήστη στο σύστημα. Συνεπώς, ο κάθε χρήστης του οποίου ο ρόλος είναι ασθενής θα μπορεί να έχει πρόσβαση σε ιατρικά αρχεία, όπως το EHR, αλλά μόνο σε αυτά που αναφέρονται σε αυτόν ή ισοδύναμα περιέχονται σε φάκελο του οποίου η διαδρομή

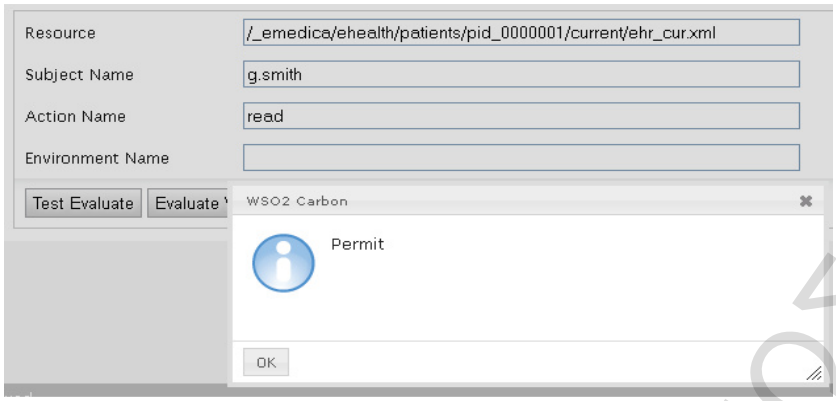
ταιριάζει με τον προκαθορισμένο στο σύστημα χώρο αποθήκευσης αρχείων για το συγκεκριμένο ασθενή.

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule_PAT2**», αναπαριστά τον δεύτερο κανόνα της πολιτικής για τους ασθενείς. Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι ασθενής, προσπαθεί να εκτελέσει την ενέργεια **write** σε κάποιον πόρο του συστήματος ή ισοδύναμα στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας **action** συμπίπτει με την συμβολοσειρά χαρακτήρων **write**.
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».

Στο **<Condition>** element έχουν συμπεριληφθεί δύο υπο-εκφράσεις, οι οποίες θα πρέπει να δίνουν και οι δυο την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**». Η πρώτη υπο-έκφραση είναι αντίστοιχη αυτής που εμπεριέχεται στον πρώτο κανόνα για τους ασθενείς. Η δεύτερη υπο-έκφραση χρησιμοποιείται για τις περιπτώσεις όπου η IP διεύθυνση του χρήστη είναι στο εύρος τιμών των τοπικών IP διευθύνσεων, οι οποίες θεωρούμε ότι ανήκουν στο σύνολο διευθύνσεων από **192.168.1.1** έως **192.168.1.255**. Η σύγκριση πραγματοποιείται μέσω της συνάρτησης «**ipAddress-regexp-match**» μεταξύ της συμβολοσειράς χαρακτήρων «**192.168.1.**» και της τιμής που προκύπτει από την εφαρμογή του **<AttributeDesignator>** element στο χαρακτηριστικό «**environment-id**» της κατηγορίας «**environment**». Σημειώνεται ότι αρχικά ο τύπος δεδομένων του χαρακτηριστικού «**environment-id**» είναι ο generic τύπος string ενώ με την εφαρμογή της συνάρτησης μετατροπής «**ipAddress-from-string**», το δεύτερο όρισμα παίρνει την επιθυμητή μορφή, δηλ τον τύπο δεδομένων που παριστάνει τις IP διευθύνσεις.

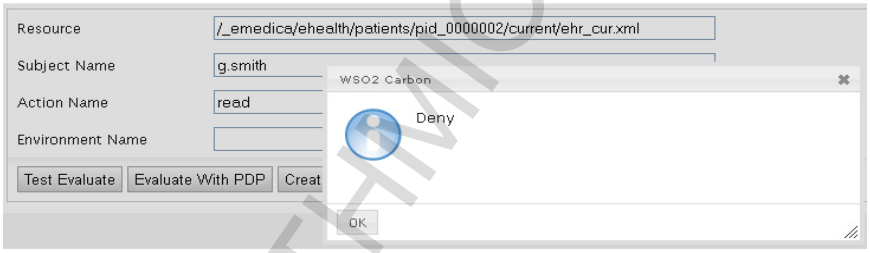
3.3.2 Αξιολόγηση και Επαλήθευση Πολιτικής - Policy_Patients

Στην ακόλουθη εικόνα (Εικόνα 11) απεικονίζονται το Request μαζί με το αντίστοιχο Response, τα οποία τεστάρουν τον πρώτο κανόνα της πολιτικής για τους ασθενείς. Ο χρήστης του οποίου ο ρόλος είναι «ασθενής» με pid_0000001, δηλ. ο g.smith αιτείται ανάγνωσης του EHR που βρίσκεται στο συγκεκριμένο path (/_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml). Το αντίστοιχο Response είναι Permit.



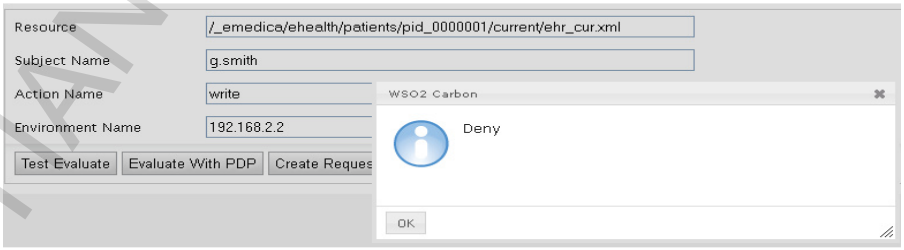
Εικόνα 11. Request_1a για Patients

Εάν όμως ο ίδιος χρήστης προσπαθήσει να διαβάσει το ηλεκτρονικό αρχείο υγείας που βρίσκεται κάτω από διαφορετικό path (πχ. το (/_emedica/ehealth/patients/pid_0000002/current/ehr_cur.xml), που ανήκει στον ασθενή με pid_0000002 (s.molder), η απάντηση σε αυτή την αίτηση, όπως είναι αναμενόμενο θα είναι Deny (Εικόνα 12).



Εικόνα 12. Request_1b για Patients

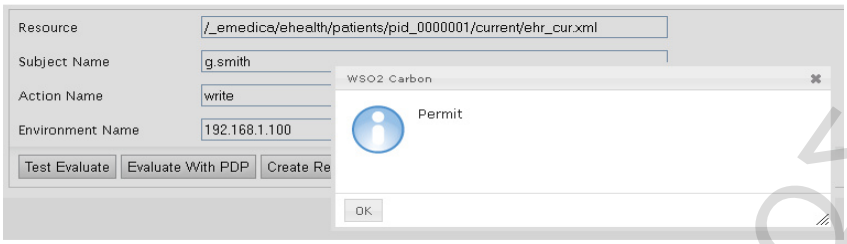
Για την αξιολόγηση του δεύτερου κανόνα της πολιτικής ασφάλειας για τους ασθενείς (Εικόνα 13), έστω ότι ο χρήστης με ρόλο Patient (g.smith) κάνει αίτηση για ενημέρωση (update) του δικού του EHR από IP που δεν ορίζεται σαν local IP της κέντρου υγείας EMEDICA (για παράδειγμα 192.168.2.2).



Εικόνα 13. Request_2a για Patients

Σε αυτήν την περίπτωση, το αποτέλεσμα αυτού του Request θα είναι Deny.

Ενώ, όταν η IP από την οποία αιτείται πρόσβασης ο «patient» βρίσκεται μέσα στο εύρος των καθορισμένων ως local IPs (192.168.1.1-192.168.1.255), τότε η απάντηση είναι Permit (Εικόνα 14).



Εικόνα 14. Request_2b για Patients

3.4 Περιγραφή Επιμέρους Πολιτικής - Policy_Guardians

Η πολιτική που σχετίζεται με τον έλεγχο πρόσβασης για χρήστες με ρόλο Guardian (κηδεμόνα) περιλαμβάνει τον ακόλουθο κανόνα:

- Rule_1: Ο κηδεμόνας μπορεί να διαβάσει και να γράψει σε οποιοδήποτε στοιχείο του EHR, το οποίο ανήκει στο δικό του προστατευόμενο μέλος και μόνο αν αυτό έχει ηλικία μικρότερη ή ίση των 16 ετών.

3.4.1 Ανάλυση Επιμέρους Πολιτικής - Policy_Guardians

Το **<Policy>** element που έχει για αναγνωριστικό το xacml attribute **@PolicyId** ίσο με «**Policy_Guardians**», αναπαριστά την επιμέρους πολιτική που καθορίζει τις προσβάσεις που μπορούν να έχουν οι χρήστες, των οποίων ο ρόλος είναι κηδεμόνας (**Guardian**). Σημαντικά elements που περιέχονται στο προαναφερόμενο **<Policy>** element είναι το **<Target>** και **<Rule>** elements.

Στο **<Target>** element χρησιμοποιείται ένα **<Match>** element που συγκρίνει μέσω της συνάρτησης «**string-regexp-match**» την συμβολοσειρά χαρακτήρων «**Guardian**» με κάθε μια από τις δυνατές επιστρεφόμενες τιμές της σακούλας, που προκύπτει κατά την εφαρμογή του **<AttributeDesignator>** element στο χαρακτηριστικό «**role**» της κατηγορίας «**access-subject**».

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule_PAR1**», αναπαριστά τον ένα και μοναδικό κανόνα της πολιτικής για τους κηδεμόνες. Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι κηδεμόνας, προσπαθεί να εκτελέσει είτε την ενέργεια **read** είτε την ενέργεια **write** σε κάποιον πόρο του συστήματος που ανήκει σε προστατευόμενο μέλος του ή ισοδύναμα στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας **action** συμπίπτει είτε με την συμβολοσειρά χαρακτήρων **read** είτε με την συμβολοσειρά **write**. Επιπρόσθετα, θα πρέπει ο κανονικός δικαιούχος του πόρου

(**resource**) πρόσβασης να διαθέτει ρόλο ασθενή στο σύστημα ή ισοδύναμα στο **<Target>** element και εσωτερικά ξεχωριστού **<AnyOf>** element, το χαρακτηριστικό «**role**» της κατηγορίας «**recipient-subject**» θα πρέπει να συμπίπτει με την συμβολοσειρά χαρακτήρων «**Patient**».
Στο σημείο αυτό, χρησιμοποιήθηκε η δυνατότητα που παρέχει η γλώσσα XACML για υποστήριξη πολλαπλών χρηστών (**multiple subjects**) κατά την διαδικασία αιτήσεων πρόσβασης. Υπάρχει όμως η αυστηρή οδηγία ότι οι διάφοροι χρήστες θα πρέπει να ενεργούν υπό διαφορετική ιδιότητα. Στην περίπτωσή μας έχουμε χρήστες της κατηγορίας «**access-subject**» με ρόλο κηδεμόνα και για τα προστατευόμενα μέλη τους χρησιμοποιήθηκε η κατηγορία χρηστών «**recipient-subject**», η οποία εσωκλείει όλα τα απαραίτητα χαρακτηριστικά στο αίτημα πρόσβασης. Σημειώνεται ότι, η κανονική χρήση της κατηγορίας χρηστών «**recipient-subject**», σύμφωνα με το πρότυπο της XACML, προορίζεται για τις περιπτώσεις όπου η απόφαση του αιτήματος πρόσβασης θα κατευθυνθεί προς διαφορετικό χρήστη σε σχέση με εκείνον που αιτήθηκε αρχικά της πρόσβασης σε κάποιον πόρο.

Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».

Στο **<Condition>** element έχουν συμπεριληφθεί τρεις υπο-εκφράσεις, οι οποίες θα πρέπει να δίνουν και οι τρεις την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**».

- $1^{η}$ συνθήκη

Ο προκαθορισμένος φάκελος αποθήκευσης των ιατρικών αρχείων του ασθενούς ταιριάζει με την διαδρομή του πόρου, που ο χρήστης αιτήθηκε, ή ισοδύναμα το χαρακτηριστικό «**url**» του χρήστη κατηγορίας «**recipient-subject**» ταιριάζει κατά μοτίβο συμβολοσειράς (συνάρτηση ταιριάσματος «**string-regexp-match**») με το χαρακτηριστικό «**resource-id**» της κατηγορίας «**resource**».

