A System For Secure Electronic Prescription Handling

D.P.Mundy, D.W.Chadwick

Contact Author

Contact Details

Darren P Mundy
Email: d.mundy@salford.ac.uk
Postal: IS Institute, University of Salford, The Crescent, Salford M5 4WT
Tel No: +44 161 295 5664
Fax No: +44 161 745 8169

Other Author

Contact Details

Prof David W. Chadwick
Email: d.w.chadwick@salford.ac.uk
Postal: IS Institute, University of Salford, The Crescent, Salford M5 4WT
Tel +44 161 295 5351
Fax +44 161 745 8169

Abstract

The National Health Service (NHS) in the United Kingdom (UK) is currently going through a period of vast reform, with guidelines for that reform set out in the NHS plan [1]. As part of the plan a system for electronic prescribing of drugs should be available by 2004. The main objective of this transformation is to remove many of the frailties of the present paper based system, in terms of fraud, inefficiency and administrative workload. However, any proposed system must also uphold the tradition of patient choice with respect to dispensing pharmacy, and must be reliable, robust and of good performance if it is to have any hope of gaining acceptance from the health professionals involved.

In this paper we set out our proposed electronic prescription processing system design, with the emphasis placed firmly on performance, scalability and security. In the early sections we aim to demonstrate just why an electronic prescribing system is required, by looking at the present system and its frailties. We also identify factors that are important in the development of any future system. Our proposed system is then detailed, along with its anticipated benefits and disadvantages.

Keywords

Public Key Infrastructure (PKI), Attribute Certificates, Electronic Signature, Encryption, Secure Sockets Layer (SSL), X.509, Electronic Prescription Processing.

Introduction

The UK NHS came into being in 1948 and since that time has provided fixed or zero cost medical services to all UK citizens. One of the fixed cost medical services is the UK drug prescription system controlled by a government organisation called the Prescription Pricing Authority (PPA). The NHS also provides free prescriptions to a large proportion of its clients in the form of exemptions for reasons such as age. With the recent production of a National Plan of Reform for the NHS [1] came a goal to adopt Electronic Prescribing by 2004 to replace the current paper based system. Paper prescriptions, in one form or another, were introduced in 1948 at the outset of the NHS

We define Electronic Prescription Processing (EPP) as *the electronic transmission and processing of medical information contained within medicinal prescriptions through all components of the prescription system, from the initial prescribing of the drugs, through dispensation to the patient, to the eventual close of transaction at some prescription-processing agent*[1].

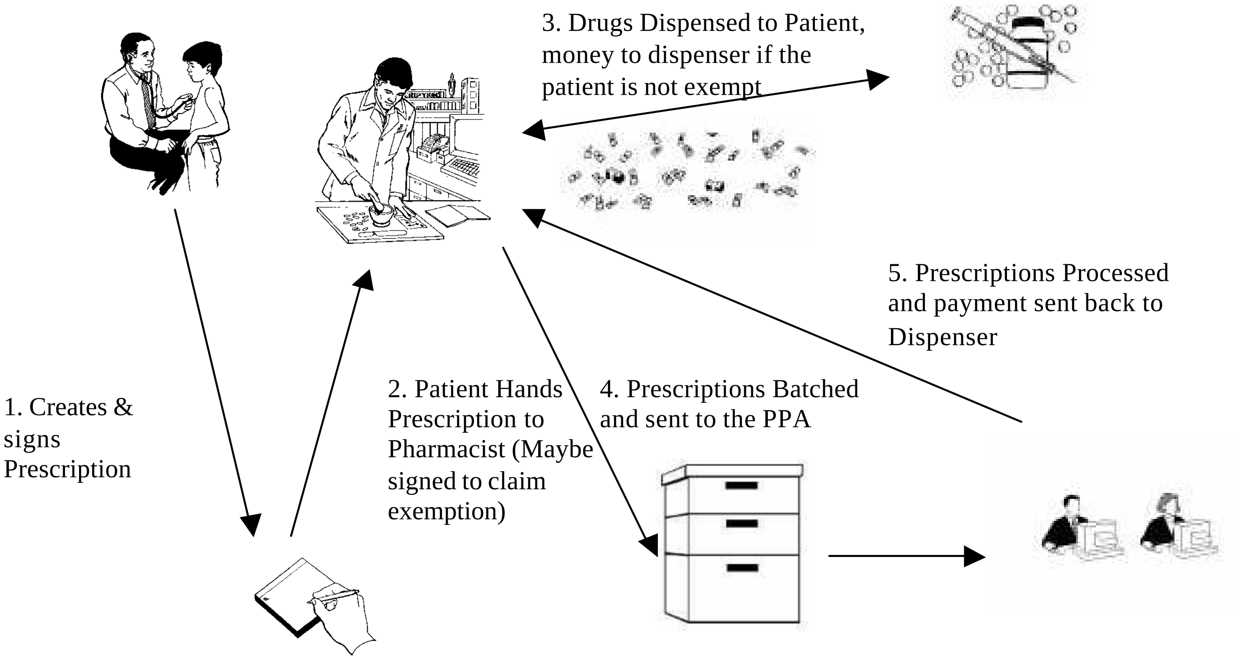
In this paper we set out our proposed electronic prescription processing system design, with the emphasis firmly placed on performance, scalability and security. In the early sections we aim to demonstrate just why an electronic prescribing system is required, by looking at the present paper based system and its failures. We also identify factors that are important in the development of any future system. Our proposed system is then detailed, along with its anticipated benefits and disadvantages.

