(T&F) TMIF100292

MED. INFORM. (MONTH 2003) VOL. 0, NO. 0, 00–00

Taylor & Francis
healthsciences

Security issues in the electronic transmission of prescriptions

D. P. MUNDY* and D. W. CHADWICK

IS Institute, University of Salford, The Crescent, Salford, M5 4WT, UK

Abstract. The UK government has stated within its plan of reform for the National Health Service that a secure system for the Electronic Transfer of Prescriptions will be available by 2004. The objectives of this paper are to highlight the significant barriers faced in securing an ETP system, to provide a critical analysis of the security mechanisms in the models currently being piloted and to suggest an alternative revised model which overcomes the identified deficiencies and security hurdles. To identify the significant security issues relevant to the adoption of ETP, the authors have combined their analysis of present prescription processing practice with their knowledge of computer security. The authors identify and describe how the issues of patient confidentiality, authorization, identity authentication, audit, scalability, availability and reliability are significant barriers to the adoption of ETP, particularly if they effect ease of use. The paper's contribution to the field of ETP is to suggest solutions to each of the identified security issues and to combine the solutions together in a revised and developed model.

Keywords: Authentication; Electronic signatures; Encryption; Electronic Transmission of Prescriptions (ETP); Public Key Infrastructure (PKI); X.509

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 500 million prescriptions per year which is far in excess of what any present day ETP system handles. A centralized body called the Prescription Pricing Authority (PPA) processes payment for prescriptions for the UK NHS and all electronic prescriptions would need to be sent to the PPA for processing.

Health professionals have a legal and ethical obligation to protect the confidentiality of patient information [4,5]. Therefore the unprotected transfer of plain textual prescriptions across insecure networks is clearly not an option. It is also necessary to ensure that only health professionals involved in ETP can access the system and the prescriptions within it. Clearly the security of the electronic information and of the system itself will be a key factor in the success or failure of ETP. In this paper we present the main electronic security issues that need to be adequately addressed in order for the introduction of ETP in the UK NHS to be successful.

However, introducing security into systems can often make them less convenient to use – consider for example putting locks on doors or security guards on the access to buildings. Generally the more secure something is, the less easy it is to use. Therefore if security is to be adequately addressed in order for ETP to be successful, there has to be a delicate balance drawn between the strength of the secur-

*Author for correspondence; e-mail: d.mundy@salford.ac.uk

Medical Informatics & The Internet in Medicine ISSN 1463-9238 print/ISSN 1464-5238 online © 2003 Taylor and Francis Ltd
http://www.tandf.co.uk/journals
DOI: 10.1080/1463923031000162167 5

ity and the inconvenience of using ETP to its users, or they are likely to reject it. Too weak a security infrastructure would cause the professionals to refuse to use it. Too strong a security infrastructure that makes the system time consuming or awkward to use, is likely to cause some or all of the users to prefer to continue using the existing paper based system.

After introducing the security issues, we then describe the various ETP models involved in the current UK government trials [6], as well as other systems that have undergone trials elsewhere, and analyse each of them from a security and user convenience perspective. Finally we present the model developed by ourselves [7] that has been designed to overcome the security issues presented here whilst not unnecessarily inconveniencing the users.

2. The existing paper-based system

Before considering ETP, it is necessary to appreciate the current paper-based system and its strengths and weaknesses. A patient has a consultation with a prescribing doctor, and is handed a paper prescription at the end of the consultation, written on a NHS FP10 prescription form. The doctor may have taken handwritten notes during the consultation and handwritten the prescription, or, as is increasingly likely, made notes on a PC-based patient management system, which has access to a drugs database and allows the prescription to be constructed on the PC and printed out on the attached printer. 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. It will usually also note contra-indications and combinatorial effects of the prescription cocktail. 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 and they are delivered to the PPA in Newcastle once a month.

We can immediately see a number of benefits with the existing system:

(i) the patient is physically given a prescription by the GP so they feel satisfied with the fact that drugs have been prescribed and know that the consultation is over (Noted from comments made by speakers at the PPA Conference, 2003 and focus group sessions run by the authors [8]).
(ii) the patient is free to go to any pharmacy of their choosing.
(iii) the system is easy to use and understand. The doctor, who is short of time, has a minimum of fuss in prescribing.
(iv) the system is resilient to technology failures and can fall back to an entirely paper-based system.
(v) the system is confidential, as only the patient and his professionals see the prescription.

There are of course many disadvantages with the paper based system:

(i) the doctor's handwriting may be illegible to the pharmacist.
(ii) the paper prescription could be lost or damaged by the patient.
(iii) the entitlement to free prescriptions is open to abuse.
(iv) the pharmacist has to re-enter all the details into his PC system by hand, giving potential rise to re-keying errors.
(v) the PPA has to re-enter all their details into their system in Newcastle, giving potential rise to re-keying errors.
(vi) the pharmacist has no way of knowing if they have been fully recompensed by the PPA for the prescriptions they have dispensed.
(vii) the doctor never knows if the patient has been to a pharmacist to have the drugs dispensed.
(viii) theft of NHS FP10 prescription forms can lead to the theft of drugs.
(ix) GPs and pharmacists can collude to defraud the NHS by prescribing drugs for dead patients or well people.

