Policy Based Electronic Transmission of Prescriptions

D.W.Chadwick
IS Institute, University of Salford, The Crescent, Salford M5 4WT
d.w.chadwick@salford.ac.uk

D. Mundy
IS Institute, University of Salford, The Crescent, Salford M5 4WT
d.mundy@salford.ac.uk

Abstract

This paper describes the PERMIS PMI role based authorisation policy, and shows how it has been applied to the electronic transfer of prescriptions (ETP). The assignment of roles is distributed to the appropriate authorities in the health care and government sectors. This includes the assignment of both professional roles such as doctor and dentist, as well as patient roles that entitle patients to free prescriptions. All roles are stored as X.509 attribute certificates (ACs) in LDAP directories, which are managed by the assigning authorities. The PERMIS policy based decision engine subsequently retrieves these role ACs in order to make Granted or Denied access control decisions required by the ETP applications. The Source of Authority for setting the ETP policy is assumed to be the Secretary of State for Health. The ETP policy says what roles are recognised, who is authorised to assign the roles, what privileges are granted to each role and what conditions are attached to these privileges. The ETP policy is then formatted in XML, embedded in an X.509 attribute certificate, digitally signed by the Secretary of State for Health, and then stored in an LDAP directory. From here it can be accessed by all the ETP applications in the UK National Health Service that contain embedded policy based PERMIS decision engines.

1. Introduction

The UK Government has stated that the Electronic Transmission of Prescriptions (ETP) will be available within the UK National Health Service (NHS) by 2004 [1]. Although electronic prescription transfer systems do exist in other countries [2] [3] the UK NHS system would need to handle in the order of 600 million prescriptions per year [13] which is far in excess of what any current ETP system handles. A centralised body called the Prescription Pricing Authority (PPA) processes payments for medicinal prescriptions dispensed within the UK NHS. Therefore all electronic prescriptions will need to be sent to the PPA for processing.

Medical professionals have a legal and ethical obligation to protect the confidentiality of patient information [4] [5]. This means that the unprotected transfer of plain textual prescriptions across insecure networks is clearly not an option. It is also necessary to ensure that only medical professionals involved in ETP can access the system and the prescriptions within it. Further, the professionals are guided by the principles of the Caldicott Report [10] which states that in relation to identifiable patient information, health care professionals should justify the purpose(s) for using confidential information, only use it when absolutely necessary and use the minimum that is required. For example, if electronic prescriptions are stored in a central repository, then a pharmacist should not have access to every prescription in the store, but only to the ones that he is going to dispense. Therefore the proper authorisation of individuals is essential. Clearly the security of the electronic information and of the system itself will be a key factor in the success or failure of ETP.

There are currently 3 pilot systems undergoing trials in the UK [6]. Each uses a different model for ETP, and different security mechanisms. All make trade-offs between security and usability [7]. But none of them implement policy based authorisation. Indeed, from the limited information available it would seem that none of the ETP pilot systems enforce authorisation at all, but rather rely on the integrity of the professionals to not abuse their privileges. In this paper we describe a policy based ETP authorisation system that enforces the rights and privileges of all the different parties involved in ETP, including those of patients to receive free prescriptions. Other security aspects of ETP have been described in a previous paper [20].

2. The Existing Paper Based System

Before considering ETP, it is necessary to appreciate the current paper based system with its inbuilt

authorisations and roles. A patient has a consultation with a prescribing doctor (or dentist or nurse), and is handed a paper prescription at the end of the consultation, written on a NHS FP10 prescription form. The doctor then signs the prescription and hands it to the patient, who carries it to the pharmacy for dispensing. In some cases it may be a relative or friend of the patient who takes the prescription to the pharmacy, especially if the patient is too ill to go themselves. The patient is free to choose whichever pharmacy they wish to go to - it could be in another town if this is convenient to the patient.

The pharmacist is handed the paper prescription and enters the details into his pharmacy PC system. This system will print out the labels for the drug packages, as well as recording details for stock taking and re-ordering. The patient is asked to sign the prescription and to tick a box if he is entitled to free prescriptions, otherwise he pays the dispensing fee. The patient is given the drugs and the pharmacist batches the dispensed prescription forms to be delivered to the PPA in Newcastle once a month.

Different prescribing practitioners are entitled to prescribe different drugs sets in the UK. Prescribing nurses for example are only allowed to prescribe a limited set of drugs. In the paper world, the physical possession of a NHS FP10 prescription form indicates the authority to prescribe. Entitlement to prescribe different drugs sets is controlled by colour coding the prescription forms, and allocating the different forms to the different prescribing groups: doctors, dentists, nurses etc. Clearly the same mechanism cannot be used in an electronic system, given that electronic prescription forms can easily be copied. Instead we have chosen to base authorisations on the different roles allocated to each professional (see below).

Pharmacists are authorised to dispense in general by their professional body, the Royal College of Pharmacy, and are entitled specifically by the patient (or their representative) to dispense a given prescription, by being handed the prescription form. It is the patient who ultimately decides who will be authorised to dispense a particular prescription.