Prescription Processing – The Present System

To explain the present prescribing system in the UK NHS (depicted pictorially in Figure 1) it is best to describe a general case scenario of a patient requiring unrestricted drugs (e.g. not drugs like Methadone for which there are UK controls on prescribing) on a visit to their family doctor. After assessment of the medicinal requirements of the patient the doctor writes or prints off a prescription on a special form called an FP10 [6]. FP10 prescription forms come in different sizes and colours according to its intended use e.g. by General Medical Practitioners, by General Dental Practitioners, or for controlled drugs etc. The doctor then signs the form by hand in ink.

[1] The processing agent is optional. The UK NHS uses a governmental processing agent in the form of the PPA.

Figure 1 An Example Of The Present Paper Based Prescribing System



The patient takes this paper prescription to any pharmacy in the country and signs it to claim any exemptions from prescription charges that they are entitled to. The drugs are dispensed to the patient and the Pharmacist either takes the standard prescription charge from the patient or performs checks on their exemption. The form remains with the Pharmacist until the end of the month. After this time the forms are sent in a batch to the PPA who deals with the administration of the system. The PPA provides payment to the pharmacies for the drugs dispensed and also checks claims for exemption where no evidence has been shown to the Pharmacist.

To gain a background insight into the present prescribing system, visits have been made to a number of local Pharmacists and the PPA. These visits have included tours to see how the present prescription processing system works in practice and discussions on the implications of electronic prescribing to the current business processes.

Problems with the Present System

Fraud

From current government documents [4] and information in the media [8] it is estimated that prescription fraud costs the NHS of the order of £70-100 million a year. The fraud is perpetuated at many different tiers of the system from the patient to the dispenser of the drugs and comes in a variety of forms. Two examples of these are described below:

Prescription Pad Theft –

"*a deputising locum obtained blank prescriptions from a practice and then scanned them into a computer along with a genuine signature of the GP. The computer was then used to generate prescriptions for high cost drugs which were obtained from a number of chemists*" [9]

Prescription pads are stolen from GP practices and bogus prescriptions are written or printed out on them. Current countermeasures involve the recording of prescription pad identification numbers and issuing warnings to pharmacies. In a busy pharmacy though a check against these numbers will be very rare. The only hope of detection really is in local pharmacies where they know the format of local GP's scripts and can recognise the signatures and therefore can identify differences.

Altered prescription dispensation –

"*Pharmacists have made significant amounts of money by substituting an expensive drug with a cheaper alternative, but the claim is made for the more expensive one. Alternatively, money can be made by making up prescriptions slightly short of the correct quantity, or indeed, by adding items to prescriptions or changing the amounts of the drugs prescribed*"[9]

When making up the items for dispensation, Pharmacist's may simply give to patients different quantities from those stated on the prescriptions. The surplus amounts of drugs can then either be sold on the black market or dispensed to other patients.

Measures have been introduced into the present system to counter fraud and the actual amount lost by fraud is diminishing [4], however, the integration of electronic prescribing is seen as another way of countering prescription fraud.

Data Integrity

It is estimated that 40 percent of all prescriptions in the USA require rework [45] with 5% of these requiring a phone call to the physician. We would suggest that in the UK the percentage would be of a similar proportion. EPP wouldn't completely remove the need for phone call clarification but with electronic scripts instead of often illegible hand-written scripts the requirement for calls should be reduced. Electronic scripts suggest that each prescriber will be using an electronic prescribing system. The many existing electronic prescribing systems will help with formulating the prescription so that the number of errors produced when generating the prescription should also be reduced. This will also help in the fight to reduce the number of hospital admissions caused by medication errors, recently stated in the UK to be one patient in every twenty admissions [20].

Administrative Workload

Each year the PPA processes an increasing number of prescriptions, with the figure reaching 578 million prescription items in 2001 [3] [25]. All of these come in batches each month from dispensaries all over the UK. Each script has to be input into the authorities computer system in order to calculate payment. The administrative burden is tremendous requiring a large number of data operators performing labour intensive, repetitive data input tasks that often result in entry errors. Indeed in a previous project we found input errors to be a significant factor in duplicate entry data systems [11]. The introduction of EPP should allow for a large reduction in the number of paper scripts processed by the PPA and a reduction in the amount of time taken to process the prescriptions accumulated over each monthly period. Indeed many pharmacists believe that the introduction of EPP will lead to a reduced payment period for dispensed drugs.

Efficiency

In general the present prescription processing system is reasonably efficient up until the actual processing of the prescriptions at the PPA. Prescribers and dispensers have particularly efficient internal practices that have evolved over a number of years. It is difficult to see how computerisation, especially a national prescription processing system, could bring any significant efficiency benefits to them. In order to be accepted by these stakeholders, one of the main objectives of any EPP system must be to ensure a lack of degradation of the efficiency of present working practices. From UK research conducted by Kember Associates [12] 60% of Pharmacists believed that the introduction of electronic prescribing would lead to timesavings within the dispensation process with 55% believing it would lead to shorter patient waiting times for their dispensed prescription. Such high expectations place additional demands on the implementation of EPP. One area where benefits may accrue from electronic processing could be improvements in the handling of repeat prescriptions.