An ideal ETP system would counter the above disadvantages whilst retaining the advantages of the paper-based system.

3. Security issues in ETP

There are a number of security issues that need to be considered for the ETP, irrespective of the actual model employed.

3.1. *Patient confidentiality*

By this, we mean ensuring that both patient and prescribing details are not made available to unauthorized parties, either singularly or collectively. In the electronic world data confidentiality can be provided by either using a private network with tightly controlled access, or by data encryption techniques, or both. If a private network is to be employed instead of encryption, then we need to be sure that only authorized people can access the network. All access terminals, computers, cables and network ports will need to be in physically secured areas to ensure that unauthorized people cannot tap into the network. Authorized users will also need to be educated to ensure that they don't willingly or mistakenly connect the private network to a public one, thereby breaching its privacy. Clearly maintaining totally secure private networks is very difficult, and needs to be carefully managed. Consequently there is a high cost associated with this.

Encryption techniques allow confidential data to be carried across public networks such as the Internet, providing of course that the encryption mechanism is strong enough to prevent unauthorized disclosure of the contents. There are two types of encryption, symmetric and asymmetric. In the former case the same key is used to encrypt and decrypt the data, in the latter case different keys are used to encrypt and decrypt the data. Symmetric encryption systems have been in existence for thousands of years ranging from early examples such as the Caesar Cipher [9] to more modern algorithms such as DES [10], CAST-128 [11] and AES [12]. The latter symmetric ciphers possess some very desirable qualities such as the strength of their encryption algorithms, the speed of the encryption/decryption processes (encoding/decoding of information) and relatively small key sizes to en-

sure strong encryption. (A 16-byte key for example has 3.4×10^{38} combinations, which is more seconds than the universe has been in existence.) However they also have a disadvantage, which is how to distribute the secret key to the communicating parties. This becomes a significant problem when large numbers of users are involved such as ETP.

Asymmetric cryptography on the other hand is a relatively recent invention through the work of Whitfield Diffie and Martin Hellman in the mid 1970s [13]. Asymmetric cryptography requires the production of two separate keys, one for encryption and the other for decryption, where the two keys cannot reasonably be determined from each another. One key, the private decryption key, is only known to the recipient of confidential information, whilst the other key, the public encryption key, is made available to anyone who wishes to send a confidential message to the holder of the private key. 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 [14]. This certificate contains information about the public key (e.g. its validity period, and what cryptographic functions the key can be used for), the owner of the corresponding private key, and details about the certification authority (CA) or Trusted Third Party (TTP) that is attesting to this ownership. The whole data structure is digitally signed by the CA thereby ensuring its integrity. Usually the validity periods for public key certificates are fairly long (of the order of years) because the issuing process can be quite lengthy. A full description of X.509 certificates and TTPs is given in [15].

When sending encrypted messages over networks, typically both symmetric and asymmetric encryption technologies are used together. The message is usually 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(s) of the recipient(s), in order to confidentially distribute the symmetric key to the recipient(s).

If encryption is to be employed in ETP then thought has to go into key distribution, i.e. which recipients should have access to the decryption keys (e.g. should it be the patient, the pharmacist, a group of pharmacists, the prescriber or a combination of these). We also need to cater for both normal and extraordinary situations so that a patient is not left with an undecipherable block of electronic data that cannot be used. Further, if encryption is to be employed, should it only be whilst the prescription is being electronically transferred over an insecure network, and not during any intermediate storage stages (assuming there are some, and that these are secure), or should it be for the entire duration from when the prescription is created by the prescriber until it is read by the dispenser? Clearly a decision to use encryption is not on its own sufficient to guarantee confidentiality and availability. Other factors need to be taken into account.

3.2. *Authorization issues*

We have to make sure that only authorized personnel have access to the patient confidential data, and furthermore that they only have access to that subset of data that they need to see. In the security world this is known as the principle of least privilege, but it is also incorporated into the principles of the Caldicott Report [16] 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. When relating this to ETP, it has two consequences. Firstly, pharmacists should not be able to have access to all prescriptions that have been prescribed by all GPs, but should only have access to those prescriptions that the patient has asked them to dispense. Therefore, if 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. (Pharmacists should obviously keep their own historical records of what they have dispensed to whom and when, but this is not functionally part of ETP and therefore will not be discussed further.) Secondly, when prescriptions are in transfer between systems, no-one other than authorized professionals should have access to them. This means that the prescriptions should be encrypted so that only the authorized recipients can decrypt them.

How do we ensure that only authorized parties can prescribe and dispense? Problems in manually checking these authorizations, especially in the employment of locums, have led to cases like that of Godwin Onubogu [17], who was only a lab technician, yet managed to act as a locum with a penchant for misdiagnosing venereal diseases and falsely prescribing the corresponding drugs. This has led to calls for improvements in the employment procedure [18,19] and a request from the National Audit Commission to reduce the reliance on locum professionals [20].