Some patients are entitled to free prescriptions. The current paper based system relies on pharmacists questioning patients and checking documents such as benefit cards to ensure that a patient is entitled to reduced charges, and then the patient must sign the prescription to claim the benefit. This situation can lead to conflict in the workplace for the Pharmacist and also to prescription fraud through unchecked exemptions. Indeed if the patients do not have any details to prove their entitlement often the prescription will be dispensed with a Pharmacist endorsement on the prescription note asking the PPA to check the exemption.

3. Converting the Paper System to ETP

In our design [20], electronic prescriptions are created by the prescriber, digitally signed (for authentication purposes), symmetrically encrypted (for confidentiality), then sent to a central storage location. The patient is given a paper prescription containing a bar code that holds the symmetric encryption key. The patient then goes to a pharmacy of his choosing, hands over the prescription, the pharmacist scans in the barcode then retrieves the prescription and decrypts it. The patient ultimately controls who is authorised to dispense his prescription, as in the current paper based system. But this is not enough. We also want to have controls on who is authorised to prescribe and dispense which drug sets, and who is entitled to free prescriptions.

Given the large numbers of professionals involved in ETP in the UK (34,500 GPs, 10,000 prescribing nurses rising to 120,000 over the next few years, 44,000 registered pharmacists and 22,000 dentists) [8][9], and the very few authorisations that are actually required (i.e. various permission levels for prescribing, dispensing, and entitlements to free prescriptions), then role based access controls (RBAC) seems to be the ideal authorisation mechanism to use for ETP. When this is coupled with the number of potential patients in the UK (60 million), and the fact that free prescriptions account for 85% of prescribed items [21], then RBAC should also be used to control access to free prescriptions if possible. Given the very large numbers of people who need to be authorised/entitled, it is essential that we distribute the management of roles to competent authorities, rather than try to centralise it, otherwise it will become unmanageable.

Each professional has an authoritative body who grants them the right to engage in their profession. In the UK, the General Medical Council is responsible for registering doctors, and for striking them off the list in cases of professional misconduct. The General Dental Council performs the same role for dentists, the Nursing and Midwifery Council for nurses, and the Royal College of Pharmacy for pharmacists. In our ETP system we propose to distribute the allocation of roles to these bodies, since it is a function that they are already performing well.

Created in June 2001, the Department for Work and Pensions (DWP) has taken over the responsibilities of the former Departments of Social Security, and Education and Employment. It is responsible for paying unemployment benefits and pensions, and along with the PPA, determining entitlement to free prescriptions. Many people are entitled to free prescriptions including: people aged 60 and over, children under age 16, young people aged 16, 17 or 18 in full-time education, people or their partner in receipt of Income Support or Jobseeker's

Allowance, people named on a current NHS Low Income Scheme Full Help Certificate (HC2), expectant mothers, women who have given birth in the past 12 months, and war disablement pensioners. Consequently the management of this entitlement is distributed between different branches of the DWP and the PPA.

The EC PERMIS project has developed a policy driven, role based, privilege management infrastructure [11]. When a user wishes to access an electronic resource, he presents a set of one or more roles[1] (encoded as X.509 attribute certificates (ACs) [12]), and the PERMIS API returns Granted or Denied based on the policy for accessing the resource and any relevant environmental parameters, such as time of day, or number of previous accesses etc. The PERMIS API can work in either push or pull mode. In the push mode, the user pushes his role ACs to the policy driven decision engine, in pull mode, the decision engine picks up the user's role ACs from the set of configured LDAP directories. ACs are digitally signed by the authority assigning the roles to the individual, so that they are tamper resistant and provide authenticity. Consequently, the PERMIS PMI would seem to be ideal for implementing policy based authorisation in ETP.

If each professional is allocated a role AC by their professional body, and this is stored in the LDAP directory belonging to the professional body, then the ETP system will be able to make authorisation decisions about prescribing and dispensing if it has access to those LDAP directories. Similarly, if the Department for Work and Pensions allocates role ACs to people who are entitled to free prescriptions for various reasons, and stores these in its LDAP directory (or directories), then the ETP system will be able to make decisions about entitlement to free prescriptions by accessing this LDAP directory, without the pharmacist needing to quiz the patient about their entitlement. The latter will only be needed in cases when a patient becomes newly entitled, for example when a pregnant woman is first diagnosed by her GP, and the DWP has had insufficient time to create the official AC. This distributed allocation of roles, embedded in digitally signed ACs and stored in the local LDAP directories of the assigning authorities, is shown in Figure 1.