Patient Exemptions / Identification

At present the emphasis for checking patient exemption from NHS charges and checking of the patient's identification is placed firmly on the Pharmacist. This weak control helps people who claim fraudulent benefits. It also puts increased pressure/stress on the Pharmacist by introducing confrontation into their working lives, since they have to ask patients questions such as "Have you got evidence of you age?" and "Can you prove that you have an exemption?" These types of questions automatically alienate their customers, indeed in some cases exemptions from charges may not be claimed because of customers reluctance to prove their circumstances or from lack of knowledge that they can claim exemption.

Electronic Prescription Processing Systems

Applications designed to electronically generate prescriptions have existed for a number of years with a large majority of practitioners in the UK now producing printed prescription forms [3]. However, no system exists in the UK for the Electronic Transmission of Prescriptions (ETP) to pharmacies and the PPA. Prior to the commencement of this study Pharmed [13] had planned for the trial introduction of one such system within the NHS. Hospital systems have been trialed within the Wirral Hospital trust [14] and the British government has demonstrated its commitment to the adoption of ETP, firstly by funding individual projects [15][16], and then in 2001, by approving the proposals of 3 commercial consortia to mount self-financed pilots [5].

Electronic prescribing is not just a UK phenomenon. Electronic prescription systems [17][18][19] linked to pharmacies exist in the USA but these are in small cluster groups of selected pharmacies and prescribers all signed up to the same system provider. Prescriptions within these systems are sent either by fax or electronic mail. In Denmark it is estimated that 35 per cent of prescriptions are sent electronically [20] and a project [21] on the impact of electronic prescription systems has also been carried out. In Germany research has taken place into the transfer of prescriptions and health information on a patient smart card [22].

The present UK Prescription Processing system generates "550 million pieces of paper per year between GP, Pharmacy and Pricing systems" [23], countless numbers of phone calls checking prescription validation and has a patient population of around sixty million. When these scaling factors are coupled with reliability, security, efficiency and are set against a changing background of patient identifying factors[2] the complexity of the problem begins to materialise.

Design of an Electronic Prescription Processing System

The basic system design consists of the three different 'users' of the system (Prescribers, Dispensers and the PPA) calling a common Application Programming Interface (API) called the Electronic Prescription Processing (EPP) API. The actual prescriptions within the system are stored as digitally

[2] The UK NHS is rapidly changing its practices to deal more effectively with data protection laws whereby restrictions on identifying factors for patient information are now being imposed. E.g. not identified by patient name.

signed certificates within a Lightweight Directory Access Protocol (LDAP) directory [24]. LDAP was chosen because it is designed to store digitally signed certificates and is a basic component of a Public Key Infrastructure (see later). The prescription directory is distributed between the regions for scalability reasons, as a centralised directory would be required to deal with upwards of 500,000,000 prescriptions a year (see the directory sizing section). Other directories also exist. A patient directory holds patient details, such as their NHS number and any particular exemptions they may have, and a national NHS directory contains the details of prescribers, dispensers and regulatory bodies.

The electronic prescription is encapsulated in a construct called an attribute certificate [26] and this structure contains the electronic signature of the prescriber. The security of the system is described in greater detail in the following section of this paper.

To explain the design in detail it is again useful to go through a typical scenario. The patient would visit their GP and explain their illness. The GP would search through his local prescribing application database for the patient's electronic record. This record would contain the patient's NHS number and other details such as age and previous prescriptions etc. The GP prepares the prescription on his PC, using existing electronic prescribing software that contains details of all current drugs recognised by the NHS. When finished, the patient optionally may be asked if they would like to name a pharmacy that they wish to go to for the prescribed drugs. However neither the GP nor the patient is required to do this, as freedom of choice of pharmacy is retained. The advantage of choosing a pharmacy at this stage is that the pharmacy can be notified in advance, so that the prescription can be dispensed prior to patient arrival, thereby reducing their waiting time. The electronic prescription is generated within the application, and the GP is asked to digitally sign it. The process of digital signing only requires the GP to enter a secret password or PIN and so is no more difficult than hand signing. The rest of the digital signing process is carried out automatically by the application. The system then connects to the local regional LDAP directory and the prescription is stored as a unique entry, referenced by its Prescription Unique Identifier (PUID). The doctor gives the patient a print out "comfort" slip that contains the patient's name, NHS number and list of drugs prescribed and also a barcode containing the PUID. The comfort slip denoting the prescription is merely a confirmation note, which is used for fast lookup by pharmacies using a barcode scanner. It can also be used as a pharmacy picking[3] list.

[3] Pharmacists often carry the paper prescriptions around their pharmacy with them in order to know which drugs to dispense. Therefore a completely computerised system would not be accepted by a large majority of them unless a paper copy of the prescription was available to them.

The prescription is stored in one of the many regional LDAP directories, depending upon which GP the patient visited. Each pharmacy system is capable of contacting all of these directories, so that if the patient travels between prescribing and dispensing he is not disadvantaged. The patient visits a pharmacy of choice and gives the Dispenser the comfort slip or their name and address. If the latter, the Dispenser will have to search the regional LDAP directories looking for the patient's prescription. If the comfort slip is given the barcode uniquely identifies the patient and prescription within the correct regional directory, thereby speeding up retrieval. The prescription is retrieved, decoded and displayed then the Prescriber's signature is verified. Displaying the prescription before signature verification allows the Dispenser to start dispensing the prescription instead of waiting for the verification (checking) of the signature to complete. In the rare cases where the signature verification fails (which means that the prescription has been tampered with or an error has occurred) the Dispenser will be notified before they finally dispense the drugs to the patient. In the vast majority of cases the signature should prove to be valid and therefore it is better to check the signature during a period of low processing while the Dispenser is picking the drugs for the prescription. The Dispenser then adds to the prescription the dispensation information and digitally signs the updated document and stores it back in the LDAP directory from whence it came.