Further, how do we ensure that a genuine prescriber is entitled to prescribe all the drugs written onto a prescription? Different prescribing practitioners are entitled to prescribe different drugs sets in the UK. With the advent of increased numbers of prescribing nurses this situation will become more acute as we will need to monitor and control the limited sets of drugs that they are allowed to prescribe. 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. But how do we achieve the same thing in an electronic system?

Access control schemes are the accepted way of protecting access to computer resources. If each electronic prescription is regarded as being a computer resource, then each prescription will need to have its own access controls to ensure that only authorized prescribers can write to it, and only authorized dispensers can read it. Further, these access controls will need to ensure that each prescriber can only add to the prescription the drugs sets that they are entitled to add. Alternatively, if a central prescription store model is used, access controls can be placed on the store to ensure that only authorized prescribers can write to it, and further that they can only write the correct type of prescription i.e. ones containing the correct drugs set. Additionally the access controls will ensure that only genuine dispensers can retrieve prescriptions from the store, otherwise patient confidentiality could be compromised, and prescriptions could be stolen.

Finally, how do we ensure that a patient is entitled to reduced fees or free prescriptions? The current paper-based system relies on pharmacists 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. How might this work in an electronic system? The UK government has suggested the introduction of Entitlement Cards in a recent white paper [21], using smartcard technology. The Entitlement Card could contain details about particular exemptions to NHS charges, held in the computer chip on the card. The pa-

tient would give the dispenser their Entitlement Card and the dispenser would read the embedded chip to obtain their exemption details. However, this may not be the ideal solution for the authorization of exemptions, as the card would need to be updated every time a person's entitlement changed. Would the card have to be sent away to the relevant exemption awarding body each time, or could the entitlement simply be claimed at the local Post Office or Department of Social Services? The distribution of entitlements and the work involved in passing the exemptions on to the beneficiaries becomes a very real problem within any Entitlement Card system. Finally, the introduction of Entitlement Cards cannot be relied upon in the short term, as it is a long-term UK government proposal. In comparison the introduction of ETP will be in a much shorter time scale and pilots are already running.

3.3. *Identity authentication*

Every professional who uses the ETP system must be reliably identified so that the system knows who the person is. This is needed to ensure that only authorized professionals can access the system, and also that accurate records can be kept about all accesses. In the paper system prescribers sign the prescription to identify and authenticate themselves. In an electronic system, a digital signature serves an equivalent purpose. Digital signatures are based on asymmetric cryptography, where the private key is used to create the digital signature, and the public key is used to validate it. We can have confidence that a prescriber did actually digitally sign a prescription if we have a reliable binding of the prescriber's name to his public key, and we can be sure that only the prescriber has access to the private key. Access to the private key is usually protected with a PIN or password, and in addition the key may be held in a smart card or other physical token that the prescriber can carry on his person. (This is known as two factor authentication, since the prescriber must possess something e.g. a smart card, and know something e.g. a PIN.) Thus the way that private signing keys are protected and used in ETP are important issues.

Current UK legislation requires the handwritten signature of the prescriber to be on the prescription form, but electronic signature legislation [22] lays down strict (but general) guidelines for how an electronic signature can be generated so that it is treated as being equivalent to a handwritten one. The technical guidelines developed by the European Electronic Signature Standardization Initiative in support of the EC legislation requires the private signing key to be held in a secure signature creation device, i.e. tamper proof hardware such as a smartcard [23]. So, providing the ETP system follows the electronic signature legislation and technical guidelines, the digital signature on an electronic prescription should be satisfactory for authentication purposes.

An additional consideration is how can we cater for mobile health professionals who move between organizations or doctors who visit patients in their homes? Should they carry their signing keys around with them e.g. on a smartcard, or should they be held in a central key server in tamperproof hardware that is accessible from anywhere? In the paper world, carrying a pen with which to sign prescriptions is not a burden, but if in the electronic world we ask a GP to carry a laptop and smartcard in addition to his existing equipment (stethoscope, mobile phone, briefcase etc.) we might find a great reluctance to do this. Thus the mechanism has to be both secure and practical.

In the paper system, patients sign their prescriptions to claim their entitlement to free prescriptions, so the ETP system will need to have an equivalent mechanism to stop anyone fraudulently claiming the right to free prescriptions. This implies that patients as well as professionals should possess private signing keys, but is this a realistic scenario? Or can an alternative authentication mechanism be developed?

3.4. *How can we ensure that if a problem occurs we can trace it back to its source?*

The ETP system must have a reliable audit trail that will allow problems to be traced, as well as mistakes, attempted fraud and system misuse. Since the ETP system spans many computers in different locations e.g. doctors surgeries, pharmacists shops etc. the audit component must cover all of these computers. At present the paper prescription is the audit trail. Prescription forms are linked uniquely to GPs and when they are dispensed they come in batches from the pharmacy that dispensed them. Models for ETP require the same level of accountability in order for an ETP system to be successfully adopted and accepted. The signature on a written prescription is the GP's bond to that prescription; in ETP the GP's bond will be the digital signature on the electronic prescription. This initial electronic script must remain unaltered all the way through ETP for the GP's bond to the prescription to remain intact.