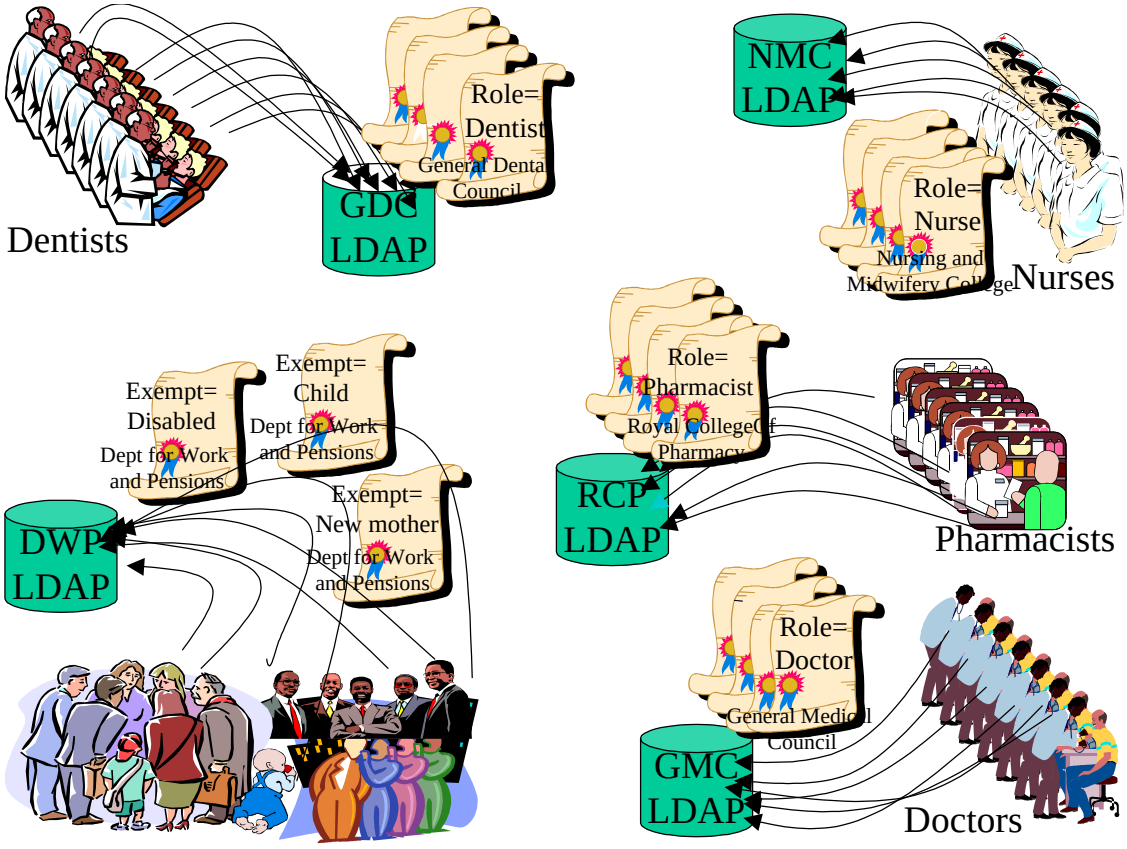

Figure 1. The distributed allocation of roles

[1] Note that PERMIS is very liberal in its definition of a role. It can in fact be any attribute comprising a type and a value.

These roles are subsequently used by the PERMIS decision engine to determine whether doctors are allowed to prescribe, pharmacists to dispense, and patients to receive free prescriptions, according to the ETP policy. Each ETP application (prescribing system, dispensing system, PPA system) reads in the ETP policy at initialisation time, then when specific professionals request actions, such as prescribe or dispense, the PERMIS decision engine fetches the persons role from the configured in LDAP directory, and makes its decision according to the policy. This is shown in Figure 2.

The remainder of this paper describes the ETP policy that is used by the PERMIS decision engine.