When the PPA requests all the dispensed prescriptions they would scan each of the regional directories. All dispensed prescriptions will be retrieved and verification would then take place after retrieval so as not to slow down the retrieval process. Once retrieved, the PPA would then delete or move to backup the original prescriptions and the dispensed prescriptions from the directory.

This is a basic summary of the system design and describes a typical prescription transaction. There are many other factors that have been considered in the research, for example patient signing, controlled drugs distribution and the problems caused by integration of the electronic system with the paper based system. Some of these are detailed in following sections of this paper.

EPP Security Requirements

Medical professionals have a legal obligation to protect the confidentiality of patient information [27] [31]. Therefore 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 the electronic prescription processing can access the system. Secure authentication (assurance of identity) and authorisation (confirmation of privileges) of such professionals is consequently a requirement of the system. Further, how do we know that a third party has not subsequently altered a prescription after generation? Consequently, we are required to provide an integrity mechanism (assurance that the prescription has not been altered) to protect the prescription against modification. Finally, the system should be able to ensure that repudiation of origin (denial of ownership) is difficult to achieve.

EPP Security Technologies

Authenticity, integrity, non-repudiation and confidentiality are all security services that can be provided directly or indirectly by a Public Key Infrastructure (PKI) [28]. So to provide all the security services required by an Electronic Prescription Processing System it is expected that a PKI will be necessary. We have used the PKI provided by Entrust Inc. to set up our demonstrable version of the system but any PKI could be used in place of this.

Confidentiality is provided by cryptography. Symmetric cryptographic systems operate on a basis of a shared token (key). Both parties in a symmetric key transaction have the same encryption and decryption key or have keys that can be easily derived from each other. Such systems have been in existence for thousands of years ranging from early examples such as the Caesar Cipher [34] to more modern representations such as DES [35], CAST-128 [36] and AES [30]. Symmetric ciphers possess some very desirable qualities such as speed of encryption/decryption (encoding/decoding of information) and small key sizes. However they also have a disadvantage, which is how to distribute the initial key to the communicating parties. This becomes a significant problem when large numbers of users are involved.

The principles of asymmetric cryptography have only recently been determined through the work of Whitfield Diffie and Martin Hellman in the mid 1970's [37]. Asymmetric cryptographic exchanges require the production of separate keys for encryption and decryption where the keys cannot be determined from one another. One key, the private key, is only known to one party, whilst the second key, the public key, can be made available to anyone. The public key can be published in a key server or can be sent directly to the remote parties involved in the transactions. In order to know that a public key is genuine and has not been tampered with, the public key can be published as part of a data structure called an X.509 public key certificate [26]. This certificate contains information about the public key (e.g. what cryptographic functions the key can be used for and its validity period), the owner of the key pair, and details about the certification authority (CA) that is attesting to this ownership. The whole data structure is digitally signed by the CA. Usually validity periods for public key certificates are fairly long (of the order of years) because the authentication and issuing process can be quite lengthy. Consequently you wouldn't want to be continually changing your electronic identity (as identified by the public key certificate). When sending encrypted messages via a PKI both symmetric and asymmetric encryption technologies are used. The message is encrypted using a new one-off symmetric key, to gain the benefit of encryption speed, then the symmetric key is encrypted using the public key of the recipient, in order to confidentially distribute the key to the recipient.

A relatively new development in the world of cryptography is the introduction of attribute certificates. These certificates allow for the allocation of privileges (or indeed any attributes) to an electronic entity. An X.509 attribute certificate [26], see Figure 2, consists of a data structure called Attribute Certificate Information, see Figure 3, which contains details about the issuer, the holder, the times of validity etc. as well as the embedded attribute(s). In our EPP design the prescription is stored as an attribute within Attribute Certificate Information, the holder is the patient and the issuer is the prescriber. This Attribute Certificate Information structure is then digitally signed by the issuer and the signature method used and value of the signature are all amalgamated together to form the attribute certificate.

Figure 2 Attribute Certificate

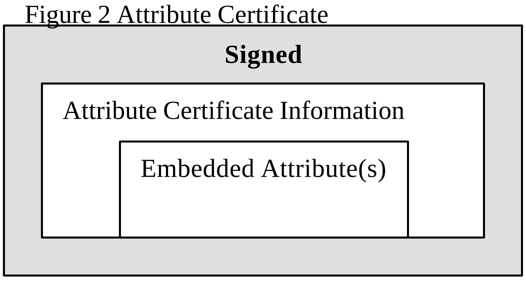


Figure 3Attribute Certificate Information

```
Attribute Certificate Info ::= SEQUENCE {
        version                    AttCertVersion,
        holder                     Holder,
        issuer                     Issuer,
        signature                  AlgorithmIdentifier,
        attrCertValidityPeriod     AttCertValidityPeriod,
        attributes                 SEQUENCE of Attribute,
        issuerUniqueID             UniqueIdentifier OPTIONAL,
        extensions                 Extensions OPTIONAL
}
```