When a pharmacy dispenses the drugs stipulated on the prescription, the pharmacist may annotate the script to show any changes he has made. His handwritten signature may be used to indicate who did this, although this is not a requirement of current practice, since it is the pharmacy rather than the pharmacist that is judged responsible. With ETP the pharmacist's digital signature may need to be added to the annotated script.

In the UK the patient or third party who picks up the dispensed drugs must also provide an audit trail by signing the back of the prescription form to authenticate themselves. This implies that patients must also possess private signing keys. Access to these may be by one factor authentication e.g. a PIN to access a key held remotely in a central store, or two factor e.g. a PIN and a smart card holding the key.

3.5. *Scalability, availability and reliability*

The ETP system must be available 24 hours a day, 365 days a year, since an illness can strike anyone at anytime. This means that every prescriber and dispenser should always have access to the ETP system under all operational circumstances. If we are not able to replace the present paper-based system with a totally reliable ubiquitous electronic one, what are the consequences of this? Does it mean that we will always have to run a paper-based system in parallel with an electronic system? What are the consequences of running two systems in parallel? Further the ETP system must be scalable to cater for the entire UK population of over 60 million people, and an ever-increasing rate of prescribing.

In all probability the paper prescribing system will need to remain operational, at least as a backup system, for the foreseeable future. This raises the issues surrounding dual systems processing throughout the prescription lifecycle. The prescriber will have to work with both pen and electronics, the dispenser will be required to alternate between batching up paper prescriptions for payment and electronically transmitting prescriptions for payment. The PPA will also require a mechanism for dealing with both forms of prescription processing. The patient may be given an electronic prescription on one visit and a paper one on another visit. Unfortunately it is easy

to imagine that having dual systems for prescription processing will bring about mistakes in the operation of either or both systems, as people switch between the two. It is envisaged that the paper-based system will be slowly wound down in favour of the electronic one, but herein lays another danger. A much-reduced paper processing capacity will not easily be able to cope with a sudden surge in demand if the electronic system catastrophically fails for whatever reason. We noted evidence of this when we visited pharmacists using their current PC-based systems. We were told that when their PC system crashes, the pharmacists find it difficult to keep up, and to process the same volume of prescriptions purely by hand. For all its failings, the current paper-based system is amazingly robust in the face of power and technology failures, the new electronic system can never be.

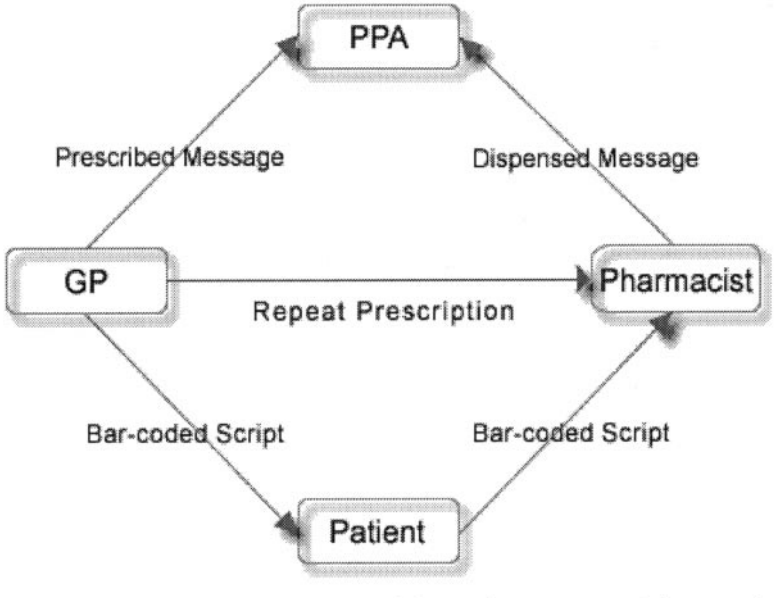
4. ETP models

There are three different ETP systems currently undergoing trials by the UK NHS. These are being provided by the Transcript Consortium, the Pharmacy 2U Consortium, and the SchlumbergerSema Consortium.

4.1. *The Transcript Consortium model*

Within the proposed Transcript Consortium model (see figure 1) prescribers will generate prescriptions for their patients, digitally sign them, and print out a barcoded script containing the prescription data. An encrypted electronic version is sent directly to the PPA.

The patient will take the barcoded script to any Pharmacy of their choice and the pharmacist will generate a dispensed message after dispensation and send this to the PPA on completion.



Source: http://www.ppa.org.uk/news/etp-consortia/transcript_model.htm

Figure 1. Transcript consortium model.

For repeat prescriptions patients will be asked to nominate a Pharmacy of their choice, and periodically the prescriptions will be sent directly there by the GP, encrypted for the pharmacy. After dispensation the Pharmacist will send a dispensed message to the PPA. The PPA uses the messages they have received from the pharmacy to effect payment to it, and from the GP to feed back prescribing information.