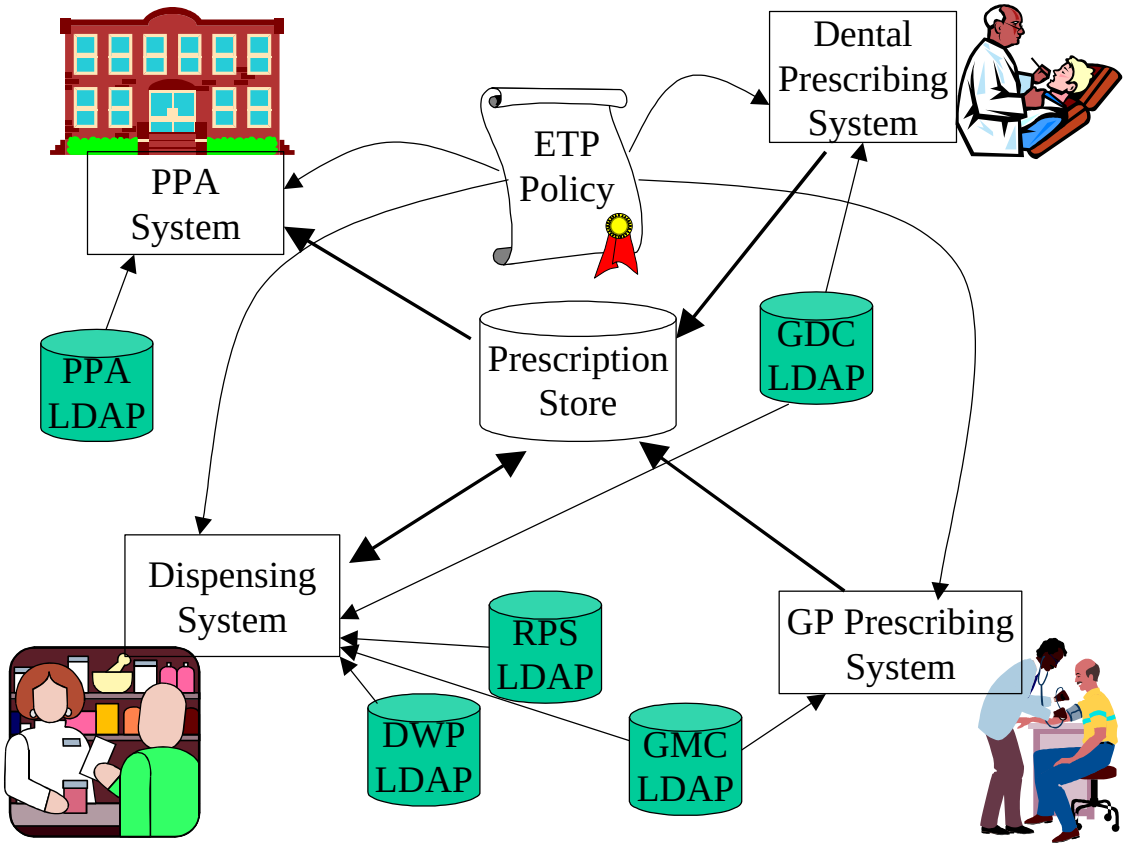

Figure 2. The ETP policy based authorisation system

4. The PERMIS Policy DTD

The PERMIS policy is based on a subset of the concepts defined in Ponder [14]. Policies are written in XML, according to a DTD grammar that has been published at XML.org [15]. The PERMIS policy DTD comprises the following components:

- SubjectPolicy – this specifies the subject domains i.e. only users from a subject domain may be granted rights covered by the policy. If a user is not from a subject domain he will be denied all rights. Each domain is specified as a subtree using LDAP distinguished names (DNs) [19], based on the X.500 subtree specification [16]. A subtree is specified using Include DN and Exclude DN statements, and Include statements can specify layers of the tree to be included using Max and Min depth statements. In this way arbitrarily complex subtrees can be described.
- RoleHierarchyPolicy – this specifies the different roles recognised by the policy, and their hierarchical relationships to each other. Superior roles inherit the privileges granted to their subordinate roles. A role is loosely defined as any attribute type and value, so that patient entitlements to free prescriptions can be encoded as a role.
- SOAPolicy – this specifies a list of Sources Of Authority who are trusted to allocate roles to subjects. The first SOA in the list is the locally trusted SOA and it is this SOA who issues the overall policy. By including more than one SOA in this list, the locally trusted SOA is effectively cross certifying remote authorisation domains, and saying that it

trusts the remote SOAs to allocate roles as defined in the following Role Assignment Policy. In ETP there are many remote SOAs, these being the professional bodies who allocate the roles to the different professional groups e.g. doctors, nurses, pharmacists etc.

- RoleAssignmentPolicy – this specifies which roles may be assigned to which subjects by which SOAs, whether delegation of roles may take place or not, and how long the roles may be assigned for. Whilst PERMIS has catered for the delegation of authority in the policy, the PERMIS decision engine is not yet capable of validating delegation chains. This functionality will be implemented in a subsequent release.
- TargetPolicy – this specifies the target domains covered by this policy. Target domains are specified in the same way as subject domains, i.e. as LDAP subtrees, but in addition subtree filtering is supported. Subtrees can be filtered by specifying particular object classes within the target domain, so that for example, all laser printers in an organisational unit could be specified (filtered), thus excluding colour inkjet printers. Filtering is supported in target domain specifications, since the PERMIS decision engine can trust the target application to say what object class it is. The same is not true for subjects, as they could claim to be of any object class they desired. Subjects can only reliably claim to be of a particular object class if a trusted SOA vouches for it, in an AC. Hence the subject's object class just becomes another role assigned as part of the role assignment policy.
- ActionPolicy – this specifies the actions (or methods) supported by the targets, along with the parameters that should be passed along with each action e.g. action Open with parameter Filename. Specifying the Action Policy as a separate subpolicy, rather than including it as part of the Target Access Policy, is purely a matter of efficiency of policy creation, since the action and its parameters only needs to be declared once rather than each time with every target access.
- TargetAccessPolicy – this specifies which roles have permission to perform which actions on which targets, and under which conditions. Note that the policy implicitly operates the Deny All Unless Explicitly Granted rule, so that only those permissions in the target access clauses will ever be granted. The Target Access Policy is an enhanced version of the privilege policy specified in clause D.2 of Annex D of X.509 [12]. Conditions are specified using Boolean logic and might contain constraints such as "IF time is GT 9am AND time is LT 5pm OR IF Calling IP address is a subset of 125.67.x.x". A condition comprises:
  - a comparison (logical) operator
  - the LHS operand(variable), described by its source, name and type, and
  - a series of one or more variables or constant values against which the LHS operand is to be compared.

  The operator is chosen from the following set: PRESENT | EQ | GT | LT | LE | GE |Subordinate | Substrings | Subset | Superset | NonNullIntersection | ApproxEQ | and Operator, where Operator is an extensibility mechanism to allow policy setters to define new operators for their condition statements. The meaning of any new operator and the number of operands it operates on is application specific. The PERMIS API will support the calling of new Java objects that implement the new operators and their operands.

A full specification of the policy can be found in [17].