- $2^{η}$ συνθήκη

Υπάρχει έγκυρη σχέση κηδεμόνα-ασθενή μεταξύ των δύο περιεχομένων κατηγοριών χρηστών στο αίτημα πρόσβασης. Η σχέση αυτή αναπαρίσταται από το χαρακτηριστικό «**title**» του Profile, όπου για κάθε κηδεμόνα έχει συμπεριληφθεί ως τιμή του χαρακτηριστικού η συμβολοσειρά guardianof_<**user**>. Σημειώνεται ότι, υπάρχει η δυνατότητα ορισμού πολλαπλών τιμών για κάθε χαρακτηριστικό χρήστη, με κάθε μια να χωρίζεται από τις υπόλοιπες μέσω του χαρακτήρα «**,**», δηλαδή το χαρακτηριστικό «**title**» μπορεί να πάρει την συνολική τιμή « guardianof_<**user1**>, guardianof_<**user2**> ». Συνεπώς, στην έκφραση συγκρίνεται το χαρακτηριστικό «**title**» του χρήστη κατηγορίας «**access-subject**» (κηδεμόνας) με το όρισμα που προκύπτει από την ένωση των συμβολοσειρών «**guardianof_**» και του χαρακτηριστικού «**recipient-id**» του χρήστη κατηγορίας «**recipient-subject**» (ασθενής).

- $3^{η}$ συνθήκη

Ο ασθενής θα πρέπει να είναι είτε μικρότερος είτε στην ηλικία των δεκαέξι ετών για να μπορεί ο κηδεμόνας του την συγκεκριμένη χρονική στιγμή να προσπελάσει τα ιατρικά του αρχεία. Η ανωτέρω πρόταση απεικονίζεται με την παρακάτω εξίσωση:

(Τρέχον Έτος) – (Έτος Γέννησης) ≤ 16 ⇔ (Έτος Γέννησης) +16 ≥ (Τρέχον Έτος)

Συνεπώς, συγκρίνουμε το έτος γέννησης του ασθενή, χαρακτηριστικό «**dob**» του χρήστη κατηγορίας «**recipient-subject**», προσαυξημένο κατά 16 έτη (συνάρτηση «**integer-add**»), με το χαρακτηριστικό «**environment-id**» της κατηγορίας «**environment**» (τρέχον έτος). Για την μετατροπή των ορισμάτων από τον τύπο τιμών string στον τύπο ακεραίου χρησιμοποιήθηκε η συνάρτηση «**integer-from-string**», ενώ για την μετατροπή της σακούλας τιμών σε μοναδική τιμή χρησιμοποιήθηκε η συνάρτηση «**string-one-and-only**».

3.4.2 Αξιολόγηση και Επαλήθευση Πολιτικής - Policy_Guardians

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">w.molder</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:recipient-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">s.molder</AttributeValue>
</Attribute>
<Attribute AttributeId="http://wso2.org/claims/role" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patient</AttributeValue>
</Attribute>
<Attribute AttributeId="http://wso2.org/claims/url" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000002/</AttributeValue>
</Attribute>
<Attribute AttributeId="http://wso2.org/claims/dob" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">2000</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000002/current/ehr_cur.xml</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">2013</AttributeValue>
```

Εικόνα 15. Request_1a για Guardians

Ένα ενδεικτικό Request για την επαλήθευση του κανόνα πρόσβασης για χρήστες με ρόλο "Guardian", αποτυπώνεται στην παραπάνω εικόνα (Εικόνα 15). Όπως φαίνεται, ο χρήστης-κηδεμόνας w.molder με προστατευόμενο μέλος τον χρήστη-ασθενή s.molder, αιτείται ανάγνωσης του EHR του ασθενή με pid_0000002 (που αντιστοιχεί στον ασθενή s.molder). Στο Request φαίνεται επίσης ότι ο συγκεκριμένος ασθενής έχει χρονολογία γέννησης το 2000 και ότι το τρέχον έτος είναι το 2013. Οπότε με βάση την κατασκευή της αντίστοιχης πολιτικής για τους Guardians, το αποτέλεσμα της αίτησης είναι Permit (Εικόνα 16).

Entitlement Policy Response [XACML]

10 pt

```
1  <Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
2  <Result>
3  <Decision>Permit</Decision>
4  <Status>
5  <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
6  </Status>
7  </Result>
8  </Response>
9
10
```

Εικόνα 16. Response_1a για Guardians

Στο παραπάνω Request, αν ο χρήστης-κηδεμόνας w.molder (με προστατευόμενο μέλος τον χρήστη-ασθενή s.molder), αιτείται ανάγνωσης του EHR του ασθενή με pid_0000001 (που αντιστοιχεί στον ασθενή g.smith), τότε όπως φαίνεται και στις παρακάτω εικόνες (εικόνες 17, 18), η αίτηση θα απορριφθεί.

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">w.molder</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:recipient-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">g.smith</AttributeValue>
</Attribute>
<Attribute AttributeId="http://wso2.org/claims/role" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patient</AttributeValue>
</Attribute>
<Attribute AttributeId="http://wso2.org/claims/url" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000001/</AttributeValue>
</Attribute>
<Attribute AttributeId="http://wso2.org/claims/dob" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">1932</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:environment">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">2013</AttributeValue>
```

Εικόνα 17. Request_1b για Guardians

Entitlement Policy Response [XACML]

```
1  <Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
2  <Result>
3  <Decision>Deny</Decision>
4  <Status>
5  <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
6  </Status>
7  </Result>
8  </Response>
9
10
```

Εικόνα 18. Response_1b για Guardians

3.5 Περιγραφή Επιμέρους Πολιτικής - Policy_Nurses

Η πολιτική ασφάλειας για τους χρήστες του συστήματος που κατέχουν το ρόλο Nurse (Νοσοκόμος/α) δομείται από τους παρακάτω τέσσερις κανόνες:

- Rule_1: Η νοσοκόμα μπορεί να διαβάσει το στοιχείο <Result> από ένα EHR, μόνο αν είναι η υπεύθυνη για τις συγκεκριμένες ιατρικές εξετάσεις.

- Rule_2: Η νοσοκόμα μπορεί να δημιουργήσει ένα καινούργιο στοιχείο <Result> για ένα EHR ενός ασθενή.

- Rule_3: Η νοσοκόμα μπορεί να γράψει μόνο στα στοιχεία <Notes> και <Result> ενός EHR, και μόνο αν είναι η υπεύθυνη για τις συγκεκριμένες ιατρικές εξετάσεις.

- Rule_4: Η νοσοκόμα δεν μπορεί να γράψει στα στοιχεία <TestType>, <Value>, <PerformedDate> και <PerformedBy> .

3.5.1 Ανάλυση Επιμέρους Πολιτικής - Policy_Nurses

Το **<Policy>** element που έχει για αναγνωριστικό το xacml attribute **@PolicyId** ίσο με «**Policy_Nurses**», αναπαριστά την επιμέρους πολιτική που καθορίζει τις προσβάσεις που μπορούν να έχουν οι χρήστες, των οποίων ο ρόλος είναι νοσοκόμος (**Nurse**). Σημαντικά elements που περιέχονται στο προαναφερόμενο **<Policy>** element είναι το **<Target>** και **<Rule>** elements.
Στο **<Target>** element χρησιμοποιείται ένα **<Match>** element που συγκρίνει μέσω της συνάρτησης «**string-regexp-match**» την συμβολοσειρά χαρακτήρων «**Nurse**» με κάθε μια από τις δυνατές επιστρεφόμενες τιμές της σακούλας, που προκύπτει κατά την εφαρμογή του **<AttributeDesignator>** element στο χαρακτηριστικό «**role**» της κατηγορίας «**access-subject**».
Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-NUR1**», αναπαριστά τον πρώτο κανόνα της πολιτικής για νοσοκόμους.
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι νοσοκόμος, προσπαθεί να εκτελέσει την ενέργεια **read** σε κάποιον πόρο του συστήματος ή ισοδύναμα στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» συμπίπτει με την συμβολοσειρά χαρακτήρων **read**.
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».

Στο **<Condition>** element έχουν συμπεριληφθεί τρεις υπο-εκφράσεις, οι οποίες θα πρέπει να δίνουν και οι τρεις την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**».

- 1η συνθήκη

Το χαρακτηριστικό ταυτοποίησης Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ – SSN_ID) μιας νοσοκόμας θα πρέπει να συμπίπτει με αυτό που περιέχεται εσωτερικά του element **<MedicalRec>**, στο EHR του ασθενούς. Συνεπώς, θα πρέπει το χαρακτηριστικό «**im**» του χρήστη κατηγορίας «**access-subject**» να συμπίπτει (συνάρτηση «**string-equal**») με οποιαδήποτε από τις τιμές που περιέχονται στη σακούλα τιμών, η οποία προκύπτει από την εφαρμογή του element **<AttributeSelector>** στα περιεχόμενα στοιχεία του πόρου EHR, σύμφωνα με την XPath έκφραση:

@Path="//xacml:**ehealthrec**/xacml:**MedicalRec**/xacml:**Treatment**/xacml:**Result**/
xacml:**PerformedBy**/text()"

- 2η συνθήκη

Ο πόρος του συστήματος, το υπο-στοιχείο του οποίου ζητείται να διαβαστεί από τον χρήστη (Ηλεκτρονικό Αρχείο Υγείας ασθενούς - EHR) θα πρέπει να ακολουθεί το μοτίβο τόσο για το όνομα όσο και για το πλήρες μονοπάτι που έχει προκαθοριστεί για τους ασθενείς στο Πληροφοριακό Σύστημα **E-MEDICA**:
Μονοπάτι ⇔ /_emedica/ehealth/patients/pid_[επταψήφιος αριθμός]/current/

Όνομα πόρου ⇔ ehr_cur.xml

- 3η συνθήκη

Το συγκεκριμένο υπό-στοιχείο εντός του πόρου EHR, που ο χρήστης αιτείται πρόσβασης, είναι το **<Result>** element. Συνεπώς συγκρίνεται η συμβολοσειρά «**Result**», μέσω της συνάρτησης «**string-regexp-match**», με το χαρακτηριστικό «**resource-name**» της κατηγορίας «**resource**». Το προαναφερόμενο χαρακτηριστικό είναι τύπου user-defined, και αυτό μπορεί να παρατηρηθεί και από το αναγνωριστικό του attribute **@AttributeId**, που είναι ίσο με το URI «http:://wso2.org/**my_attributes**/resource-name». Σημειώνεται ότι, αντίστοιχο χαρακτηριστικό έχει συμπεριληφθεί και στο αίτημα πρόσβασης, στην κατηγορία χαρακτηριστικών «**resource**», για να παριστάνει το υπο-στοιχείο εντός του πόρου πρόσβασης που ο χρήστης ζητεί να προσπελάσει.
Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-NUR2**», αναπαριστά τον δεύτερο κανόνα της πολιτικής για νοσοκόμους.
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι νοσοκόμος, προσπαθεί να εκτελέσει την ενέργεια (action) **create** σε κάποιον πόρο (resource) του συστήματος ή ισοδύναμα στο **<Target>**

element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» συμπίπτει με την συμβολοσειρά χαρακτήρων **create**.
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».

Στο **<Condition>** element έχουν συμπεριληφθεί δύο υπο-εκφράσεις, οι οποίες θα πρέπει να δίνουν και οι δυο την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**».
Οι υπο-εκφράσεις που έχουν συμπεριληφθεί στον υπο-εξέταση κανόνα είναι αντίστοιχες με τις δύο τελευταίες υπο-εκφράσεις του προηγούμενου κανόνα.

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-NUR3**», αναπαριστά τον τρίτο κανόνα της πολιτικής για νοσοκόμους.
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι νοσοκόμος, προσπαθεί να εκτελέσει την ενέργεια **write** στο υπο-στοιχείο **<NurseNotes>** του πόρου EHR ενός ασθενούς ή ισοδύναμα στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» συμπίπτει με την συμβολοσειρά χαρακτήρων **write** και επιπρόσθετα το χαρακτηριστικό «**resource-name**» της κατηγορίας «**resource**» συμπίπτει (συνάρτηση «**string-equal**») με την συμβολοσειρά χαρακτήρων «**NurseNotes**».
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».
Στο **<Condition>** element έχουν συμπεριληφθεί δύο υπο-εκφράσεις, οι οποίες θα πρέπει να δίνουν και οι δυο την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**».