4.2. *The Pharmacy2U consortium model*

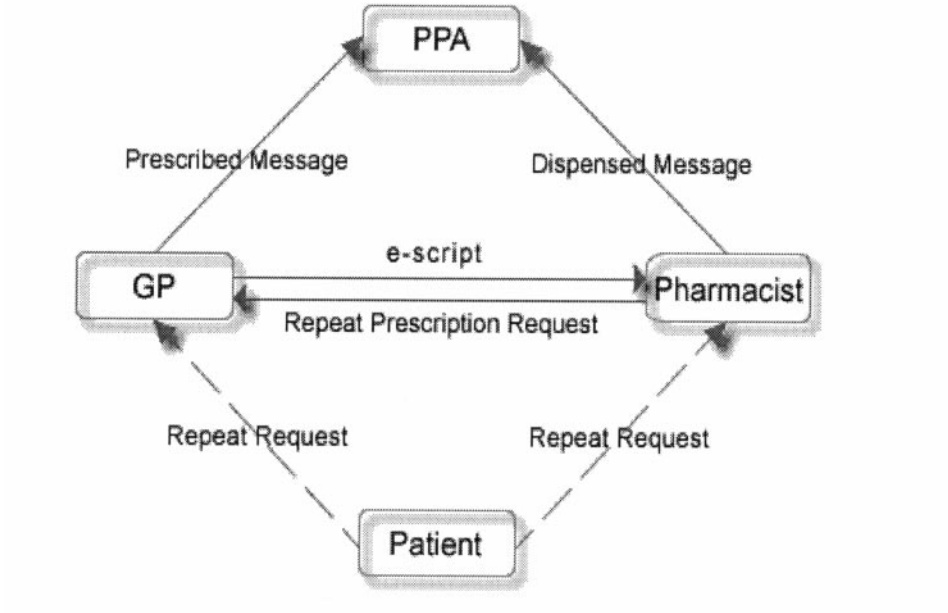
The Pharmacy2U Consortium have proposed a system relying solely on direct prescription messaging to patient designated Pharmacists (see figure 2). The patient will visit their GP and at the end of the consultation will be asked which Pharmacy they wish to have dispense their prescription drugs. The GP will then digitally sign the prescriptions, and send them directly to the chosen pharmacy, encrypted with a key for the pharmacy.

The patient will either have their prescriptions delivered to their door by home service pharmacies and Internet Pharmacies, or go into their designated Pharmacy and pick up their prescription, which should be ready for them on their arrival. On dispensation the Pharmacy generates a dispensed message and sends this to the PPA for processing.

The system works in the same way for repeat prescriptions.

4.3. *The SchlumbergerSema Consortium model (Flexiscript)*

The Schlumberger/Sema Consortium has settled for a relay approach in their proposed ETP system (see figure 3). Prescribers send digitally signed electronic prescriptions to a prescription data store, with an encrypted copy sent directly to the PPA. The system generates a prescription token containing a unique data store



Source: http://www.ppa.org.uk/news/etp-consortia/Pharmacy2u_model.htm

Figure 2. Pharmacy 2U Consortium model.

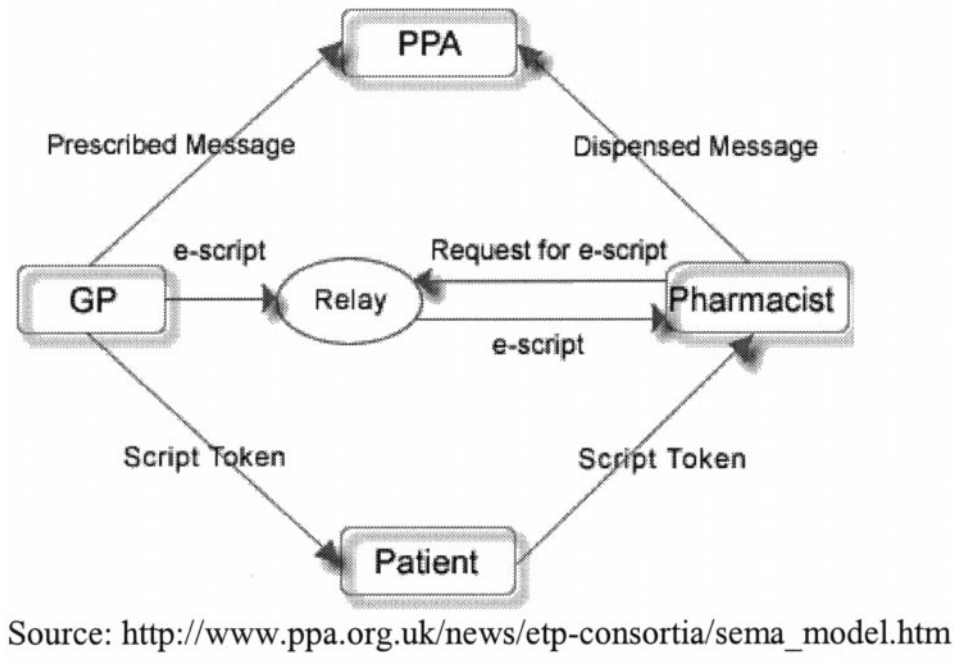


Figure 3. SchlumbergerSema Consortium model.

identification number for the patient. The patient then takes this prescription token to any Pharmacy and the Pharmacist uses the identification number to retrieve the prescription from the data store. All transfers to and from the data store are encrypted, but the prescription is unencrypted whilst in the data store. Patients may also phone the pharmacist ahead of arrival, giving them the identification number so that the prescription is ready to collect when they arrive. After dispensation the pharmacist sends a dispensed message to the PPA. Repeat prescriptions are handled in exactly the same way as initial prescriptions, so that the patient can go to any pharmacy to pick up their repeat prescriptions.