5. ETP Policy Specification

The Department of Health is responsible for running the 3 current UK ETP trials. Consequently in our pilot, we have assumed that the ETP policy will be specified by the head of the Department of Health (of course it could be his nominee in real life). The head of the DoH is therefore the locally trusted SOA for the policy. Once the policy has been specified, it will be converted into XML format (according to the above DTD), embedded into an X.509 attribute certificate, and digitally signed by the head of the DoH. It will then be stored in an LDAP directory from where it can be accessed by every ETP application in the UK. Each ETP application is configured with the LDAP distinguished name of the person who has signed the policy (the trusted SOA), the URL of the LDAP directory where the policy is stored, and the globally unique object identifier of the policy. (Each policy is given a globally unique object identifier, so that multiple policies can be created by the trusted SOA, and the application can be told which policy to use each time.)

Each component of the policy is described below. Appendix 1 contains the complete ETP policy encoded in XML format.

5.1. Subject Policy

The UK NHS has defined a standard [18] for globally uniquely naming every hospital, NHS trust, and health care professional in the UK. We have used this standard to define the subject domain that will encompass all NHS professionals, namely O=NHS, C=GB. If an ETP professional does not have an attribute certificate with a

subject name from this domain, he will be denied access to ETP. Unfortunately, the NHS standard says nothing about naming patients. For the purposes of our pilot application, we have chosen the subject domain OU=Patients, C=GB, and named all patients using their National Health number, a 10 digit string. Of course, this can be changed as appropriate in a live system.

5.2. Role Hierarchy Policy

In our pilot we have defined five professional roles: GPPrescriber, NursePrescriber, DentalPrescriber, Dispenser and PPAAdministrator. None of these roles form a role hierarchy in the RBAC sense, in that none of them inherit the privileges of their subordinate roles. We thus did not need to make use of the hierarchical RBAC feature supported by PERMIS.

We have also defined 11 exemption roles for patients, namely: DSSExempt, Under16, Under19FE, Over60, ValidExemptionCertificate-MedicalExemption, ValidExemptionCertificate-NewMother, ValidExemptionCertificate-DisablementExemption, DSSbyAssociation, ValidPrePaymentCertificate, and TaxCreditHC2Entitlement. Again none of these exemptions form a role hierarchy. In a live system, these can be added to and subtracted from as legislation evolves.

5.3. SOA Policy

The trusted SOA is the head of the Department of Health, whose LDAP DN is "cn=Secretary of State for Health, ou=Department of Health, o=Government, c=GB". The ETP policy AC will be digitally signed by the private key belonging to this person.

The remote SOAs who are trusted to assign roles to the various ETP participants are the ETP administrators of the four professional bodies (the General Medical Council, the General Dental Council, the Royal College of Pharmacy, and the Nursing and Midwifery Council (formerly the UK Central Council for Nursing UKCC)), and the Department for Work and Pensions and the Prescription Pricing Authority who administer entitlements to free prescriptions. Each of these has been given a unique LDAP DN according to the NHS naming standard [18]. If the DWP wanted to distribute the management of free prescriptions to other departments and branches, then it would be a simple matter to add further names to this list of trusted remote SOAs.

In the XML version of the policy, each SOA in the list is given a short name ID, and it is the name ID that is used in the following role assignment policy so that their full LDAP DNs do not have to be repeated.

5.4. Role Assignment Policy

The role assignment policy simply states that the GMC may assign GP Prescriber roles to subjects from the NHS professionals' domain, the GDC may similarly assign Dental Prescriber roles, the NMC may similarly assign Nurse Prescriber roles, and the RCP may similarly assign Dispenser roles. The PPA may assign the PPA Administrator role to subjects from the NHS professionals' domain, and any of the 11 exemption roles to subjects from the patients' domain. The DWP are similarly authorised to assign the 11 exemption roles. It would be possible to partition the exemption assignments if required, so that the DWP and PPA each could assign a subset of the exemption roles to patients.

Delegation of role assignment is currently not allowed. This is not a limitation of the PERMIS policy design, but rather that the policy driven decision engine is currently not able to validate attribute certificate delegation chains. This is due to be added in a future research project. The current work around to support delegation of authority, is to add the name of the subordinate assigning authority into the list of trusted remote SOAs in the SOA policy. This is a static delegation of authority, rather than a dynamic one that would be allowed if delegation were enabled in the role assignment policy.

5.5. Target Policy

There are three target application domains in ETP: the dispensing applications in the pharmacies, the prescribing applications in the GP, dental and nurses surgeries, and the administrative application at the PPA. Each application will have a globally unique LDAP DN allocated to it at configuration time, chosen from the appropriate target domain specified in the policy. For example, the dispensing application at Boots the Chemist, in the High Street in Oldham, Lancashire, may have the name cn="Boots, High St, Oldham", ou=e-Dispensing Applications, ou=Applications, o=NHS, c=GB allocated to it in its configuration file.

An alternative way of specifying the three target domains would have been to use the object class filtering mechanism supported by PERMIS for describing target domains. Thus the three target domains of the ETP policy could all have been defined using the same subtree root of ou=Applications, o=NHS, c=GB; with each using a different object class filter of Prescribing Application, Dispensing Application or PPA Administration Application.

5.6. Action Policy

Four different methods can be invoked in our ETP application, namely: dispense, prescribe, administrate and

dontCharge. The dispense action is called by a pharmacist, and has no arguments. Prescribe is called by doctors, dentists and nurses. The method has one argument, which is the type of prescription to be prescribed. This is used to mirror the paper based system of having different coloured NHS FP10 prescription forms allocated to different classes of prescriber. The prescriber calls the prescribe method passing the type of prescription to be written. If the prescriber is authorised to write this type of prescription then they will be Granted access, otherwise Denied access. The dontCharge action is called within the dispensing application to determine if the patient is entitled to free prescriptions or not. It has no arguments, as the patient name is extracted from the electronic prescription.