Attribute certificates have the properties of integrity, authenticity and non-repudiation, but not confidentiality. In many present systems, encrypted links are used to provide confidentiality during transfer over the Internet, using mechanisms such as Transport Layer Security (TLS) [39] or Secure Sockets Layer (SSL) [40]. Our design similarly allows for encrypted links between all associated entities. However, we can also provide for the transfer of encrypted prescriptions without the need for a protected link. In the latter case all parties would need to be specified prior to encryption (thereby requiring the patient to choose which pharmacy they wish to pick up the prescription from). The prescription would be encrypted so that only the chosen recipients (the pharmacist, the PPA, the prescriber and optionally the patient) can subsequently have access to it. Later in our research we plan to evaluate the performance and usability of these two alternative encryption methods (encrypted links vs. encrypted prescriptions).

Authorisation / Privilege Management

Other project work within our security research group at Salford (http:\\sec.isi.salford.ac.uk) has been focused on building a Privilege Management Infrastructure for Authorisation purposes (PERMIS) [41]. PERMIS is a trust management infrastructure according to the definition given by Blaze [2]. A trust management system defines privileges, actions and the various parties involved, and a policy that says which parties are trusted to perform which actions on which target objects. A decision engine is built that enforces the policy. The PERMIS infrastructure is general purpose and caters for the granting and verification of privileges in relation to any electronic transaction. The infrastructure is role based, whereby the various parties are allocated roles, and the roles are given privileges. The roles are stored in attribute certificates. We were able to integrate PERMIS into our design for EPP, to provide for the secure authorisation of the various parties (e.g. the role of Doctor is allocated to a GP, and Doctors are given the privilege to prescribe). This also allows us to provide a more effective solution for handling patient exemptions to prescription charges.

Prescriber /Dispenser Privileges

The overseer of the UK NHS, which to all intents and purposes is the Secretary of State for Health in the UK Government, would generate and electronically sign a PERMIS policy stipulating who can carry out which actions in the Prescription Processing System[4]. For example the policy might state that the General Medical Council is trusted to allocate the role of Doctor to people, and that anyone with the role of Doctor is allowed to prescribe. Therefore a signatory member of the General Medical Council indirectly gives all General Practitioners in the UK NHS the right to prescribe when they are issued with a Doctor role attribute certificate. When the GP is generating a prescription the EPP API calls the PERMIS decision engine to determine if the GP is authorised to do so according to the rules laid down in the policy. As long as the prescriber has the role of Doctor, they will have been granted permission

[4] It need not be the Secretary of State himself who signs the policy, but could be anyone authorised by him. The system would be told who the authorised trusted person is.

to prescribe and they will be allowed access to the operation to generate an electronic prescription and send it to the prescription directory for storage. In the case of Dispensers, they are given the role of Pharmacist by a trusted professional from the Royal Pharmaceutical Society. The policy would state that anyone with a role of Pharmacist has the privilege to retrieve prescriptions from the prescription directory and to view them, and then subsequently to submit the dispensed prescription back to the prescription directory. The EPP API will call the PERMIS decision engine in order to enforce these rules.

Exemption Handling

Exemptions within the NHS can be for a wide variety of purposes and can be for varying amounts of time. For example:

after the age of 65 or before the age of 16 patients are exempt from all prescription charges

or

while patients are on national supported benefit they are exempt from all charges.

Within our design for electronic prescriptions we propose that these exemptions would become patient roles, and the policy would state what privileges these roles conferred. The roles, in the form of attribute certificates, could either be stored within a national system or on a smart card issued to and carried by the patient. This will alleviate the dispenser from the job of checking for proof of exemption. Approved bodies would generate the exemption roles for certain validity periods. For example, after the age of 65 patients could be issued with an exemption attribute certificate for the rest of their lives or every set period of time whilst on benefit an exemption certificate could be issued to a claimant e.g. quarterly or annually. The EPP API calls the PERMIS decision engine in order to determine and enforce eligibility for free prescriptions.

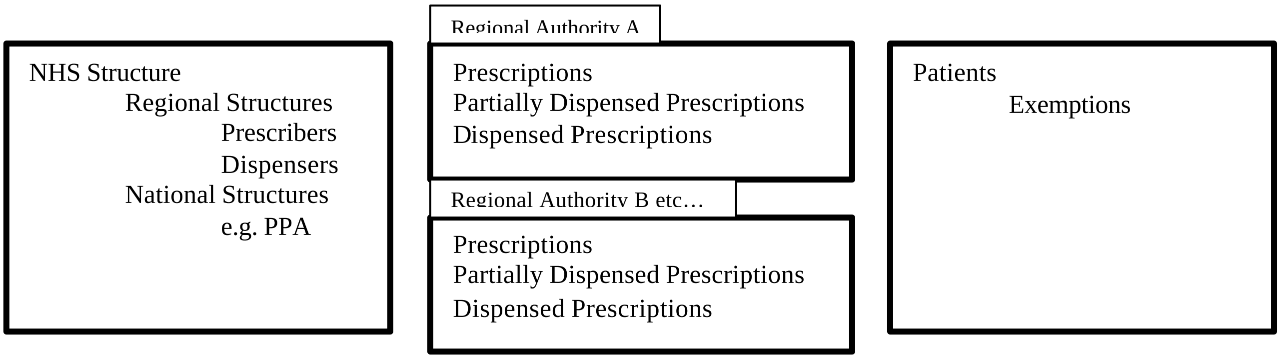
Specification of the Electronic Prescription