4.4. *Other models*

Applications that electronically prepare paper prescriptions have been in existence for a number of years, with the large majority of practitioners in the UK now providing printed scripts to their patients [24]. However, at present no ETP system exists in the UK for the transferral of prescriptions to pharmacies and the PPA. Several years ago Pharmed [25] had planned for the trial introduction of one such system within the NHS [26] and are now involved in the present trials as part of the Transcript Consortium. Hospital ETP systems have undergone trials within trusts such as the Wirral Hospital trust [27] with varying amounts of success.

Globally there have been numerous trials of different ways of electronically transferring prescriptions under different circumstances. In Denmark it is estimated that 35% of prescriptions are now sent electronically [3] and a project [28] on the impact of electronic prescription systems has also been carried out. Patients select the Pharmacy they wish to go to and the Danish GP sends the electronic pre-

scription directly to the Pharmacy. Electronic prescription systems [2,29,30] linked to pharmacies exist in the USA but these are in small cluster groups of selected pharmacies and prescribers who are all signed up to the same system provider. Prescriptions within these systems are sent either by fax or electronic mail. Around the world research has also taken place into ETP using patient smartcards to store the electronic prescription [31–33]. The patient would visit their GP and receive a prescription either on a personal smartcard that is always carried by the patient, or on a surgery smartcard that is given to the patient and returned to the GP once the process has been completed.

A trial has also taken place in the UK into using a Portable Data File 417 barcode (PDF417). This prints a two-dimensional barcode containing the prescription information onto an existing prescription form [34]. The idea was that the Pharmacist on receiving the prescription would be able to simply scan the barcode and the prescription would be electronically generated on the Pharmacist's PC from the barcode. One interesting point to note from this trial was that of the 12 730 scripts that were scanned 3% (382) could not be read during the trial. Whilst an error rate this high may not occur in other implementations using such barcodes, the previous trial is a key indicator that 2D barcodes may not be viable for use in containing electronic prescriptions. Importantly there is no recovery mechanism for the information contained in a 2D barcode if it fails to scan. The prescription itself could still be readable if it is produced in printed form above the barcode but the digital signature would not be.

4.5. *The Salford model*

The model, see figure 4, designed by the authors relies on the transmission of generated electronic prescriptions and dispensation notes to a prescription storage centre. The patient will visit their GP and be asked whether they wish to nominate a pharmacy from which to pick up their prescription items. At the culmination of the session the GP will digitally sign the electronic prescription, symmetrically en-

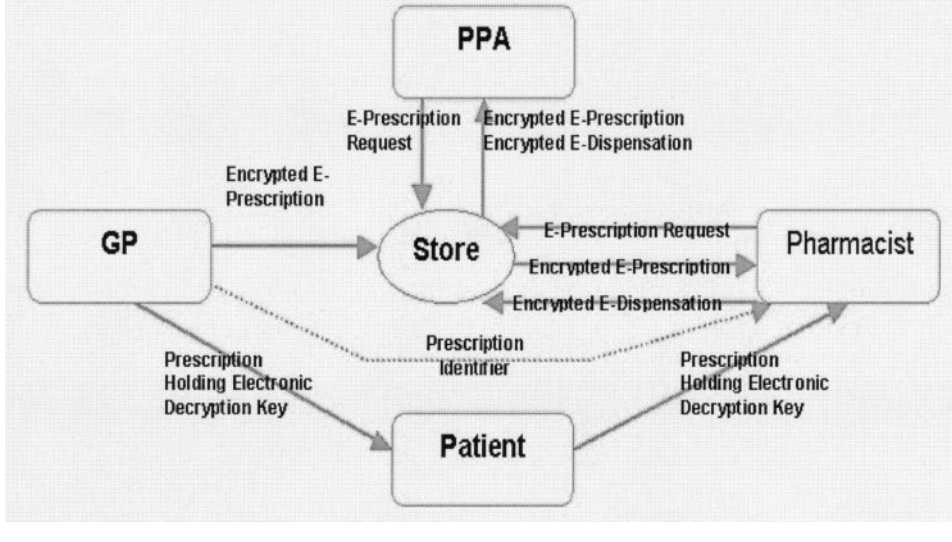


Figure 4. University of Salford ETP model.

crypt the electronic prescription and send it directly to a prescription store. The patient will be provided with a printed paper prescription on which will be a reference 1-dimensional Code128 barcode to allow fast access to the prescription in the prescription store and a 1D Code128 symmetric key barcode containing the one time symmetric key used to encrypt the prescription for transit and storage. When a patient chooses a particular Pharmacy (and for repeat prescriptions) an email message is generated containing the reference barcode and the one time symmetric key, encrypted for the chosen pharmacy. The pharmacy can then retrieve the prescription using the information within the email.