5.7. Target Access Policy

The target access policy specifies which roles are needed to perform which actions on which targets, and what conditions, if any, are attached to granting the actions. Anyone with the role of GP Prescriber is allowed to perform the prescribe action on the prescribing application. Anyone with the role of Nurse Prescriber is similarly authorised, but only if the Prescription Type has the string value *Nursing*. Likewise anyone with the role of Dental Prescriber is only authorised to prescribe prescriptions of type *Dental*. Since GPs are allowed to prescribe any and every drug, no conditions have been attached to granting permission for their action. It would be possible to refine the policy to differentiate between prescribing controlled drugs and non-controlled drugs, by including two target access policies instead of the current one for GPs. In the first policy, permission would only be granted if "Prescription Type equals Controlled Drugs", and the second would have the condition "only if Prescription Type is not equal to Controlled Drugs". But there seemed little point in including both permissions in the same policy.

The prescriber calls the prescribe method passing the type of prescription to be written as an argument. The prescribe application calls the PERMIS decision engine, passing it the action name and the type of prescription to be written in the environmental parameters. If the prescriber has the appropriate role commensurate with the prescription type, they will be Granted access. In the case of GPs, the PERMIS decision engine will never inspect the environmental parameters, since there are no conditions attached to granting the request, other than the possession of the GP Prescriber role.

The dispense action will be granted to anyone with the Dispenser role, and once authorised by the PERMIS decision engine, the dispensing application will fetch the prescription from the prescription store, decrypt it, verify the digital signature on it and display it to the pharmacist. Remember that whilst pharmacists are in general authorised to dispense any prescription, they are only enabled to dispense specific ones since the patient is the custodian of the symmetric decryption key in the barcode on his prescription.

Anyone with the role of PPA Admin will be granted permission to perform PPA administrative actions from any PPA administrative application in the PPA Domain. Actions that a PPA administrator may invoke are: retrieve and remove from the central prescription store all prescriptions that have dispensed, and delete time expired prescriptions from the central store. These three actions could have been separately specified in the policy, so that each time the PPA administrator called one of the actions, the PERMIS decision engine would have been called to either Grant or Deny permission. We thought it more efficient to authorise the administrator once when he logged onto the application in administrative mode, and then let him perform a series of actions without further authorising each one. This was purely an application design decision on our part, as we weighed up the overhead of authorising each action against the risk of only authorising once at login time. The PERMIS decision engine is capable of supporting either mode of operation, as it is a policy issue as to which actions are to be authorised and which are not.

Finally, any patient with any of the 11 exemption roles is entitled to free prescriptions, so the dispensing application must pass the patient's name to the PERMIS decision engine to ask if free prescriptions are granted or not.

6. Conclusion

We have described the generic PERMIS PMI role based authorisation policy, and shown how it has been successfully applied to the electronic transfer of prescriptions (ETP) application. None of the current UK ETP trials have implemented an authorisation mechanism, which the authors believe is a deficiency. The PERMIS PMI is suitable for a large-scale application such as ETP, since the assignment of roles can be distributed to the appropriate authorities in the health care and government sectors, and the policy is digitally signed so as to protect it from tampering. The policy can then be easily distributed to all the ETP applications in the UK National Health Service. Furthermore, the PERMIS PMI is standards based, using XML to formulate policies, X.509 attribute certificates to package roles and policies, and LDAP directories to store roles and policies. This will facilitate interoperability between competing suppliers, and ease development effort as standards supporting toolkits are readily available.