- $1^{η}$ συνθήκη

Το χαρακτηριστικό ταυτοποίησης Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ – SSN_ID) μιας νοσοκόμας θα πρέπει να συμπίπτει με αυτό που περιέχεται εσωτερικά του element **<MedicalRec>**, στο EHR του ασθενούς.

- $2^{η}$ συνθήκη

Ο πόρος του συστήματος, το υπο-στοιχείο του οποίου ζητείται να διαβαστεί από τον χρήστη (Ηλεκτρονικό Αρχείο Υγείας ασθενούς - EHR) θα πρέπει να ακολουθεί το μοτίβο τόσο για το όνομα όσο και για το πλήρες μονοπάτι που έχει προκαθοριστεί για τους ασθενείς στο Πληροφοριακό Σύστημα **E-MEDICA**:

Μονοπάτι ⇔ /_emedica/ehealth/patients/pid_[επταψήφιος αριθμός]/current/

Όνομα πόρου ⇔ ehr_cur.xml

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-NUR4**», αναπαριστά τον τέταρτο κανόνα της πολιτικής για νοσοκόμους.
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι νοσοκόμος, προσπαθεί να εκτελέσει την ενέργεια **write** σε κάποιο υπο-στοιχείο διάφορο του element **<NurseNotes>**, εσωτερικά του element

<Result>, του πόρου EHR ενός ασθενούς ή ισοδύναμα στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» συμπίπτει με την συμβολοσειρά χαρακτήρων **write** και επιπρόσθετα το χαρακτηριστικό «**resource-name**» της κατηγορίας «**resource**» συμπίπτει (συνάρτηση «**string-equal**») με οποιαδήποτε εκ των παρακάτω συμβολοσειρών χαρακτήρων:

- «**TestType**»
- «**Value**»
- «**PerformedDate**»
- «**PerformedBy**»

Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Deny**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».
Στο **<Condition>** element έχουν συμπεριληφθεί δύο υπο-εκφράσεις, οι οποίες θα πρέπει να δίνουν και οι δυο την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**».

- $1^{η}$ συνθήκη

Το χαρακτηριστικό ταυτοποίησης Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ – SSN_ID) μιας νοσοκόμας θα πρέπει να συμπίπτει με αυτό που περιέχεται εσωτερικά του element **<MedicalRec>**, στο EHR του ασθενούς.

- $2^{η}$ συνθήκη

Ο πόρος του συστήματος, το υπο-στοιχείο του οποίου ζητείται να διαβαστεί από τον χρήστη (Ηλεκτρονικό Αρχείο Υγείας ασθενούς - EHR) θα πρέπει να ακολουθεί το μοτίβο τόσο για το όνομα όσο και για το πλήρες μονοπάτι που έχει προκαθοριστεί για τους ασθενείς στο Πληροφοριακό Σύστημα **E-MEDICA**:

Μονοπάτι ⇔ /_emedica/ehealth/patients/pid_[επταψήφιος αριθμός]/current/

Όνομα πόρου ⇔ ehr_cur.xml

Συνεπώς, σε περίπτωση που πληρούνται οι συνθήκες Target-**Match** και Condition-**True** ο ανωτέρω κανόνας καταλήγει σε απόφαση «**Deny**», επιπλέον όμως παρέχονται συμπληρωματικές πληροφορίες προς τον χρήστη για τον λόγο που του αρνήθηκε η πρόσβαση. Για την υλοποίηση του ανωτέρω έχει συμπεριληφθεί στο τέλος του κανόνα το element **<AdviceExpressions>**, το οποίο περιέχει εκφράσεις που παρέχονται βοηθητικά στο PEP εάν ο κανόνας καταλήξει στην απόφαση «**Deny**» (xacml attribute **@AppliesTo**). Το προαναφερόμενο element περιέχει ένα βοηθητικό μήνυμα για το χρήστη, αυτό της μη-δυνατότητας τροποποίησης κάποιου στοιχείου εσωτερικά του EHR (xacml attribute **@AdviceId** = «**NO_UPDATES_ALLOWED**»). Για την κατασκευή του μηνύματος χρησιμοποιείται το xacml element **<AttributeAssignmentExpression>**, το οποίο περιέχει την ακόλουθη συμβολοσειρά χαρακτήρων: «**You are not allowed to update these elements. Proceed to perform a new Test.**»

3.5.2 Αξιολόγηση και Επαλήθευση της πολιτικής - Policy_Nurses

Για την αξιολόγηση του πρώτου κανόνα, έστω ότι ο χρήστης με ρόλο «Nurse», s.jacson αιτείται ανάγνωσης του element <Result> που ανήκει στο EHR ενός χρήστη-ασθενή (Εικόνα 19), για παράδειγμα του g.smith (pid_0000001). Εφ'όσον το sub-element <PerformedBy> που βρίσκεται μέσα στο element <MedicalRec> του EHR, συμπίπτει με τον αριθμό κοινωνικής ασφάλισης (SSN) του χρήστη «Nurse» που κάνει την αίτηση πρόσβασης, τότε το αποτέλεσμα θα είναι Permit, όπως φαίνεται και στα επόμενες εικόνες (εικόνες 20, 21).

```
<MedicalRec>
    <Treatment>
        <Prescription>
        <PhysicianNotes>Patient is having high body temperature and neck pain</PhysicianNotes>
        <Result>
            <TestType>Body Temperature</TestType>
            <Value>37.5 C</Value>
            <PerformedDate>3/4/2013</PerformedDate>
            <PerformedBy>05028216572</PerformedBy>
            <NurseNotes>Patients temperature becomes stable</NurseNotes>
        </Result>
    </Treatment>
    <Status>OPEN</Status>
    <LeaveDate>NULL</LeaveDate>
    <BlockMark>NO</BlockMark>
</MedicalRec>
```

Εικόνα 19. Απεικόνιση του στοιχείου <Result>

Request_Nurses_1.xml

```
1  <Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
2  <!--Action Category-->
3  <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
4  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
5  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
6  </Attribute>
7  </Attributes>
8  <!--Subject Category-->
9  <Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
10 <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
11 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">s.jacson</AttributeValue>
12 </Attribute>
13 </Attributes>
14 <!--Resource Category-->
15 <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
16 <Content>
17 <ehealthrec id="24023203132">
85 </Content>
86 <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
87 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
88                 /_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml</AttributeValue>
89 </Attribute>
90 <Attribute AttributeId="http:://wso2.org/my_attributes/resource-name" IncludeInResult="false">
91 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Result</AttributeValue>
92 </Attribute>
93 </Attributes>
94 <!-- -->
95 </Request>
```

Εικόνα 20. Request_1a για Nurses

Evaluate Entitlement Policy

Entitlement Policy Response [XACML]

```
<Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
<Result>
<Decision>Permit</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

Εικόνα 21. Response_1a για Nurses

Εάν όμως αντί του χρήστη “Nurse” s.jacson, έκανε το ίδιο Request ένας άλλος χρήστης «Nurse» για παράδειγμα η v.sting, η οποία έχει διαφορετικό SSN με βάση το προφίλ (08098992032) από αυτό που αναγράφεται στο EHR του ασθενούς, τότε θα αναμενόταν αρνητικό Response (Deny). Αυτό καταγράφεται στις εικόνες 22 και 23.

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<!--Action Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
</Attribute>
</Attributes>
<!--Subject Category-->
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">v.sting</AttributeValue>
</Attribute>
</Attributes>
<!--Resource Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Content>
<ehealthrec id="24023203132">
</Content>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml</AttributeValue>
</Attribute>
<Attribute AttributeId="http::://wso2.org/my_attributes/resource-name" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Result</AttributeValue>
</Attribute>
</Attributes>
<!-- -->
</Request>
```

Εικόνα 22. Request_1b για Nurses

```
<Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
<Result>
<Decision>Deny</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

Εικόνα 23. Response_1b για Nurses

Όσον αφορά τον δεύτερο κανόνα, στο επόμενο ΣΧΗΜΑ, ο χρήστης s. jacson κάνει αίτηση για δημιουργία ενός νέου <Result> element μέσα στο EHR του χρήστη με ρόλο ασθενή g.smith. Το αποτέλεσμα του Request όπως είναι αναμενόμενο είναι Permit (εικόνες 24, 25).

Request_Nurses_2.xml

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<!--Action Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">create</AttributeValue>
</Attribute>
</Attributes>
<!--Subject Category-->
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">s.jacson</AttributeValue>
</Attribute>
</Attributes>
<!--Resource Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml</AttributeValue>
</Attribute>
<Attribute AttributeId="http:://wso2.org/my_attributes/resource-name" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Result</AttributeValue>
</Attribute>
</Attributes>
<!-- -->
</Request>
```

Εικόνα 24. Request_2 για Nurses

Entitlement Policy Response [XACML]

```
<Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
<Result>
<Decision>Permit</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

Εικόνα 25. Response_2 για Nurses

Σχετικά με τον τρίτο κανόνα της πολιτικής, ο χρήστης με ρόλο «Nurse», s.jacson, αιτείται εγγραφής στο <NurseNotes> element του EHR του ασθενή με pid_0000001. Όμοια με την πρώτη περίπτωση, δεδομένου ότι στο συγκεκριμένο EHR έχει καταχωρηθεί το SSN του αιτούμενου χρήστη “Nurse”, πάντα στο <PerformedBy> element, η αίτηση εγγραφής θα έχει αποτέλεσμα Permit (εικόνες 26, 27).

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<!--Action Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
</Attribute>
</Attributes>
<!--Subject Category-->
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">s.jacson</AttributeValue>
</Attribute>
</Attributes>
<!--Resource Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Content>
<ehealthrec id="24023203132">
</Content>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml</AttributeValue>
</Attribute>
<Attribute AttributeId="http:://wso2.org/my_attributes/resource-name" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">NurseNotes</AttributeValue>
</Attribute>
</Attributes>
<!-- -->
</Request>
```

Εικόνα 26. Request_3 για Nurses

```
<Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
<Result>
<Decision>Permit</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

Εικόνα 27. Response_3 για Nurses

Τέλος για τον τέταρτο κανόνα της πολιτικής, ο χρήστης «Nurse» προσπαθεί να γράψει μέσα σε ένα από τα απαγορευμένα sub-elements του <Result> element, για παράδειγμα το <Value>. Εφόσον εκεί η συγκεκριμένη ομάδα χρηστών «Nurse» δεν έχει δικαίωμα για πράξη τροποποίησης μετά της αρχικής εγγραφής, η αίτηση λαμβάνει απόφαση Deny, σύμφωνα με τις εικόνες 28 και 29. Την αρνητική απάντηση, στην αίτηση, συνοδεύει και η συμβουλή ότι επιτυχημένη αίτηση εγγραφής στο παραπάνω element, γίνεται μόνο υπό την προϋπόθεση διεξαγωγής νέας εξέτασης.

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<!--Action Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
</Attribute>
</Attributes>
<!--Subject Category-->
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">s.jacson</AttributeValue>
</Attribute>
</Attributes>
<!--Resource Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Content>
<ehealthrec id="24023203132">
</Content>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml</AttributeValue>
</Attribute>
<Attribute AttributeId="http::://wso2.org/my_attributes/resource-name" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Value</AttributeValue>
</Attribute>
</Attributes>
<!-- -->
</Request>
```

Εικόνα 28. Request_4 για Nurses

Entitlement Policy Response [XACML]

```
1                   <Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
2  <Result>
3  <Decision>Deny</Decision>
4  <Status>
5  <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
6  </Status>
7  <AssociatedAdvice>
8  <Advice AdviceId="NO_UPDATES_ALLOWED" >
9  <AttributeAssignment  AttributeId="advise-attribute:message" DataType="http://www.w3.org/2001/XMLSchema#string">
10 You are not allowed to update these elements. Proceed to perform a new Test.</AttributeAssignment>
11 </Advice>
12 </AssociatedAdvice>
13 </Result>
14 </Response>
```

Εικόνα 29. Response_4 για Nurses

3.6 Περιγραφή Επιμέρους Πολιτικής - Policy_Accountants

Η πολιτική για χρήστες με ρόλο Accountant (Λογιστής), αποτελείται από δύο διακριτούς κανόνες:

- Rule_1: Ο Λογιστής μπορεί να διαβάσει οποιαδήποτε απόδειξη αποθηκευμένη στο σύστημα.
- Rule_2: Ο Λογιστής μπορεί να ενημερώνει (write) οποιαδήποτε απόδειξη αποθηκευμένη στο σύστημα, μόνο σε ώρες γραφείου (07:00-15:00).