It is essential to ensure that any electronic prescription processing system is optimised to provide the most efficient system possible, due to the limited time available to prescribers and dispensers, and the volume of prescriptions issued annually. Therefore it is imperative to ensure that the prescription is specified in a language and form which provides the most efficient data transfer possible. As part of our research into the design of an EPP system we have produced a comparison of two such data transfer syntaxes [43], Abstract Syntax Notation One (ASN.1) [32] with its Basic Encoding Rules (BER) [33] and eXtensible Markup Language (XML) [38]. The comparison was prompted by the impending adoption of XML as the protocol for UK electronic government services including ETP. We compared the transfer of three different sizes of data structure specified in both transfer syntaxes, all with and without data security (digital signatures). We found ASN.1 BER to be the most efficient transfer syntax by approximately an order of magnitude when used to specify a digitally signed prescription [43]. Earlier research by our group [7] [11] causes us to believe that performance will be a critical factor in EPP system success.

Directory Sizing

With over 500 million prescriptions to process a year, we believe that a national centralised prescription store will be an expensive option for such a large scale EPP system. Performance of such a centralised system would be major delimiting factor in the introduction of EPP. It would also be a central point of failure. Therefore we propose a distributed prescription store as depicted in figure 4.

Figure 4 Directory Structure



The system comprises one centralised directory that holds details of all the NHS participants. Another holds details of all patients and their exemptions (although this also could be distributed or replaced by each patient having their own smart card). The prescription directory is distributed throughout the NHS regions. Precisely how distributed is a configuration option but we suggest at a maximum each directory should hold no more than 10 million prescriptions (taking into account a prescription's expiry period). In fact our design is such that in the extreme the prescription directory could even be distributed down to servers within each prescriber's surgery. However, we are not proposing this, as it would cause large problems in terms of system administration for each surgery. We are currently experimenting with different distribution scenarios in order to determine an optimal distribution policy.

Data Protection

The UK NHS is going through a period of data protection review with recommendations outlined within the Caldicott Report [42]. The key issue is how much personal information should practitioners at different levels within the NHS see for each patient. Everybody in the UK has a NHS identification number and in transaction data flows it is recommended that this be used instead of the patient's name. There are other systems that enable practitioners to search using the patient's name and address to find their NHS identification number, but the use of the NHS ID provides a suitable level of abstraction. Our EPP system is designed to use NHS IDs in line with the Caldicott recommendations. Our system also allows for prescription data to be encrypted within the directory store should the patient request it, or policy require it, as long as the patient chooses a pharmacist to decrypt it or the patient has their own NHS personal smart card holding their decryption key.

Patient Identification / Controlled Drugs

Within the UK NHS certain medications are designated controlled drugs. These drugs are subject to the prescription requirements of the Misuse of Drugs Regulations (1985). They are drugs that are likely to cause addiction, or for which there is concern about abuse, for example the heroin substitute methadone. For these types of drugs it is extremely important that they are prescribed and dispensed to the right people. One solution could be that a photograph of the individual requiring controlled drugs could be stored either within the patient's directory entry or on their smart card. This would provide prescribers and dispensers with a point of reference for patient identification. The photograph need not necessarily be of the person's face. It could be of their hand written signature or some other unique defining feature.

Expedited Prescriptions

In the present processing system patients can take their prescription to any dispensary and receive their designated drugs subject to the drugs being in stock. The government wishes patients to have the same choice when they have been given an electronic prescription. This will help to ensure that there is no monopolisation of either a local dispensary market or the national market. However, patients may like to be able to designate in advance a pharmacy where they will pick up their prescription. This allows our system to send an electronic notification that a prescription is awaiting dispensation directly to the pharmacy (via secure email S/MIME [44]). This will enable pharmacies to dispense a prescription before the patient arrives leading to patients spending less time waiting for their medication to be dispensed.

Proposed Benefits and Problems with our Design

We believe that the adoption of electronic prescribing within the NHS will cause a multitude of different problems for system designers to overcome. Our system will counter a large proportion of the fraud within the NHS, for example the stealing of prescription forms, fraudulent signatures and altered prescriptions. However some fraud will still be hard to overcome such as the dispensation of fraudulent amounts of drugs or conspiracy between a prescriber and dispenser. The electronic system may also provide the capability for new fraud, caused for example by the theft of electronic signature tokens or authentication mechanisms (e.g. passwords). An operational system would require a secure transaction logging system for audit purposes, a facility we have not yet built.

The current paper system is optimised for prescribers and dispensers, so the introduction of any new system might bring an expected slowdown during the initial period whilst operators become used to working with the new system. Therefore performance optimisation before roll out is a major aspect of any design.

Overall the main benefits and drawbacks of the system, apart from a reduction of fraud, can be categorised according to the different user groups of the system (Patients, Prescribers, Dispensers and the PPA).

Patients

They will not perceive any immediate difference in the new system apart from the different design of the paper prescription (with barcode). However, they will find that by electing to go to a particular pharmacist, their dispensed prescription may be ready on arrival. Also the new system will deal with some patient exemptions automatically via the use of the PERMIS API and built in privileges. Therefore these patients will benefit from not having to prove their exemption at the pharmacy.