7. References

[1] The NHS Plan, *http://www.nhs.uk/nationalplan/nhsplan.htm*, (February 21 2002)
[2] AllScripts, *http://www.allscripts.com/ahcs/index.htm*, (November 2002)
[3] H. Middleton, "*Electronically Transmitted Prescriptions – a good idea"*, The Pharmaceutical Journal, Vol 265 No 7107 p172-176, July 2000
[4] UK Government, *"Data Protection Act 1998 (c.29)"*, Crown Copyright 1998
[5] Protection and Use of Patient Information. *http://www.doh.gov.uk/ipu/confiden/protect*, (January 2002)
[6] ETP Trials *http://www.doh.gov.uk/Pharmacy/etp.htm*
[7] D.P.Mundy, D.W.Chadwick. "Security Issues in the Electronic Transmission of Prescriptions". Submitted to "Medical informatics and the Internet in Medicine", Taylor and Francis Healthsciences, December 2002
[8] http://www.nationalstatistics.gov.uk/STATBASE/Expodata/Spreadsheets/D5945.xls
[9] http://www.pharmj.com/Editorial/20010825/comment/lett03.html
[10] NHS Executive, "The Caldicott Committee: report on the review of patient-identifiable information – December 1997", Available at http://www.doh.gov.uk/confiden/crep.htm (November 2002)
[11] D.W.Chadwick, A. Otenko. "The PERMIS X.509 Role Based Privilege Management Infrastructure", Proc 7th ACM Symposium On Access Control Models And Technologies (SACMAT 2002), Monterey, USA, June 2002. pp135-140.
[12] ITU-T Rec. X.509 (2000) | ISO/IEC 9594-8 The Directory: Authentication Framework
[13] Dept of Health "Prescriptions dispensed in the Community, Statistics for 1991 to 2001: England" http://www.doh.gov.uk/public/sb0214.htm
[14] Damianou, N., Dulay, N., Lupu, E., Sloman, M. "The Ponder Policy Specification Language", Proc Policy 2001, Workshop on Policies for Distributed Systems and Networks, Bristol, UK 29-31 Jan 2001, Springer-Verlag LNCS 1995, pp 18-39
[15] http://www.xml.org/xml/registry.jsp (11 December 2002)
[16] ITU-T Rec. X.501 (2000) | ISO/IEC 9594-2 The Directory: Models
[17] D.W.Chadwick, A. Otenko. "RBAC Policies in XML for X.509 Based Privilege Management" in Security in the Information Society: Visions and Perspectives: IFIP TC11 17th Int. Conf. On Information Security (SEC2002), May 7-9, 2002, Cairo, Egypt. Ed. by M. A. Ghonaimy, M. T. El-Hadidi, H.K.Aslan, Kluwer Academic Publishers, pp 39-53.
[18] NHS Information Authority. "Directory Services. National Health Service Standard NHS 0001". 2nd Ed. Reference NHS 0001:1999
[19] Wahl, M., Kille, S., Howes, T. "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC2253, December 1997
[20] Mundy, D.P. and Chadwick, D.W. *"A system for secure electronic prescription handling"*, Second International Conference On The Management Of Healthcare And Medical Technology On: The Hospital of the Future Bringing Together Technology, Health Care and Management. Abstract and Main Paper on accompanying CD-Rom, Stuart Graduate School of Business, Center for the Management of Medical Technology, Illinois Institute of Technology, Chicago, Illinois, USA, July 28-30, 2002.
[21] Free prescriptions statistics http://www.doh.gov.uk/public/sb0119.htm

Appendix 1 The ETP Policy in XML

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE X.509_PMI_RBAC_Policy SYSTEM
"file://localhost/C:/research/projects/permis/policy7.dtd">
<X.509_PMI_RBAC_Policy
OID="1.2.826.0.1.3344810.6.0.1.1">
  <SubjectPolicy><!-- 2 domains. NHS professional and
patients   -->
          <SubjectDomainSpec
ID="NHS_professionals">
     <Include LDAPDN="O=nhs,C=gb"/>
   </SubjectDomainSpec>
   <SubjectDomainSpec ID="Patients">
     <Include LDAPDN="OU=Patients,O=NHS,c=gb"/>
   </SubjectDomainSpec>
  </SubjectPolicy>
  <RoleHierarchyPolicy>
   <RoleSpec OID="1.2.826.0.1.3344810.1.1.22"
Type="eppRole">
     <SupRole Value="GPPrescriber"/>
     <SupRole Value="NursePrescriber"/>
     <SupRole Value="DentalPrescriber"/>
     <SupRole Value="Dispenser"/>
     <SupRole Value="PpaAdmin"/>
   </RoleSpec>
   <RoleSpec OID="1.2.826.0.1.3344810.1.1.23"
Type="exemptionRole">
     <SupRole Value="DSSExempt"/>
     <SupRole Value="Under16"/>
     <SupRole Value="Under19FE"/>
     <SupRole Value="Over60"/>
     <SupRole Value="ValidExemptionCertificate-
MedicalExemption"/>
     <SupRole Value="ValidExemptionCertificate-
NewMother"/>
     <SupRole Value="ValidExemptionCertificate-
DisablementExemption"/>
     <SupRole Value="DSSbyAssociation"/>
     <SupRole Value="ValidPrePaymentCertificate"/>
     <SupRole Value="TaxCredit"/>
     <SupRole Value="HC2Entitlement"/>
   </RoleSpec>
  </RoleHierarchyPolicy>
  <SOAPolicy>
    <SOASpec ID="Owner" LDAPDN=
"cn=Secretary of State for Health,ou=Department of
Health,o=Government,c=GB"/>
   <SOASpec ID="GMC" LDAPDN=
```