3.6.1 Ανάλυση Επιμέρους Πολιτικής - Policy_Accountants

Το **<Policy>** element που έχει για αναγνωριστικό το xacml attribute **@PolicyId** ίσο με «**Policy_Accountants**», αναπαριστά την επιμέρους πολιτική που καθορίζει τις προσβάσεις που μπορούν να έχουν οι χρήστες, των οποίων ο ρόλος είναι λογιστές (**Accountant**). Σημαντικά elements που περιέχονται στο προαναφερόμενο **<Policy>** element είναι τα **<Target>** και **<Rule>** elements.

Στο **<Target>** element χρησιμοποιείται ένα **<Match>** element που συγκρίνει μέσω της συνάρτησης «**string-regexp-match**» την συμβολοσειρά χαρακτήρων «**Accountant**» με κάθε μια από τις δυνατές επιστρεφόμενες τιμές της σακούλας, που προκύπτει κατά την εφαρμογή του **<AttributeDesignator>** element στο χαρακτηριστικό «**role**» της κατηγορίας «**access-subject**».

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-ACC1**», αναπαριστά τον πρώτο κανόνα της πολιτικής για λογιστές.
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι λογιστής, προσπαθεί να εκτελέσει την ενέργεια (action) **write** σε κάποιο από τα φορολογικά παραστατικά (π.χ. πόρος **invoice_1.txt**) που αποθηκεύονται στο σύστημα ή ισοδύναμα στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» συμπίπτει με την συμβολοσειρά χαρακτήρων **write** και το χαρακτηριστικό «**resource-id**» της κατηγορίας «**resource**» περιέχει το μονοπάτι της διαδρομής «**/_emedica/ehealth/invoices**», φάκελος που έχει επιλεγεί για την αποθήκευση όλων των πόρων τύπου παραστατικών.
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».

Στο **<Condition>** element έχει συμπεριληφθεί μία μόνο έκφραση, η οποία θα πρέπει να δίνει την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**». Στην έκφραση αυτή χρησιμοποιείται η συνάρτηση «**time-in-range**», για να διαπιστωθεί εάν το αίτημα πρόσβασης πραγματοποιείται σε χρονικό διάστημα εντός των συνηθισμένων ωρών εργασίας, δηλ. από **07:00:00** το πρωί έως **15:00:00** το μεσημέρι. Η συνάρτηση «**time-in-range**» δέχεται τρία ορίσματα τύπου δεδομένων **time**, και επιστρέφει τιμή «**True**», όταν το πρώτο όρισμα βρίσκεται εντός των ορίων που καθορίζονται από τα δύο τελευταία ορίσματα. Το πρώτο όρισμα της έκφρασης προκύπτει από το χαρακτηριστικό «**environment-id**» της κατηγορίας χαρακτηριστικών «**environment**», το οποίο δίδεται στο αρχικό request και παριστάνει την τρέχουσα ώρα. Για την μετατροπή της σακούλας τιμών, που επιστρέφει το element **<AttributeDesignator>**, σε μοναδική τιμή χρησιμοποιήθηκε η

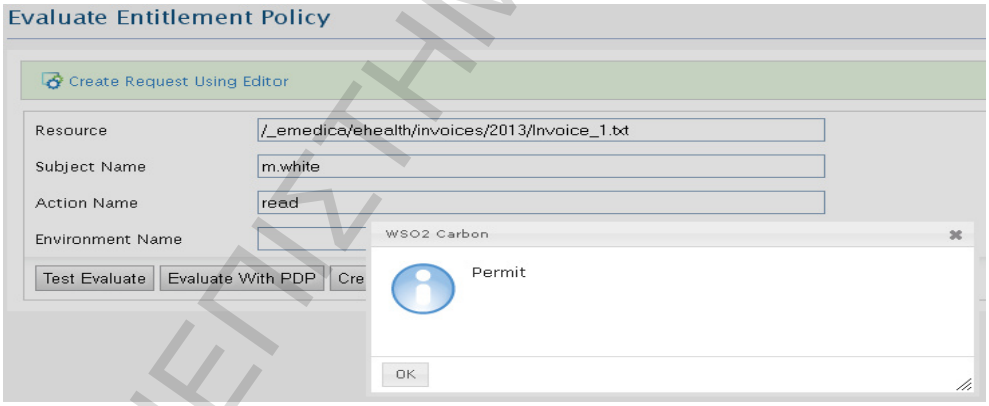
συνάρτηση «**string-one-and-only**», ενώ για την μετατροπή της τιμή στον επιθυμητό τύπο δεδομένων χρησιμοποιήθηκε η συνάρτηση «**time-from-string**».

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-ACC2**», αναπαριστά τον δεύτερο κανόνα της πολιτικής για λογιστές.
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι λογιστής, προσπαθεί να εκτελέσει την ενέργεια (action) **read** σε κάποιο από τα φορολογικά παραστατικά (π.χ. πόρος **invoice_1.txt**) που αποθηκεύονται στο σύστημα ή ισοδύναμα στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» συμπίπτει με την συμβολοσειρά χαρακτήρων **read** και το χαρακτηριστικό «**resource-id**» της κατηγορίας «**resource**» περιέχει το μονοπάτι της διαδρομής «**/_emedica/ehealth/invoices**», φάκελος που έχει επιλεγεί για την αποθήκευση όλων των πόρων τύπου παραστατικών.

Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός του **<Target>** element καταλήγει σε αληθή έκφραση, δηλ. το **<Target>** σε «**Match**». Σημειώνεται ότι, ο κανόνας δεν περιέχει κάποιο **<Condition>** element.

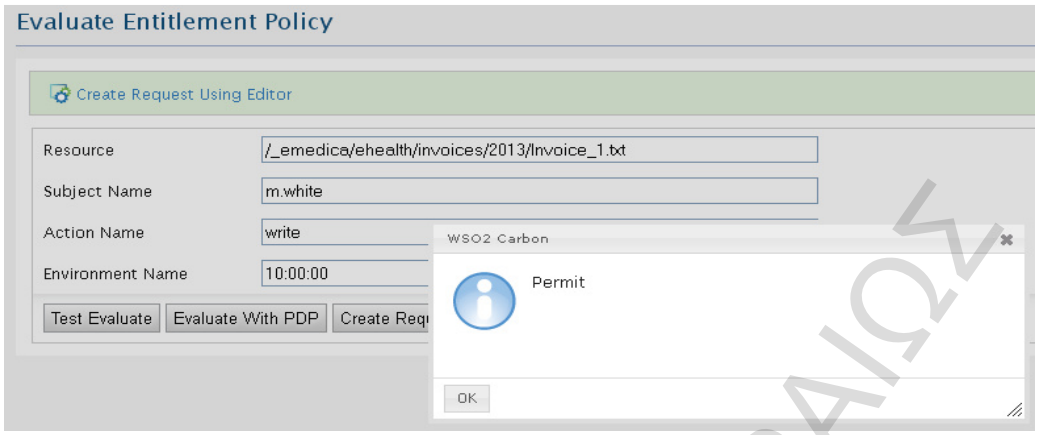
3.6.2 Αξιολόγηση και Επαλήθευση Επιμέρους Πολιτικής - Policy_Accountants

Η παρακάτω εικόνα (εικόνα 30) δείχνει το Request που σχετίζεται με την πολιτική για τους λογιστές.



Εικόνα 30. Request_1/Response για Accountants

Το Subject m.white κάνει αίτηση για να διαβάσει (read) τις αποδείξεις του τρέχοντος έτους (/_emedica/ehealth/invoices/2013/Invoice_1.txt). Φαίνεται ότι το Resource συμπληρώνεται ακριβώς με την μορφή που είναι αποθηκευμένο στο σύστημα.
Άρα όταν κάποιος σύμφωνα με το προφίλ του είναι λογιστής και ζητά να διαβάσει δεδομένα που χαρακτηρίζονται και έχουν αποθηκευτεί ως αποδείξεις, τότε το αποτέλεσμα της αίτησης είναι Permit.
Σύμφωνα με τον δεύτερο κανόνα της πολιτικής, όταν πρόκειται για αίτηση για WRITE, πρέπει να ορίζεται ακριβώς η ώρα πρόσβασης και αυτή να είναι μέσα στις δεδομένες ώρες γραφείου και μόνο (07:00-15:00). Στο επόμενη εικόνα (Εικόνα 31) ο χρήστης, του οποίου ο ρόλος είναι λογιστής, m.white κάνει request για να γράψει στο αρχείο των αποδείξεων στις 10:00.



Εικόνα 31. Request_2a/Response για Accountants

Το αποτέλεσμα αυτού του Request είναι Permit, δεδομένου ότι η ώρα που καθορίζεται στο πεδίο Environment Name βρίσκεται μέσα στο χρονικό πλαίσιο όπου επιτρέπεται από την πολιτική ασφάλειας, η πράξη της εγγραφής.
Αν όμως ο χρήστης με ρόλο λογιστή κάνει αίτηση εγγραφής στο resource για παράδειγμα στις 21:00 τότε η απάντηση θα είναι Deny (Εικόνα 32).

Εικόνα 32. Request_2b/Response για Accountants

3.7 Περιγραφή Επιμέρους Πολιτικής - Policy_ITadmins

Η πολιτική για τους χρήστες που κατέχουν ρόλο ITadmin (Διαχειριστής) περιλαμβάνει τους ακόλουθους δύο κανόνες:

- Rule_1: Ο Διαχειριστής δεν επιτρέπεται να διαβάζει και να γράφει στα Ηλεκτρονικά Αρχεία των ασθενών (EHR).

- Rule_2: Ο Διαχειριστής επιτρέπεται να διαβάζει όλα τα log files, που είναι αποθηκευμένα στο σύστημα, και σχετίζονται με προσβάσεις στα EHRs.

3.7.1 Ανάλυση Επιμέρους Πολιτικής - Policy_ITadmins

Το **<Policy>** element που έχει για αναγνωριστικό το xacml attribute **@PolicyId** ίσο με «**Policy_ITadmins**», αναπαριστά την επιμέρους πολιτική που καθορίζει τις προσβάσεις που μπορούν να έχουν οι χρήστες, των οποίων ο ρόλος είναι διαχειριστές του Πληροφοριακού Συστήματος (**ITadmin**). Σημαντικά elements που περιέχονται στο προαναφερόμενο **<Policy>** element είναι τα **<Target>** και **<Rule>** elements.

Στο **<Target>** element χρησιμοποιείται ένα **<Match>** element που συγκρίνει μέσω της συνάρτησης «**string-regexp-match**» την συμβολοσειρά χαρακτήρων «**ITadmin**» με κάθε μια από τις δυνατές επιστρεφόμενες τιμές της σακούλας, που προκύπτει κατά την εφαρμογή του **<AttributeDesignator>** element στο χαρακτηριστικό «**role**» της κατηγορίας «**access-subject**».

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-ITA1**», αναπαριστά τον πρώτο κανόνα της πολιτικής για διαχειριστές Πληροφοριακού Συστήματος.
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι διαχειριστής IT, προσπαθεί να εκτελέσει είτε την ενέργεια **write** είτε την ενέργεια **read** σε κάποιο από τα ιατρικά αρχεία των ασθενών που αποθηκεύονται στο σύστημα ή ισοδύναμα στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» συμπίπτει είτε με την συμβολοσειρά χαρακτήρων **write** είτε με την συμβολοσειρά χαρακτήρων **read**.
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Deny**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».

Στο **<Condition>** element έχει συμπεριληφθεί μία μόνο έκφραση, η οποία θα πρέπει να δίνει την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**». Στην έκφραση αυτή συγκρίνεται μέσω της συνάρτησης «**string-regexp-match**» το χαρακτηριστικό «**resource-id**» της κατηγορίας «**resource**» με την συμβολοσειρά χαρακτήρων «**/_emedica/ehealth/patients/**», το οποίο παριστάνει την διαδρομή του φακέλου, εσωτερικά του οποίου αποθηκεύονται όλα τα ιατρικά αρχεία των ασθενών. Συνεπώς, δεν επιτρέπεται στους διαχειριστές IT να έχουν πρόσβαση εσωτερικά των ατομικών φακέλων των ασθενών.

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-ITA2**», αναπαριστά τον δεύτερο κανόνα της πολιτικής για τους διαχειριστές του Πληροφοριακού Συστήματος.