Prescribers

Prescribers are the least inconvenienced by the new system. They should see little difference in the new system, except that now they will have to enter a password or PIN number[5] in order for the electronic prescription to be digitally signed. They may also notice some performance degradation of their

[5] Other forms of authentication could also be used and indeed may be recommended, as password schemes can easily be overcome [10].

Prescribing application as the prescription is digitally signed and sent to the directory. An electronic system also allows additional modules to be built, for example, to notify prescribers when a prescription has actually been dispensed, a feature not available in paper based prescribing. Finally, an enhanced user interface (not provided by our project) should be able to store the written prescriptions and automatically reschedule them for repeat prescribing. Since repeat prescriptions account for 70% of GP prescriptions, this should be a significant realisable benefit from electronic prescribing (although it is recognised that some systems already have this feature today).

Dispensers

Dispensers are the high-risk users in this system. They may or may not benefit from electronic prescriptions depending upon the functionality of their current system. Scanning in prescriptions should be quicker than entering prescription details by hand, but the electronic prescription may still require some drug selection and data entering. Also the speed of retrieval from the regional directory will be a critical success factor we believe. Dispensers should benefit from system knowledge of patient exemptions, and from the prescriptions going straight to the PPA. Hopefully this will lead to less conflict with patients and earlier payments for their services. It should also allow additional modules to be built to correlate payments with dispensed drugs, something the dispensers are not able to do today. They simply have to trust that the PPA gives them all their dues. However, for some prescribing, as doctors migrate to the electronic system, and as a backup for electronic system failure, paper based prescription processing is expected to be required for some time (maybe forever). Consequently dispensers will have to work with the two systems running in parallel, which will bring its own problems and frustrations.

The PPA

The PPA is likely to be the main beneficiary from electronic prescriptions. The reduction in the amount of paper documents they have to handle will lead to reduced transcription administration at the PPA and automation of their business processes. It will also allow them to better forecast trends in drug prescribing, and plan for the future. Apart from the reduction of fraud, this could be one of the main benefits of Electronic Prescription Processing to the NHS.

The system at the moment is optimised for handling paper prescriptions, so the introduction of a new system with its expected teething problems is going to cause negative effects in the interim period until operators become used to working with the new system. Further, the PPA will have to operate paper and electronic systems in parallel for a significant period of time (if not forever) whilst GPs migrate to the new system, and as a fallback mechanism in times of crisis.

Integration with End Systems

At the moment there exists a large number of disparate applications used to process prescriptions. The NHS and indeed many large organisations refuse to be 'tied-in' to any one system provider. These applications provide a wide variety of functions for their users such as prescribing help and stock control. A number of these services are already provided by links into separate Application Programming Interfaces (API) provided by third party organisations such as links into the Prodigy [29] system for primary care prescribers. Therefore we have built an API in Java that is designed to facilitate the introduction of electronic prescription processing into any existing electronic prescribing application in use in the UK NHS. The API itself is easy to use, and will be detailed in a subsequent research paper. We will also be detailing performance results once laboratory tests are completed.

Summary

Our system design has the capability for transforming the paper based prescription system of the UK NHS into a secure computerised system. The API for the design described in this paper has been implemented by our research group and built into a prototype system. Integration of the EPP API into operational GP and pharmacist end user systems must be done by the current suppliers of these systems.

Overall the main benefits apart from reduction of fraud can be categorised by the different user groups of the system (Patients, Prescribers, Dispensers and the PPA). It is believed that as long as the system is easy to use and performance matches or exceeds that of the current system then the user groups will not experience any significant adverse effects in the new system, and may experience real benefits. Patients and dispensers should benefit from some exemptions being handled automatically. Dispensers should benefit from the prescriptions going straight to the PPA and hopefully this will lead to earlier payments for their services. Add on features like the feedback of dispensed prescriptions to prescribers and the correlation of payments received with claims made by the dispensers, should provide users with a higher quality of information. The main beneficiaries however will be the PPA, with a significantly reduced administrative load, and the NHS with a reduction in fraud.

The emphasis of our research has been to design a scalable, secure system for the transport of electronic prescriptions between all the parties involved. Over the next year we will be concentrating on performance optimisation, plus scalability tests to ensure that the system will have the capacity to cater for the entire population of the UK. From these results and simulation tests in the laboratory we should be able to make some interesting conclusions on the adoption of ETP/EPP within the UK NHS.

Acknowledgements

This research was funded by the UK EPSRC under grant number GR/M83483 . The authors would also like to thank Entrust Inc. for making their PKI security software available to the university on preferential terms.