```
"cn=ETP Administrator,o=General Medical
Council,l=National,o=NHS,c=gb"/>
   <SOASpec ID="RCP" LDAPDN=
"cn=ETP Administrator,o=Royal
CP,l=National,o=NHS,c=gb"/>
   <SOASpec ID="NMC" LDAPDN=
"cn=EPP
Administrator,o=NMC,l=National,o=NHS,c=gb"/>
   <SOASpec ID="GDC" LDAPDN=
"cn=ETP Administrator,o=General Dental
Council,l=National,o=NHS,c=gb"/>
   <SOASpec ID="DWP" LDAPDN=
"cn=ETP Administrator,ou=Dept for Work and
Pensions,o=Government,c=gb"/>
   <SOASpec ID="PPA" LDAPDN=
"cn=ETP
Administrator,o=PPA,l=National,o=NHS,c=gb"/>
  </SOAPolicy>
  <RoleAssignmentPolicy>
    <RoleAssignment>
      <SubjectDomain ID="NHS_professionals"/>
      <RoleList>
        <Role Type="eppRole" Value="GPPrescriber"/>
      </RoleList>
      <Delegate Depth="0"/>
      <SOA ID="GMC"/>
      <Validity/>
    </RoleAssignment>
    <RoleAssignment>
      <SubjectDomain ID="NHS_professionals"/>
      <RoleList>
        <Role Type="eppRole" Value="NursePrescriber"/>
      </RoleList>
      <Delegate Depth="0"/>
      <SOA ID="NMC"/>
      <Validity/>
    </RoleAssignment>
    <RoleAssignment>
      <SubjectDomain ID="NHS_professionals"/>
      <RoleList>
        <Role Type="eppRole" Value="DentalPrescriber"/>
      </RoleList>
      <Delegate Depth="0"/>
      <SOA ID="GDC"/>
      <Validity/>
    </RoleAssignment>
    <RoleAssignment>
      <SubjectDomain ID="NHS_professionals"/>
      <RoleList>
        <Role Type="eppRole" Value="Dispenser"/>
      </RoleList>
      <Delegate Depth="0"/>
      <SOA ID="RCP"/>
      <Validity/>
    </RoleAssignment>
    <RoleAssignment>
      <SubjectDomain ID="NHS_professionals"/>
      <RoleList>
        <Role Type="eppRole" Value="PpaAdmin"/>
      </RoleList>
      <Delegate Depth="0"/>
      <SOA ID="PPA"/>
      <Validity/>
    </RoleAssignment>
    <RoleAssignment>
      <SubjectDomain ID="Patients"/>
      <RoleList>
        <Role Type="exemptionRole" Value=""/>
      </RoleList>
      <Delegate Depth="0"/>
      <SOA ID="DWP"/>
      <Validity/>
    </RoleAssignment>
    <RoleAssignment>
      <SubjectDomain ID="Patients"/>
      <RoleList>
        <Role Type="exemptionRole" Value=""/>
      </RoleList>
      <Delegate Depth="0"/>
      <SOA ID="PPA"/>
      <Validity/>
    </RoleAssignment>
  </RoleAssignmentPolicy>
  <TargetPolicy>
    <TargetDomainSpec ID="PharmacistApplications">
      <Include LDAPDN="ou=e-Dispensing
Applications,ou=Applications,o=NHS,c=GB"/>
    </TargetDomainSpec>
    <TargetDomainSpec ID="PrescribingApplications">
      <Include LDAPDN="ou=e-Prescribing
Applications,ou=Applications,o=NHS,c=GB"/>
    </TargetDomainSpec>
    <TargetDomainSpec ID="PpaDomain">
      <Include LDAPDN="ou=Administration
Applications,ou=Applications,o=NHS,c=GB"/>
    </TargetDomainSpec>
  </TargetPolicy>
  <ActionPolicy>
    <Action Args="PrescriptionType"
Name="Prescribe"/>
    <Action Args="" Name="Dispense"/>
    <Action Args="" Name="DontCharge"/>
    <Action Args="" Name="PpaAdministration"/>
  </ActionPolicy>
  <TargetAccessPolicy>
    <TargetAccess>
      <RoleList>
        <Role Type="eppRole" Value="GPPrescriber"/>
      </RoleList>
      <TargetList>
```

```
    <Target Actions="Prescribe">
      <TargetDomain ID="PrescribingApplications"/>
    </Target>
  </TargetList>
</TargetAccess>
<TargetAccess>
  <RoleList>
    <Role Type="eppRole" Value="NursePrescriber"/>
  </RoleList>
  <TargetList>
    <Target Actions="Prescribe">
      <TargetDomain ID="PrescribingApplications"/>
    </Target>
  </TargetList>
  <IF>
    <EQ>
      <Arg Name="PrescriptionType" Type="String"/>
      <Constant Type="String" Value="Nursing"/>
    </EQ>
  </IF>
</TargetAccess>
<TargetAccess>
  <RoleList>
    <Role Type="eppRole" Value="DentalPrescriber"/>
  </RoleList>
  <TargetList>
    <Target Actions="Prescribe">
      <TargetDomain ID="PrescribingApplications"/>
    </Target>
  </TargetList>
  <IF>
    <EQ>
      <Arg Name="PrescriptionType" Type="String"/>
      <Constant Type="String" Value="Dental"/>
    </EQ>
  </IF>
</TargetAccess>
<TargetAccess>
  <RoleList>
    <Role Type="eppRole" Value="Dispenser"/>
  </RoleList>
  <TargetList>
    <Target Actions="Dispense">
      <TargetDomain ID="PharmacistApplications"/>
    </Target>
  </TargetList>
</TargetAccess>
<TargetAccess>
  <RoleList>
    <Role Type="eppRole" Value="PpaAdmin"/>
  </RoleList>
  <TargetList>
    <Target Actions="PpaAdministration">
      <TargetDomain ID="PpaDomain"/>
    </Target>
  </TargetList>
</TargetAccess>
<TargetAccess>
  <RoleList>
    <Role Type="exemptionRole"/>
  </RoleList>
  <TargetList>
    <Target Actions="DontCharge">
      <TargetDomain ID="PharmacistApplications"/>
    </Target>
  </TargetList>
</TargetAccess>
</TargetAccessPolicy>
</X.509_PMI_RBAC_Policy>
```