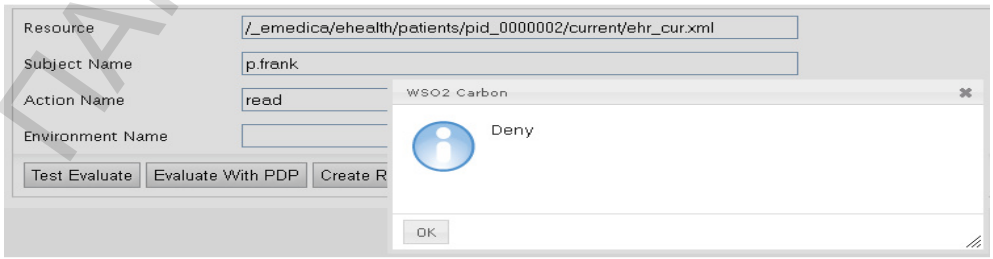
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι διαχειριστής IT, προσπαθεί να εκτελέσει την ενέργεια **read** σε κάποιο από τα log αρχεία του συστήματος. Συνεπώς, στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» συγκρίνεται με την συμβολοσειρά χαρακτήρων **read**.
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».

Στο **<Condition>** element έχει συμπεριληφθεί μία μόνο έκφραση, η οποία θα πρέπει να δίνει την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**». Στην έκφραση αυτή συγκρίνεται μέσω της συνάρτησης «**string-regexp-match**» το χαρακτηριστικό «**resource-id**» της κατηγορίας «**resource**» με την συμβολοσειρά χαρακτήρων «**/audit/**», το οποίο παριστάνει μέρος της διαδρομής των φακέλων, εσωτερικά των οποίων αποθηκεύονται τα log αρχεία και τα οποία δημιουργούνται κατά την εκτέλεση κάποιας ενέργειας στους πόρους του συστήματος. Σημειώνεται ότι, για κάποιον ασθενή τα log αρχεία (π.χ. ehr_2013_04_10.log) αποθηκεύονται εντός συγκεκριμένου υπο-φακέλου, «**audit**», σε ξεχωριστό μονοπάτι για κάθε ασθενή π.χ. για τον ασθενή με patient_id="0000001" έχουμε «**/_emedica/ehealth/patients/pid_0000001/**».

Στους ανωτέρω δύο κανόνες παρατηρούμε μια διένεξη αποφάσεων, η οποία προκύπτει όταν ο διαχειριστής IT προσπαθεί να κάνει read σε ένα log αρχείο. Επειδή, τα αρχεία αυτού του είδους βρίσκονται εσωτερικά υπο-φακέλων σε προσωπικό χώρο αποθήκευσης των ασθενών, ο πρώτος κανόνας καταλήγει σε απόφαση «**Deny**». Η διένεξη αυτή επιλύεται με τελική απόφαση της πολιτικής να επικρατεί το «**Permit**», λόγω του ότι έχει χρησιμοποιηθεί στην πολιτική ο αλγόριθμος συνδυασμού κανόνων «**deny-unless-permit**», ο οποίος δίνει πάντα προτεραιότητα στις θετικές αποφάσεις.

3.7.2 Αξιολόγηση και Επαλήθευση Επιμέρους Πολιτικής - Policy_ITadmins

Για την αξιολόγηση του πρώτου κανόνα της πολιτικής, έστω ότι ο χρήστης με ρόλο «διαχειριστής», p.frank, προσπαθεί να αποκτήσει πρόσβαση (read) στο EHR της ασθενούς s.molder. Το σύστημα εκτιμώντας της πολιτική ασφάλειας για ITadmins θα δώσει ως Response Deny (εικόνα 33).



Εικόνα 33. Request_1 για ITadmins

Με βάση τώρα τον δεύτερο κανόνα, εάν ο διαχειριστής κάνει αίτηση να διαβάσει log files που κρατά το σύστημα από «ενέργειες» που γίνονται , για παράδειγμα στον φάκελο του ασθενούς g.smith (pid_0000001), τότε το αποτέλεσμα θα είναι φυσικά Permit (Εικόνα 34).

Εικόνα 34. Request_2 για ITadmins

3.8 Περιγραφή Επιμέρους Πολιτικής - Policy_Insurers

Η πολιτική που αφορά τους χρήστες με ρόλο Insurer (Ασφαλιστικός φορέας), περιέχει τον ακόλουθο κανόνα:

- Rule_1: Ο ασφαλιστικός φορέας μπορεί να διαβάσει το στοιχείο <ChargeInfo> και όλα τα υπο-στοιχεία του, δεδομένου ότι είναι ο ίδιος φορέας που αναφέρεται στο EHR του ασθενούς

3.8.1 Ανάλυση Επιμέρους Πολιτικής - Policy_Insurers

Το **<Policy>** element που έχει για αναγνωριστικό το xacml attribute **@PolicyId** ίσο με «**Policy_Insurers**», αναπαριστά την επιμέρους πολιτική που καθορίζει τις προσβάσεις που μπορούν να έχουν οι χρήστες, των οποίων ο ρόλος είναι ασφαλιστικός εκπρόσωπος (**Insurer**). Σημαντικά elements που περιέχονται στο προαναφερόμενο **<Policy>** element είναι τα **<Target>** και **<Rule>** elements.

Στο **<Target>** element χρησιμοποιείται ένα **<Match>** element που συγκρίνει μέσω της συνάρτησης «**string-regexp-match**» την συμβολοσειρά χαρακτήρων «**Insurer**» με κάθε μια από τις δυνατές επιστρεφόμενες τιμές της σακούλας, που προκύπτει κατά την εφαρμογή του **<AttributeDesignator>** element στο χαρακτηριστικό «**role**» της κατηγορίας «**access-subject**».

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-INS1**», αναπαριστά τον μοναδικό κανόνα της πολιτικής για χρήστες που εκπροσωπούν τους ασφαλιστικούς φορείς.
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι ασφαλιστικός εκπρόσωπος, προσπαθεί να εκτελέσει την ενέργεια **read** σε συγκεκριμένα υπο-στοιχεία εσωτερικά των ιατρικών αρχείων των

ασθενών που αποθηκεύονται στο σύστημα. Πιο αναλυτικά, ένας χρήστης με ρόλο ασφαλιστή θα πρέπει να έχει πρόσβαση στο element **<ChargeInfo>** καθώς και στα εσωτερικά του sub-elements **<RoomType>**, **<RoomNum>** και **<ChargeValue>**, μόνος όμως στην περίπτωση που ο ασθενής διαθέτει ασφάλιση στον αντίστοιχο ασφαλιστικό φορέα. Για την υλοποίηση της ανωτέρω συνθήκης εισάγουμε εσωτερικά του **<Target>** element δύο **<AnyOf>** elements. Στο πρώτο, συγκρίνεται μέσω του **<Match>** element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» με την συμβολοσειρά χαρακτήρων **read**. Στο δεύτερο **<AnyOf>** element έχει συμπεριληφθεί ένα σύνολο από **<AllOf>** elements, τα οποία συνδέονται με μια λογική έκφραση τύπου OR. Συνεπώς, η ολική έκφραση γίνεται αληθής εάν το χαρακτηριστικό «**resource-name**» της κατηγορίας «**resource**» συμπίπτει με οποιαδήποτε από τις συμβολοσειρές χαρακτήρων:

- **ChargeInfo ή**
- **RoomType ή**
- **RoomNum ή**
- **ChargeValue**

Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».
Στο **<Condition>** element έχουν συμπεριληφθεί δύο υπο-εκφράσεις, οι οποίες θα πρέπει να δίνουν και οι δύο την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**».

➢ 1η συνθήκη

Το όνομα του χρήστη που εκπροσωπεί τον ασφαλιστικό φορέα θα πρέπει να συμπίπτει με αυτό που περιέχεται εσωτερικά του element **<InsuranceProvider>**, στο EHR του ασθενούς. Συνεπώς, θα πρέπει το χαρακτηριστικό «**subject-id**» του χρήστη κατηγορίας «**access-subject**» να συμπίπτει (συνάρτηση «**string-equal**») με οποιαδήποτε από τις τιμές που περιέχονται στη σακούλα τιμών, η οποία προκύπτει από την εφαρμογή του element **<AttributeSelector>** στα περιεχόμενα στοιχεία του πόρου EHR, σύμφωνα με την XPath έκφραση:

@Path= "//xacml:**ehealthrec**/xacml:**ChargeInfo**/xacml:**InsuranceProvider**/text()"

➢ 2η συνθήκη

Ο πόρος του συστήματος, το υπο-στοιχείο του οποίου ζητείται να διαβαστεί από τον χρήστη (Ηλεκτρονικό Αρχείο Υγείας ασθενούς - EHR) θα πρέπει να ακολουθεί το μοτίβο τόσο για το όνομα όσο και για το πλήρες μονοπάτι που έχει προκαθοριστεί για τους ασθενείς στο Πληροφοριακό Σύστημα **E-MEDICA**:

Μονοπάτι ⇔ /_emedica/ehealth/patients/pid_[επταψήφιος αριθμός]/current/

Όνομα πόρου ⇔ ehr_cur.xml

3.8.2 Αξιολόγηση και Επαλήθευση Επιμέρους Πολιτικής - Policy_Insurers

Έστω, για το συγκεκριμένο Request, ο χρήστης με ρόλο «ασφαλιστικός φορέας», tsmede, κάνει αίτηση για ανάγνωση του sub-element "RoomNum" από το element «ChargeInfo» που βρίσκεται μέσα στο EHR του ασθενή με pid_0000001. Με άλλα λόγια το ΤΣΜΕΔΕ θέλει να διαβάσει τον αριθμό δωματίου που χρεώθηκε στον ασθενή g.smith. Η πολιτική επαληθεύει ότι αυτό είναι επιτρεπτό, συγκρίνοντας την τιμή του element <InsuranceProvider> με το όνομα του χρήστη (ρόλος Insurer) που έκανε το Request. Στην συγκεκριμένη περίπτωση αυτά συμπίπτουν, οπότε το αποτέλεσμα θα είναι Permit (Εικόνα 35).

Request_Insurer.xml

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<!--Action Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
</Attribute>
</Attributes>
<!--Subject Category-->
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">tsmede</AttributeValue>
</Attribute>
</Attributes>
<!--Resource Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Content>
<ehealthrec id="24023203132">
</Content>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
/_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml</AttributeValue>
</Attribute>
<Attribute AttributeId="http://wso2.org/my_attributes/resource-name" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">RoomNum</AttributeValue>
</Attribute>
</Attributes>
<!-- -->
</Request>
```

```
<Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
<Result>
<Decision>Permit</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

Εικόνα 35. Request/Response για Insurers

Αν τώρα, ο χρήστης που ζητά πρόσβαση στο συγκεκριμένο EHR, αλλάξει από tsmede σε ika, όπως αναμένεται θα πάρει απάντηση Deny, όπως φαίνεται στην επόμενη εικόνα (Εικόνα 36).

Request_Insurer.xml

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<!--Action Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
</Attribute>
</Attributes>
<!--Subject Category-->
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ika</AttributeValue>
</Attribute>
</Attributes>
<!--Resource Category-->
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Content>
<ehealthrec id="24023203132">
</Content>
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml</AttributeValue>
</Attribute>
<Attribute AttributeId="http:://wso2.org/my_attributes/resource-name" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">RoomNum</AttributeValue>
</Attribute>
</Attributes>
<!-- -->
</Request>
                    <Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
<Result>
<Decision>Deny</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

Εικόνα 36. Request/Response για Insurers (Deny)

3.9 Περιγραφή Επιμέρους Πολιτικής - Policy_Secretaries

Η πολιτική που σχετίζεται με τον έλεγχο πρόσβασης χρηστών με ρόλο Secretary (Γραμματείς), δομείται από τους παρακάτω δύο κανόνες:

- Rule_1: Η γραμματέας μπορεί να δημιουργήσει ένα νέο EHR.
- Rule_2: Η γραμματέας έχει την δυνατότητα να διαβάσει και να γράψει μόνο στα στοιχεία <Person> και <ChargeInfo> από το EHR.

3.9.1 Ανάλυση Επιμέρους Πολιτικής - Policy_Secretaries

Το **<Policy>** element που έχει για αναγνωριστικό το xacml attribute **@PolicyId** ίσο με «**Policy_Secretaries**», αναπαριστά την επιμέρους πολιτική που καθορίζει τις προσβάσεις που μπορούν να έχουν οι χρήστες, των οποίων ο ρόλος είναι γραμματείς (**Secretary**). Σημαντικά elements που περιέχονται στο προαναφερόμενο **<Policy>** element είναι τα **<Target>** και **<Rule>** elements.