References

[1] The NHS Plan, http://www.nhs.uk/nationalplan/nhsplan.htm, February 21 2002

[2] Blaze, M., Feigenbaum, J., Ioannidis, J. “The KeyNote Trust-Management System Version 2”, RFC 2704, September 1999

[3] http://www.doh.gov.uk/pharmacy/FAQs.htm (June 2002)

[4] Department of Health “Directorate of Counter Fraud Services, Countering Fraud in the NHS: Protecting Resources for Patients, 1999-2001 Performance Statistics”, Jan 2002. http://www.doh.gov.uk/dcfs/dcfsperfstats9901.pdf (June 2002)

[5] Electronic Transmission of Prescriptions http://www.doh.gov.uk/pharmacy/etp.htm (June 2002)

[6] UK Prescription Documents, http://www.ppa.org.uk/education/fp10.htm (June 2002)

[7] D. W. Chadwick, C. Carroll, S. Harvey, J. New, A. J. Young. “Experiences of Using a Public Key Infrastructure to Access Patient Confidential Data over the Internet”, Proceedings of the 35th Annual Hawaii International Conference on System Sciences 2002 (HICCS 2002)

[8] British Broadcasting Corporation (BBC), BBC Panorama Programme, July 1997

[9] http://www.doh.gov.uk/dcfs/examples.htm (June 2002)

[10] Granger, S. (2002), The Simplest Security: A Guide to Better Password Practices, http://online.securityfocus.com/infocus/1537 (June 2002)

[11] Chadwick, D.W., New, J.P., McDowell, D.M. and Mundy, D.P. 2001, “Providing Secure Access to Confidential Patient Information Detailing Diabetic Condition”, Proceedings of the International Conference on Internet Computing 2001 Volume I, pp 535-541.

[12] Kember Associates (July 1999), Pharmacists' Attitudes to Electronic Prescribing, http://www.pharmed.co.uk/text/reseach2.html (May 2002)

[13] Pharmed, http://www.pharmed.co.uk, June 2002

[14] Moore, J., Farrar, K., Hughes, D., Spours, A., "Electronic Prescribing – The Perfect Prescription", The British Journal of Healthcare Computing and Information Management, 1996 13(4):25-27

[15] Chemist & Druggist, "£2M for electronic prescribing project in Northern Ireland", May 8, 1999 p6

[16] Chemist & Druggist, "£4M promised for Scottish electronic prescribing", 1999, 251:6

[17] Pocketscript, http://www.pocketscript.com/

[18] Ephysician, http://www.ephysician.com/

[19] AllScripts, http://www.allscripts.com/ahcs/index.htm

[20] H. Middleton, "Electronically Transmitted Prescriptions – a good idea", The Pharmaceutical Journal, Vol 265 No 7107 p172-176, July 2000

[21] Moorman, P.W, Bernstein, K. (editors). The CoCo project report. Odense: Danish Centre for Health Telematics, 1999

[22] Eckstein, L., Struif, B. Electronic prescription and Medication Documentation on a Patient Data Card – The SmartCard – Project of the ABDA, German National Research Center for Information Technology (GMD) and Institute for Secure Telecooperation (SIT), November 1999

[23] Strange, M. Design principles for the secure messaging of prescriptions from GPs to pharmacies, Primary Health Care Specialist Group of the British Computer Society, Proceedings of the Annual Conference, Cambridge 1999

[24] Wahl, M., Howes, T., Kille, S. "Lightweight Directory Access Protocol (v3)", RFC 2251, Dec. 1997

[25] PPA, "PPA Annual Report 2001", http://www.ppa.org.uk/pdfs/PPA_An_Rep_00-01.pdf, January 2002

[26] ISO/ITU-T Rec. X.509 (2000) The Directory: Authentication Framework

[27] UK Government, "Data Protection Act 1998"

[28] Adams, C., Lloyd, S. (1999). "Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations". Macmillan Technical Publishing, 1999

[29] Prodigy, http://www.prodigy.nhs.uk/, January 2002

[30] Advanced Encryption Standard. See http://csrc.nist.gov/encryption/aes/

[31] Protection and Use of Patient Information. http://www.doh.gov.uk/ipu/confiden/protect (January 2002)

[32] ITU-T, X.680 : ITU-T Recommendation X.680 (1997) | ISO/IEC 8824-1:1998, Information Technology - Abstract Syntax Notation One (ASN.1): Specification of Basic Notation

[33] ITU-T, X.690 : ITU-T Recommendation X.690 (1997) Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

[34] Stallings, W., Cryptography and network security : principles and practice Second Edition, London, Prentice Hall, 1999

[35] National Bureau of Standards, "Data Encryption Standard", FIPS PUB 46, January 1977

[36] Adams, C. (1997), "The CAST-128 Encryption Algorithm", RFC2144

[37] Diffie, W., Hellman M. E., "Privacy and Authentication: An Introduction to Cryptography", Proc. of the IEEE, Vol 67 No 3, pp 397-427, Mar 1979 (12/2/00)

[38] Extensible Markup Language (XML) 1.0 (Second Edition), http://www.w3.org/TR/REC-xml, 6 October 2000

[39] Dierks. T, Allen, C., "The TLS Protocol Version 1.0.", RFC2246, January 1999.

[40] A. Frier, P. Karlton, and P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.

[41] 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. pp 135-140.

[42] The Caldicott Committee, Report on the review of patient-identifiable information, December 1997, http://www.doh.gov.uk/confiden/crep.htm, 27 May 2002

[43] Mundy, D.P, Chadwick, D.W (2002), Performance Comparisons of Abstract Syntax Notation One (ASN.1) vs. eXtensible Markup Language (XML), submitted to Internet Computing Journal, May 2002

[44] S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka, RFC 2311 S/MIME Version 2 Message Specification, March 1998

[45] Liew, A. E-prescribing applications benefit patients, providers and health plans, Arthur Anderson Consultant Report, www.arthurandersen.com/resource2.nsf/ vAttachLU/HI_HotERx/$File/eRx.PDF