If the patient has selected a pharmacy from which to pick up their prescription items the prescription may already be ready for dispensation when they arrive there. If the patient hasn't selected a Pharmacy then when they hand their prescription to a Pharmacist who will scan the bar codes enabling their system to retrieve the prescription and decrypt it. In the Salford system there is a recovery mechanism should the barcode fail to scan. A coded representation of the information contained in the barcode is printed underneath. The pharmacist would type this in if they had difficulties scanning the barcode. Patient exemptions, GP's prescribing rights, and pharmacist's dispensing rights are checked automatically by the ETP system using attribute certificates (see later). On dispensation the prescription will be sent back to the prescription store for subsequent collection by the PPA. The PPA will routinely scan the prescription store(s) for dispensed prescriptions and then retrieve these along with the original prescriptions. An automatic routine will also run to clear the prescription store(s) of all time expired prescriptions.

5. Analysis of ETP models

5.1. *Patient confidentiality*

Health professionals are obliged to protect patient information both by law [4] and via the statutes of their profession [5]. In the present paper-based prescribing system, prescriptions are carried by the prescription holder from the GP to the pharmacy. Consequently the patient is responsible for the privacy of their own information for the whole duration of its transfer. In some of the ETP models this mode of transport has continued. For example in the German smart card system the prescription holder carries their prescription inside the smart card to the pharmacy. However, in most models prescriptions are sent electronically over a network and the patient may not hold any information about the prescription (e.g. the Pharmacy2U model). If he does, it is purely for efficiency reasons to aid the pharmacist in retrieving the correct electronic prescription from the system (e.g. the SchlumbergerSema model). The UK Transcript Consortium uses a hybrid approach, with the initial prescription being carried by hand, whilst repeat prescriptions are sent encrypted over the network. This is a good approach, since initial prescription recipients will see no difference to current practices and the prescription retains the same level of privacy. Pharmacists should gain from scanning in prescriptions instead of having to type them in. Repeat prescription recipients' gain, since they can go straight to their regular pharmacy to collect their prescription, without needing to go to their doctors first. The main disadvantage of this approach is that the barcode on the initial prescription may be unreadable, as was found in earlier trials.

In the UK ETP trials the network being used by all three systems is the NHSnet, which is a privately managed IP-based network. It is therefore more secure than the Internet, but its security relies on a policy of trying to keep undesirable people out, rather than on any inbuilt security mechanisms. However, since many of the computers connected to it are in publicly accessible hospitals, and the network itself is connected to the Internet via various firewalls, this has caused some primary carers to remark that the NHSnet is not as secure as it should be [35–37], and that encryption should be used for protecting confidential information. For this reason all three UK models encrypt the prescriptions as they are being transferred across the NHSnet.

In some of the US models the network is the Public Switched Telephone Network (PSTN) and the prescriptions are faxed messages. Faxes are inherently insecure, since their integrity and authenticity can never be guaranteed, for example, signatures can be cut and pasted, words can be blanked out. For these reasons, the UK NHS Executive advise against faxing Personal Health Data. They do have the advantage that they are transferred over the PSTN, which is a switched network, and is relatively secure. In order to eavesdrop one has to physically tap into the line over which the message is passing, unlike IP networks where one can eavesdrop from any node. The Internet is the least secure network, since it is publicly accessible, but its ease of access and ubiquity provide significant advantages over a private network, especially with regard to cost.

The above networks have varying levels of security, and the less secure the network, the more secure the prescription message needs to be during transfer. Even the private NHSnet is judged not to be secure enough, requiring encryption to be used in all 3 UK trials. Therefore, given that encryption is being used to protect patient confidentiality, the use of NHSnet appears to give no significant benefits over using the Internet, and when one takes cost and availability into account, it might appear that using NHSnet is disadvantageous compared to the Internet.

Patient flexibility is another issue facing ETP in the UK NHS. In the current paper-based system a patient can go to any Pharmacy in the country and present their prescription for dispensing. Research by Kember Associates [38] on behalf of Pharmed has discovered that 80% of patients would not mind naming a specific Pharmacy, but this still leaves one in five people not wishing to lose their current flexibility. When encryption is used to protect electronic prescriptions, the ETP models need to consider how the decryption keys are distributed so that the dispensers can access the prescriptions. There are various solutions to this problem.

5.1.1. Provide an asymmetric key pair to all ETP professionals and the prescriber directly encrypts the message for the dispenser. In this case the prescription is symmetrically encrypted and the one-off symmetric key is encrypted with the public key of the dispenser. The patient must select the pharmacy that he wishes to go to, and the symmetric key is encrypted using all the public keys of the pharmacists at that pharmacy.

Advantages

- In cryptographic terms the system is very secure, since the prescription is encrypted from the time of issuing until it is dispensed, and it is encrypted for named individuals.