Στο **<Target>** element χρησιμοποιείται ένα **<Match>** element που συγκρίνει μέσω της συνάρτησης «**string-regexp-match**» την συμβολοσειρά χαρακτήρων «**Secretary**» με κάθε μια από τις δυνατές επιστρεφόμενες τιμές της σακούλας, που προκύπτει κατά την εφαρμογή του **<AttributeDesignator>** element στο χαρακτηριστικό «**role**» της κατηγορίας «**access-subject**».

Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-SEC1**», αναπαριστά τον πρώτο κανόνα της πολιτικής για γραμματείς.
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι γραμματέας, προσπαθεί να εκτελέσει την ενέργεια **create** για την δημιουργία ενός νέου ιατρικού αρχείου για κάποιον ασθενή. Ισοδύναμα, στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» θα πρέπει να συμπίπτει με την συμβολοσειρά χαρακτήρων **create**.
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».

Στο **<Condition>** element έχει συμπεριληφθεί μια μόνο έκφραση, η οποία θα πρέπει να δίνει την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**».

- Συνθήκη

Ο πόρος του συστήματος που ζητείται να δημιουργηθεί από τον χρήστη (Ηλεκτρονικό Αρχείο Υγείας ασθενούς - EHR) θα πρέπει να ακολουθεί το μοτίβο τόσο για το όνομα όσο και για το πλήρες μονοπάτι που έχει προκαθοριστεί για τους ασθενείς στο Πληροφοριακό Σύστημα **E-MEDICA**:

Μονοπάτι ⇔ /_emedica/ehealth/patients/pid_[επταψήφιος αριθμός]/current/

Όνομα πόρου ⇔ ehr_cur.xml

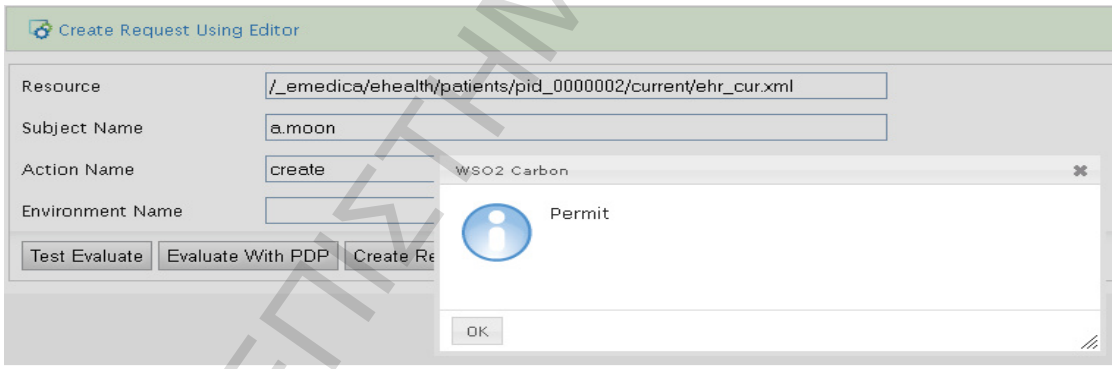
Το **<Rule>** element που έχει σαν αναγνωριστικό το xacml attribute **@RuleId** ίσο με «**Rule-SEC2**», αναπαριστά τον δεύτερο κανόνα της πολιτικής για γραμματείς.
Ο ανωτέρω κανόνας εφαρμόζεται για τα αιτήματα πρόσβασης, όπου ο χρήστης «**access-subject**», του οποίου ο ρόλος είναι γραμματέας, προσπαθεί να εκτελέσει την ενέργεια **read** ή την ενέργεια **write** σε συγκεκριμένα υπο-στοιχεία ενός ιατρικού αρχείου ασθενούς. Ισοδύναμα, στο **<Target>** element το χαρακτηριστικό «**action-id**» της κατηγορίας «**action**» θα πρέπει να συμπίπτει με την συμβολοσειρά χαρακτήρων **read** ή **write**. Επιπρόσθετα, το το υπο-στοιχείο εσωτερικά του EHR, που αιτείται να διαβάσει ο γραμματέας θα πρέπει να

είναι διάφορο του **<MedicalRec>** element. Συνεπώς, ο γραμματέας μπορεί να έχει πρόσβαση μόνο στα **<Person>** και **<ChargeInfo>** elements του EHR, ή ισοδύναμα το χαρακτηριστικό «**resource-name**» της κατηγορίας «**resource**» συμπίπτει με κάποια από τις συμβολοσειρές χαρακτήρων «**Person**» ή «**ChargeInfo**».
Σύμφωνα με το xacml attribute **@Effect**, ο κανόνας καταλήγει στην απόφαση «**Permit**», όταν ο υπολογισμός των **<Target>** και **<Condition>** elements καταλήγει σε αληθείς εκφράσεις, δηλ. το **<Target>** σε «**Match**» και το **<Condition>** σε «**True**».

Στο **<Condition>** element έχει συμπεριληφθεί μια μόνο έκφραση, η οποία θα πρέπει να δίνει την τιμή «**True**», για να υπολογίζεται το **<Condition>** element σε «**True**». Η έκφραση που έχει χρησιμοποιηθεί στον δεύτερο κανόνα είναι ακριβώς ίδια με αυτήν του πρώτου κανόνα της πολιτικής.

3.9.2 Αξιολόγηση και Επαλήθευση Επιμέρους Πολιτικής - Policy_Secretaries

Για την επαλήθευση του πρώτου κανόνα (Εικόνα 37) που αφορά την δημιουργία ενός νέου EHR από τον χρήστη με ρόλο “secretary”, έστω ότι ο χρήστης με ρόλο “secretary” αιτείται δημιουργίας ενός νέου ηλεκτρονικού αρχείου υγείας EHR για τον χρήστη-ασθενή s.molder (pid_0000002). Το Response σε αυτό το Request αναμένεται να είναι Permit.



Εικόνα 37. Request_1 για Secretaries

Όσον αφορά τον δεύτερο κανόνα, ο χρήστης με ρόλο “secretary” (a.moon), ζητά να κάνει ενημέρωση (write) στο sub-element <Person> του EHR του χρήστη-ασθενή με pid_0000001 (g.smith). Το αποτέλεσμα του Request θα είναι Permit, όπως φαίνεται στην ακόλουθη εικόνα (Εικόνα 38).

Request_Secretaries.xml

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">a.moon</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml</AttributeValue>
</Attribute>
<Attribute AttributeId="http:://wso2.org/my_attributes/resource-name" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Person</AttributeValue>
</Attribute>
</Attributes>
</Request>
                    <Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
<Result>
<Decision>Permit</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

Εικόνα 38. Request_2a/Response για Secretaries

Εάν όμως ο χρήστης με ρόλο “secretary” προσπαθήσει να γράψει για παράδειγμα μέσα σε element διαφορετικό των <ChargeInfo> και <Person>, για παράδειγμα στο <MedicalRec>, τότε το Response θα είναι Deny (εικόνα 39).

Request_Secretaries.xml

```
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" CombinedDecision="false" ReturnPolicyIdList="false">
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">a.moon</AttributeValue>
</Attribute>
</Attributes>
<Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
<Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                    /_emedica/ehealth/patients/pid_0000001/current/ehr_cur.xml</AttributeValue>
</Attribute>
<Attribute AttributeId="http:://wso2.org/my_attributes/resource-name" IncludeInResult="false">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">MedicalRec</AttributeValue>
</Attribute>
</Attributes>
</Request>
                    <Response xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
<Result>
<Decision>Deny</Decision>
<Status>
<StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok"/>
</Status>
</Result>
</Response>
```

Εικόνα 39. Request_2b/Response για Secretaries

4. Αξιολόγηση του XACML προτύπου

Στην περιοχή του ελέγχου πρόσβασης (Authorization) υπάρχουν πολλά πλεονεκτήματα από την υιοθέτηση του προτύπου XACML, τα οποία αναλύονται ακολούθως:

- Η γλώσσα XACML είναι μια πρότυπη (standard) γλώσσα έκφρασης πολιτικών ασφάλειας για πληροφοριακά συστήματα. Αυτό σημαίνει ότι έχει εξεταστεί και τεκμηριωθεί από μια μεγάλη κοινότητα ειδικών σε θέματα ασφάλειας πληροφοριακών συστημάτων, καθώς και χρησιμοποιηθεί από απλούς χρήστες. Συνεπώς, δεν χρειάζεται να αναπτυχθεί κάποια νέα γλώσσα από τον χρήστη για την υλοποίηση κάποιας πολιτικής ασφάλειας, η οποία μπορεί να οδηγήσει σε σφάλματα υπολογισμού.
- Είναι γενική και μπορεί να εφαρμοστεί σε οποιοδήποτε Πληροφοριακό Σύστημα, ανεξαρτήτως της φύσεως του και των ειδικών απαιτήσεων που θέτει στην πολιτική ασφαλείας (π.χ. Πληροφοριακό Σύστημα Υγείας).
- Είναι μια πλούσια γλώσσα που υποστηρίζει την κατασκευή σύνθετων εκφράσεων, καθότι περιλαμβάνει μια μεγάλη ποικιλία από τύπους δεδομένων, συναρτήσεις και αλγόριθμους συνδυασμού κανόνων και πολιτικών. Επιπλέον, εισάγει και την έννοια των υποχρεωτικών ενεργειών (**Obligations**) που θα πρέπει να πραγματοποιηθούν κατά την διαδικασία υπολογισμού των αποφάσεων των πολιτικών.
- Μέσω της γλώσσας XACML έχουμε την δυνατότητα καθορισμού κανόνων ασφάλειας στο επίπεδο του αντικειμένου. Ο έλεγχος πρόσβασης αυτού του τύπου αναφέρεται και ως «**fine-grained**», για να δείξει την λεπτομέρεια της επεξεργασίας κατά την απόφαση των πολιτικών. Συνεπώς, επιτυγχάνεται πληρέστερος έλεγχος κατά την πρόσβαση και υπάρχει μεγαλύτερη δυνατότητα για διαμοίραση των πόρων-πληροφοριών του συστήματος.
- Η γλώσσα XACML προωθεί το δυναμικό Attribute Based Access Control (**ABAC**) μοντέλο, το οποίο ξεπερνά τις δυνατότητες του στατικού μοντέλου **RBAC**. Συνεπώς, μια απόφαση εξουσιοδότησης είναι δυνατόν να βασίζεται στο σύνολο των χαρακτηριστικών της οντότητας που αιτείται της πρόσβασης (**subject**) και όχι μόνο στον ρόλο του, σε χαρακτηριστικά του πόρου (**resource**) καθώς και στο περιεχόμενό του (**content**), σε χαρακτηριστικά της ενέργειας (**action**) και τέλος σε ανεξάρτητα χαρακτηριστικά σχετικά με το περιβάλλον (**environment**), όπως ο τόπος και ο χρόνος.
- Ένα άλλο πλεονέκτημα της γλώσσας XACML είναι ότι στηρίζεται σε πολιτικές (policy-based), συνεπώς προτιμάται στα συστήματα όπου υπάρχει απαίτηση για παροχή στοιχείων συμμόρφωσης της υλοποιηθείσας πολιτικής ασφάλειας ως προς την θεωρητικά εφαρμοζόμενη. Επίσης, είναι εύκολα προσαρμόσιμη σε αιτούμενες αλλαγές κανόνων της πολιτικής ασφάλειας.
- Πρέπει επίσης να σημειωθεί ότι το πρότυπο XACML προσφέρει μια εξωτερικευμένη (**externalized**) λύση στο θέμα του ελέγχου πρόσβασης, με το PDP να προσφέρει την λειτουργία αυτή ως υπηρεσία (service) στο Πληροφοριακό Σύστημα. Συνεπώς, το Πληροφοριακό Σύστημα δεν διαθέτει κώδικα στην εφαρμογή για υπολογισμό

αποφάσεων, αντί αυτού μέσω του τοπικού του PEP ρωτά το PDP για κάθε αίτημα πρόσβασης.

- Τέλος, η γλώσσα XACML είναι επεκτάσιμη καθόσον αρκετά από τα XML στοιχεία που περιέχει είναι URIs και επιτρέπουν την δημιουργία καινούργιων τύπων δεδομένων, συναρτήσεων και αλγορίθμων συνδυασμού κανόνων. Επιπρόσθετα, αναπτύσσονται πολλά XACML Profiles για την επέκταση της λειτουργικότητας της γλώσσας καθώς και την συνεργασία της με άλλα πρότυπα, όπως το πρότυπο SAML.

ΠΑΡΑΡΤΗΜΑ

```
<PolicySet xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:permit-overrides" PolicySetId="EMEDICA_POLICYSET" Version="1.0">
    <Description>The EMEDICA Clinic overall security policy set</Description>
    <Target>
        <AnyOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patient</AttributeValue>
                <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
                </Match>
            </AllOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Guardian</AttributeValue>
                <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
                </Match>
            </AllOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">CarePhysician</AttributeValue>
                <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
```

```
        </Match>
 </AllOf>

<AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Nurse</AttributeValue>
        <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
         </Match>
</AllOf>
<AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Secretary</AttributeValue>
        <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
        </Match>
</AllOf>
<AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ITadmin</AttributeValue>
        <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
        </Match>
</AllOf>
<AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Accountant</AttributeValue>
```

```
                <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
                </Match>

            </AllOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Radiologist</AttributeValue>
                <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
                </Match>
            </AllOf>
            <AllOf>
                <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Insurer</AttributeValue>
                <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
                </Match>
            </AllOf>
        </AnyOf>
</Target>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="Policy_Patients"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">
        <Description>Patients are granted access to their EHRs without restrictions.</Description>
        <Target>
            <AnyOf>
                <AllOf>
```

```
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patient</AttributeValue>
            <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
           </Match>
        </AllOf>
    </AnyOf>
</Target>
<Rule Effect="Permit" RuleId="Rule-PAT1">
<Description>Patients shall be able to read their EHRs, identified by the patients ID included in patient URL attribute.</Description>
<Target>
    <AnyOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                    category:action" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
        </AllOf>
    </AnyOf>
</Target>
<Condition>
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
    <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
        <AttributeDesignator AttributeId="http://wso2.org/claims/url" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
```

```
    </Apply>
    <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
    </Apply>

 </Condition>
 </Rule>
<Rule Effect="Permit" RuleId="Rule-PAT2">
 <Description>Patients shall be able to update their EHRs, identified by the patients ID included in patient URL attribute, only from a local position in
                EMEDICA Clinic.</Description>
<Target>
<AnyOf>
      <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
          <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                    category:action" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
          </Match>
      </AllOf>
 </AnyOf>
 </Target>
 <Condition>
     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
    <!--1ST Condition: Patients URL shall regular expression match with Resource-id -->
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
        <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
```

```
                <AttributeDesignator AttributeId="http://wso2.org/claims/url" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
                </Apply>
              <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Apply>
            <!--2ND Condition: IP of Patient shall be local, in the range 192.168.1.1 to 192.168.1.255 -->
            <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:ipAddress-regexp-match">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">192.168.1.</AttributeValue>
                <Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:ipAddress-from-string">
                 <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
                  <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:environment" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
                 </Apply>
                </Apply>
               </Apply>
              </Apply>
          </Condition>
          </Rule>
</Policy>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="Policy_Guardians"
          RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">
         <Description>A Parent or Guardian may read any element in an EHR record that belongs to his guarded member, provided that it's under 16 years
                    old.</Description>
         <Target>
           <AnyOf>
              <AllOf>
```

```
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Guardian</AttributeValue>
            <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>

       </AllOf>
   </AnyOf>
 </Target>
<Rule Effect="Permit" RuleId="Rule-PAR1">
<Target>
   <AnyOf>
     <AllOf>
         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
         <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                  category:action" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
         </Match>
     </AllOf>
     <AllOf>
         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
         <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                  category:action" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
         </Match>
     </AllOf>
   </AnyOf>
```

```
    <AnyOf>
      <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Patient</AttributeValue>
          <AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject" AttributeId="http://wso2.org/claims/role"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>

          </Match>
      </AllOf>
    </AnyOf>
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
<!-- 1ST Condition: The URL of the recipient subject(patient) matches with resource-id -->
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
    <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
        <AttributeDesignator AttributeId="http://wso2.org/claims/url" Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject"
                              DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
         </Apply>
         <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                    category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
    </Apply>
 <!-- 2ND Condition: The TITLE attribute in profile of access-subject (guardianof_patient) matches with concatenation of string guardianof and recipient_id
      (patient)-->
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
    <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"></Function>
```

```
        <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:string-concatenate">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">guardianof_</AttributeValue>
             <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
             <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:recipient-id" Category="urn:oasis:names:tc:xacml:1.0:subject-
                category:recipient-subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
             </Apply>
        </Apply>
        <AttributeDesignator AttributeId="http://wso2.org/claims/title" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
    </Apply>
<!-- 3RD Condition: Recipient subject (patient) must be under 16 years old -->
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-greater-than-or-equal">
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-add">
        <Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:integer-from-string">
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
          <AttributeDesignator AttributeId="http://wso2.org/claims/dob" Category="urn:oasis:names:tc:xacml:1.0:subject-category:recipient-subject"
                                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
           </Apply>
        </Apply>
         AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">16</AttributeValue>
       </Apply>
      <Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:integer-from-string">
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
         <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                    category:environment" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
        </Apply>
       </Apply>
```

```
            </Apply>
          </Apply>
        </Condition>
        </Rule>
</Policy>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" xmlns:xacml="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="Policy_Physicians"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">
 <Description>In general a Care Physician may read/write a patient's EHR, provided that he is the designated Physician.</Description>
 <PolicyDefaults>
    <XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</XPathVersion>
 </PolicyDefaults>
 <Target>
     <AnyOf>
         <AllOf>
             <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">CarePhysician</AttributeValue>
             <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                 DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
             </Match>
         </AllOf>
         <AllOf>
             <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Radiologist</AttributeValue>
             <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                 DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
         </AllOf>
```

```
      </AnyOf>
 </Target>
 <Rule Effect="Permit" RuleId="Rule-PHY1">
 <Description>A Care Physician shall be able to read the patient's -MedicalRec- element of EHR, provided that he is the designated Physician.</Description>
 <Target>
   <AnyOf>
     <AllOf>
         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
         <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                              DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
          </Match>
       </AllOf>
    </AnyOf>
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
<!--1ST Condition: Care Physician's SSN_ID (claim = im), matches that in the Content of EHR-->
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of-any">
     <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"></Function>
     <AttributeDesignator MustBePresent="false" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                          AttributeId="http://wso2.org/claims/im" DataType="http://www.w3.org/2001/XMLSchema#string"/>
     <AttributeSelector MustBePresent="true" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        Path="//xacml:ehealthrec/xacml:Person[@Role='CarePhysician']/xacml:PersonalData/xacml:SSN_ID/text()"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
     </Apply>
 <!--2ND Condition: Resource's name and path shall regular expression match with an expected's EHR name and path. -->
```

```
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
      <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/pid_[0-9]{7}/current/ehr_cur.xml</AttributeValue>
      <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                           DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
      </Apply>

<!--3RD Condition: The node element from resource requested shall be MedicalRec element-->
     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
     <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">MedicalRec</AttributeValue>
     <AttributeDesignator AttributeId="http:://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                          DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
      </Apply>
</Apply>
</Condition>
</Rule>
<Rule Effect="Permit" RuleId="Rule-PHY2">
<Description>A Care Physician shall be able to write his designated patient -MedicalRec- element of EHR, provided that an email is sent to patient.</Description>
<Target>
   <AnyOf>
     <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
        <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                             DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
        </Match>
```

```
        </AllOf>
    </AnyOf>
</Target>
<Condition>
 <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
<!--1ST Condition: Care Physician's SSN_ID (claim = im), matches that in the Content of EHR-->

   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of-any">
   <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"></Function>
   <AttributeDesignator MustBePresent="false" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                              AttributeId="http://wso2.org/claims/im" DataType="http://www.w3.org/2001/XMLSchema#string"/>
   <AttributeSelector MustBePresent="true" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                         Path="//xacml:ehealthrec/xacml:Person[@Role='CarePhysician']/xacml:PersonalData/xacml:SSN_ID/text()"
                         DataType="http://www.w3.org/2001/XMLSchema#string"/>
   </Apply>
<!--2ND Condition: Resource's name and path shall regular expression match with an expected's EHR name and path. -->
   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
   <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/pid_[0-9]{7}/current/ehr_cur.xml</AttributeValue>
   <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                              DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
   </Apply>
<!--3RD Condition: The node element from resource requested shall be MedicalRec element-->
   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
   <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"></Function>
   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">MedicalRec</AttributeValue>
   <AttributeDesignator AttributeId="http:://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
```

```
                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
   </Apply>
 </Apply>
</Condition>
<ObligationExpressions>
    <ObligationExpression ObligationId="EMAIL-TO-PATIENT" FulfillOn="Permit">
        <AttributeAssignmentExpression AttributeId="obligation-attribute:mailto">
         <AttributeSelector MustBePresent="true" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        Path="//xacml:ehealthrec/xacml:Person[@Role='Patient']/xacml:ContactInfo/xacml:Email/text()"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </AttributeAssignmentExpression>
         <AttributeAssignmentExpression AttributeId="obligation-attribute:note">
         <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:string-concatenate">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Your Medical Record has been updated by Care Physician:</AttributeValue>
            <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
                        subject" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Apply>
         </Apply>
         </AttributeAssignmentExpression>
     </ObligationExpression>
</ObligationExpressions>
</Rule>
<Rule Effect="Permit" RuleId="Rule-RAD1">
<Description>A CarePhysician shall be able to read all xrays of patients, provided that he is also a Radiologist and his email belongs to emedica
            domain.</Description>
<Target>
```

```
    <AnyOf>
      <AllOf>
        <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
        <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                             DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
        </Match>
       <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Radiologist</AttributeValue>
       <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                            DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
       </Match>
      </AllOf>
   </AnyOf>
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
<!--1ST Condition: Resource's name and path shall regular expression match with an expected xray name and path. -->
     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
     <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
     <AttributeValue  DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/pid_[0-9]{7}/current/xray_[0-9]{8}.jpg
     </AttributeValue>
     <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                          DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
     </Apply>
<!--2ND Condition: Radiologists email shall belong to EMEDICA domain. -->
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:rfc822Name-match">
```

```
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">emedica.gr</AttributeValue>
      <Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:rfc822Name-from-string">
         <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
         <AttributeDesignator AttributeId="http://wso2.org/claims/emailaddress" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
         </Apply>
      </Apply>
     </Apply>
  </Apply>
</Condition>
</Rule>
</Policy>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" xmlns:xacml="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="Policy_Nurses"
          RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">
<Description>In general a Nurse has only access rights for the -Result- element of a patient's EHR.</Description>
<PolicyDefaults>
   <XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</XPathVersion>
</PolicyDefaults>
<Target>
    <AnyOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Nurse</AttributeValue>
            <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
         </AllOf>
```

```
  </AnyOf>
 </Target>
 <Rule Effect="Permit" RuleId="Rule-NUR1">
 <Description>A Nurse shall be able to read the patient's -Result- element of EHR, provided that she is the designated Nurse.</Description>
 <Target>
    <AnyOf>
       <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
          <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
          </Match>
       </AllOf>
      </AnyOf>
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
<!--1ST Condition: Nurse's SSN_ID (claim = im), matches that in the Content of EHR-->
     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of-any">
     <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"></Function>
     <AttributeDesignator MustBePresent="false" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                          AttributeId="http://wso2.org/claims/im" DataType="http://www.w3.org/2001/XMLSchema#string"/>
     <AttributeSelector MustBePresent="true" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        Path="//xacml:ehealthrec/xacml:MedicalRec/xacml:Treatment/xacml:Result/xacml:PerformedBy/text()"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
     </Apply>
 <!--2ND Condition: Resource's name and path shall regular expression match with an expected's EHR name and path. -->
```

```
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
    <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/pid_[0-9]{7}/current/ehr_cur.xml</AttributeValue>
    <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                         DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
    </Apply>

<!--3RD Condition: The node element from resource requested shall be Result element-->
   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
   <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Result</AttributeValue>
   <AttributeDesignator AttributeId="http::://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
    </Apply>
  </Apply>
</Condition>
</Rule>
<Rule Effect="Permit" RuleId="Rule-NUR2">
<Description>A Nurse shall be able to create a -Result- element for any patients EHR.</Description>
 <Target>
    <AnyOf>
       <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">create</AttributeValue>
          <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                               DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
          </Match>
```

```
        </AllOf>
    </AnyOf>
  </Target>
  <Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
<!--1ST Condition: Resource's name and path shall regular expression match with an expected's EHR name and path. -->
     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
     <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/pid_[0-9]{7}/current/ehr_cur.xml</AttributeValue>
     <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                              DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
     </Apply>
<!--2ND Condition: The node element from resource requested shall be Result element-->
     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
     <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Result</AttributeValue>
     <AttributeDesignator AttributeId="http:://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                              DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
      </Apply>
 </Apply>
</Condition>
</Rule>
<Rule Effect="Permit" RuleId="Rule-NUR3">
<Description>A Nurse can only update the -Notes- element of an existing -Result- element from an EHR, provides that she is the creator of
                element.</Description>
<Target>
   <AnyOf>
```

```
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
           <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">NurseNotes</AttributeValue>
           <AttributeDesignator AttributeId="http::://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                                        category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
            </Match>
        </AllOf>
    </AnyOf>
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
<!--1ST Condition: Nurse's SSN_ID (claim = im), matches that in the Content of EHR-->
     <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of-any">
     <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"></Function>
    <AttributeDesignator MustBePresent="false" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                            AttributeId="http://wso2.org/claims/im" DataType="http://www.w3.org/2001/XMLSchema#string"/>
    <AttributeSelector MustBePresent="true" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        Path="//xacml:ehealthrec/xacml:MedicalRec/xacml:Treatment/xacml:Result/xacml:PerformedBy/text()"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Apply>
 <!--2ND Condition: Resource's name and path shall regular expression match with an expected's EHR name and path. -->
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
```

```
    <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/pid_[0-9]{7}/current/ehr_cur.xml</AttributeValue>
    <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                         DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
    </Apply>
   </Apply>
</Condition>
</Rule>
<Rule Effect="Deny" RuleId="Rule-NUR4">
<Description>A Nurse can only update the -Notes- element of an existing -Result- element from an EHR, and not the other subelements, otherwise an advice is
             given.</Description>
<Target>
    <AnyOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                                 DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
         </AllOf>
    </AnyOf>
    <AnyOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">TestType</AttributeValue>
            <AttributeDesignator AttributeId="http::://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                                 category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
```

```
            </Match>
          </AllOf>
          <AllOf>
              <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Value</AttributeValue>
              <AttributeDesignator AttributeId="http:://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                                          category:resource"  DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
              </Match>
           </AllOf>
           <AllOf>
              <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">PerformedDate</AttributeValue>
              <AttributeDesignator AttributeId="http:://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                                          category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
              </Match>
           </AllOf>
           <AllOf>
              <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">PerformedBy</AttributeValue>
              <AttributeDesignator AttributeId="http:://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                                          category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
               </Match>
          </AllOf>
      </AnyOf>
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
```

```
<!--1ST Condition: Nurse's SSN_ID (claim = im), matches that in the Content of EHR-->
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of-any">
    <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"></Function>
    <AttributeDesignator MustBePresent="false" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="http://wso2.org/claims/im" DataType="http://www.w3.org/2001/XMLSchema#string"/>
     <AttributeSelector MustBePresent="true" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        Path="//xacml:ehealthrec/xacml:MedicalRec/xacml:Treatment/xacml:Result/xacml:PerformedBy/text()"
                        DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Apply>
<!--2ND Condition: Resource's name and path shall regular expression match with an expected's EHR name and path. -->
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
    <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/pid_[0-9]{7}/current/ehr_cur.xml</AttributeValue>
    <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
    </Apply>
</Apply>
</Condition>
<AdviceExpressions>
   <AdviceExpression AdviceId="NO_UPDATES_ALLOWED" AppliesTo="Deny">
   <AttributeAssignmentExpression AttributeId="advise-attribute:message">
   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">You are not allowed to update these elements. Proceed to perform a new
                                                                    Test.</AttributeValue>
    </AttributeAssignmentExpression>
    </AdviceExpression>
</AdviceExpressions>
</Rule>
```

```
 </Policy>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" xmlns:xacml="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="Policy_Secretaries"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">
<Description>In general a Secretary is able to create a new EHR, and read or update only the non-Medical part of EHR.</Description>
<PolicyDefaults>
  <XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</XPathVersion>
 </PolicyDefaults>
 <Target>
   <AnyOf>
     <AllOf>
       <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Secretary</AttributeValue>
       <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                           DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
       </Match>
     </AllOf>
   </AnyOf>
 </Target>
<Rule Effect="Permit" RuleId="Rule-SEC1">
<Description>A Secretary shall be able to create a new EHR for patients.</Description>
<Target>
   <AnyOf>
     <AllOf>
       <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
       <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">create</AttributeValue>
       <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                           DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
```

```
        </Match>
      </AllOf>
    </AnyOf>
</Target>
<Condition>
 <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
 <!--1ST Condition: Resource's name and path shall regular expression match with an expected's EHR name and path. -->
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
    <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/pid_[0-9]{7}/current/ehr_cur.xml</AttributeValue>
    <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                         DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
    </Apply>
 </Apply>
 </Condition>
 </Rule>
 <Rule Effect="Permit" RuleId="Rule-SEC2">
 <Description>A Secretary shall be able to read or write only the non-Medical Elements of an EHR.</Description>
 <Target>
    <AnyOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                                 DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
         </AllOf>
```

```
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
         </AllOf>
    </AnyOf>
    <AnyOf>
       <AllOf>
         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ChargeInfo</AttributeValue>
         <AttributeDesignator AttributeId="http:://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                                    category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
         </Match>
        </AllOf>
        <AllOf>
         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Person</AttributeValue>
        <AttributeDesignator AttributeId="http:://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                            category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
         </Match>
        </AllOf>
      </AnyOf>
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
```

```
<!--1ST Condition: Resource's name and path shall regular expression match with an expected's EHR name and path. -->
   <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
   <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
   <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/pid_[0-9]{7}/current/ehr_cur.xml</AttributeValue>
   <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
    </Apply>
</Apply>
</Condition>
</Rule>
</Policy>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="Policy_ITadmins" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-
                combining-algorithm:deny-unless-permit" Version="1.0">
<Description>An IT administrator should not be permitted to read/write the Patients' Electronic Health Records. He shall be permitted to read the audit trail files
            related to EHRs.</Description>
<Target>
    <AnyOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ITadmin</AttributeValue>
            <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
        </AllOf>
     </AnyOf>
 </Target>
```

```
<Rule Effect="Deny" RuleId="Rule-ITA1">
<Target>
   <AnyOf>
      <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
          <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
          </Match>
      </AllOf>
      <AllOf>
         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
         <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                               DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
         </Match>
      </AllOf>
   </AnyOf>
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/</AttributeValue>
<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                     DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
</Apply>
```

```
</Condition>
</Rule>
<Rule Effect="Permit" RuleId="Rule-ITA2">
<Target>
    <AnyOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
             </Match>
        </AllOf>
    </AnyOf>
</Target>
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
<Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/audit/</AttributeValue>
<AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
 </Apply>
 </Condition>
 </Rule>
  </Policy>
<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="Policy_Accountants" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-
            combining-algorithm:deny-unless-permit" Version="1.0">
<Description>An Accountant person may read any Invoice stored in the EMEDICA Information System, but can only write to (update) an Invoice during working
```

```
                hours.</Description>
<Target>
   <AnyOf>
      <AllOf>
         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Accountant</AttributeValue>
         <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                              DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
          </Match>
       </AllOf>
    </AnyOf>
</Target>
<Rule Effect="Permit" RuleId="Rule-ACC1">
<Target>
    <AnyOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
           <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                               DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
           </Match>
        </AllOf>
     </AnyOf>
     <AnyOf>
        <AllOf>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/invoices</AttributeValue>
```

```
        <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                    category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
        </Match>
      </AllOf>
    </AnyOf>
 </Target>
 <Condition>
 <Apply FunctionId="urn:oasis:names:tc:xacml:2.0:function:time-in-range">
     <Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:time-from-string">
          <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
          <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:environment:environment-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                    category:environment" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
          </Apply>
     </Apply>
     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">07:00:00</AttributeValue>
     <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">15:00:00</AttributeValue>
  </Apply>
</Condition>
</Rule>
<Rule Effect="Permit" RuleId="Rule-ACC2">
<Target>
   <AnyOf>
      <AllOf>
         <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
         <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                    DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
```

```
            </Match>
          </AllOf>
        </AnyOf>
        <AnyOf>
          <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/invoices</AttributeValue>
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                        category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
          </AllOf>
        </AnyOf>
    </Target>
    </Rule>
    </Policy>
    <Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" xmlns:xacml="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="Policy_Insurers"
            RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit" Version="1.0">
    <Description>In general an Insurer representative has only access rights for the -ChargeInfo- element of a patient's EHR.</Description>
    <PolicyDefaults>
        <XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</XPathVersion>
    </PolicyDefaults>
    <Target>
       <AnyOf>
          <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Insurer</AttributeValue>
            <AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
```

```
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
        </AllOf>
    </AnyOf>
</Target>
<Rule Effect="Permit" RuleId="Rule-INS1">
<Description>An Insurer shall be able to read the patient's -ChargeInfo- element of EHR, provided that he is being referenced in Patients EHR.</Description>
<Target>
    <AnyOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
            <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
            </Match>
        </AllOf>
    </AnyOf>
    <AnyOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ChargeInfo</AttributeValue>
            <AttributeDesignator AttributeId="http::://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                                        category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
            </Match>
        </AllOf>
        <AllOf>
            <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">RoomType</AttributeValue>
            <AttributeDesignator AttributeId="http::://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                                        category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
            </Match>
          </AllOf>
          <AllOf>
             <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">RoomNum</AttributeValue>
             <AttributeDesignator AttributeId="http::://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                                        category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
             </Match>
           </AllOf>
           <AllOf>
             <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ChargeValue</AttributeValue>
             <AttributeDesignator AttributeId="http::://wso2.org/my_attributes/resource-name" Category="urn:oasis:names:tc:xacml:3.0:attribute-
                                        category:resource" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
             </Match>
           </AllOf>
      </AnyOf>
  </Target>
  <Condition>
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">

  <!--1ST Condition: Insurers company Name, matches that in the Content of EHR-->
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:all-of-any">
      <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal"></Function>
```

```
    <AttributeDesignator MustBePresent="false" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                         AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
     <AttributeSelector MustBePresent="true" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                        Path="//xacml:ehealthrec/xacml:ChargeInfo/xacml:InsuranceProvider/text()" DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </Apply>
 <!--2ND Condition: Resource's name and path shall regular expression match with an expected's EHR name and path. -->
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of">
    <Function FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-regexp-match"></Function>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/_emedica/ehealth/patients/pid_[0-9]{7}/current/ehr_cur.xml</AttributeValue>
    <AttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                         DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"/>
    </Apply>
 </Apply>
</Condition>
</Rule>
</Policy>
</PolicySet>
```

Βιβλιογραφικές Πηγές

"Access Control: Policies, Models, and Mechanisms", 2001, Pierangela Samarati and Sabrina De Capitani di Vimercati

Whitepaper, "Getting Started With Attribute Based Access Control", Axiomatics

Whitepaper, "Attribute Based Access Control (ABAC) – the Best Cure for Sustainable eHealth Services", Axiomatics

Article, "100% pure XACML", http://www.axiomatics.com/pure-xacml.html

Article, "Fine-grained authorization", http://www.axiomatics.com/fine-grained-authorization.html

OASIS Standard, "eXtensible Access Control Markup Language (XACML) Version 3.0", 22 January 2013

OASIS, "XACML v3.0 Administration and Delegation Profile Version 1.0", 11 March 2010

OASIS, "XACML v3.0 Hierarchical Resource Profile Version 1.0", 11 March 2010

Project report, "Access Control Service Oriented Architecture Security", Yoon Jae Kim

WSO2 Identity Server documentation version 4.1.0, "Configuring the Identity Server" – "Managing Entitlement" – "Managing the Registry", http://docs.wso2.org/wiki/display/IS410/Identity+Server+Administration

"Extensible Markup Language (XML) 1.0 (Fifth Edition)", 26 November 2008, W3C Recommendation, http://www.w3.org/TR/2008/REC-xml-20081126/

"XPath – A practical guide", Arne Blankerts, TobiasSchlitt, 2009-11-17, http://www.slideshare.net