- If one of the professionals is struck off or has their key pair compromised then the individual's key pair can be immediately revoked thereby preserving patient confidentiality. The only negative side effect of this will be for prescriptions that have been encrypted to only this key pair, rather than to several, as they will no longer be readable.

Disadvantages

- Administration of the encryption key pairs is an issue, as there would need to be key management for hundreds of thousands of users [39].
- The system is inflexible for patients since they have to state the pharmacy they wish to go to at the time of prescribing [8].
- The system needs to know the current locations of all pharmacists i.e. which pharmacists are resident at which pharmacies and when. This is needed for both permanent and locum pharmacists, and pharmacists who work at different locations. But even this will not work for patients who decide to delay the dispensing for a period of time, during which the pharmacists at a given location may have changed.

In conclusion, the security advantages of encrypting for named recipients are more than offset by its disadvantages. As none of the UK trials uses this model, we will not discuss it further.

5.1.2. Provide a key pair to a group of ETP professionals and the prescriber directly encrypts the message for the group. The NHS would issue key pairs to groups of pharmacists. The size of the group could range from an individual pharmacy, to a chain of pharmacies, or pharmacies in a geographical area, or in the extreme even one key pair for all pharmacists in the UK. In the UK ETP trials it has been decided that the group size will be a pharmacy.

Advantages

- The management overhead of key issuance is reduced compared to 5.1.1. above.
- Patient flexibility may be increased compared to 5.1.1. above. Depending upon group size, patients could choose any pharmacy from the group to dispense their prescriptions.
- The system does not need to know which pharmacists are resident at which pharmacy.

Disadvantages

- Key administration would be more complex and there would be various issues such as who belongs to which group. The groups would need to have clean boundaries. Locum pharmacists may still be in several groups and have access to multiple decryption keys.
- The system is inflexible for patients since they have to state the pharmacy (group) they wish to go to at the time of prescribing.
- Overall security is reduced. Since many people now share the same decryption key, it could unknowingly become copied to unauthorized people [40].

- If a decryption key is compromised, or a member of the group is struck off, revocation of the key pair will affect all members of the group. Prescriptions still in the system and encrypted by the revoked key pair are very likely to become unreadable.

The disadvantages of using group encryption keys would seem to outweigh its advantages. Nevertheless, this is the model chosen in some of the current UK trials. The Pharmacy 2U Consortium uses this approach for all prescriptions, and the Transcript Consortium uses this approach for repeat prescriptions. We feel it is a poor design for initial prescriptions since it removes patient choice and flexibility, but is acceptable for repeat prescriptions.

5.1.3. Provide an asymmetric key pair to all ETP professionals but the prescription is only encrypted during transfer to and from a secure central storage facility. In this scenario, the central storage facility has an encryption key pair, and prescribers encrypt the prescription for the central storage facility. When it arrives there, the central store decrypts the prescription (either before or after storage). The patient can then go to the pharmacy of choice, and any pharmacist in the store can serve him. The pharmacist contacts the central store for the prescription, and it is encrypted for the pharmacist and transported across the network. The pharmacist's PC decrypts the prescription.

Advantages

- Patients can go to any pharmacy of their choice.
- The prescription is only encrypted for one recipient on each leg of its journey.
- The system caters for pharmacist mobility and locums, as it does not need to know where any pharmacist is residing.

Disadvantages

- Administration of the encryption key pairs is an issue, as there would need to be key management for hundreds of thousands of users. This could be partially offset by only issuing key pairs to groups rather than pharmacists (as in 5.1.2. above).
- Each prescription has to be encrypted and decrypted twice, and this places a significant load on the central storage facility, which might adversely affect its performance.
- The prescriptions are held unencrypted in the central storage facility, either temporarily or permanently, making them visible to the facility administrators and a central point of attack for hackers, which may lead to compromise and loss of confidentiality [41].
- Pharmacists potentially have access to all prescriptions in the central store, which violates the principles of least privilege and those in the Caldicott report.

For this model the prescription confidentiality whilst it is within the store must be considered extremely carefully. Since the decryption key is held by the store, and prescriptions are stored in the clear (at least temporarily) then we must rely on the 'gatekeepers' to the store e.g. firewalls, and on the authentication and access

control mechanism of the store to keep the prescriptions away from hackers. We must also rely on the integrity of the personnel who run the store, since system administrators usually have access to all the contents of the computer systems under their control. System administrators would easily be able to determine prescribing trends and confidential data about who is being prescribed what. Finally, pharmacists will be able to scan the store and retrieve any prescription, regardless of whether the patient asks them to dispense it or not.

In conclusion, this model has several advantages but these are offset by a weakening of the overall confidentiality and possible performance and administration disadvantages. The SchlumbergerSema Consortium Model uses this approach.

5.1.4. Provide an asymmetric key pair to all patients and encrypt the prescription for the patient. The patients would need to have some way of storing and accessing their key pairs, for example by providing them with individual smart cards holding their key pairs. Prescriptions are protected using the patient's public encryption key, and the prescription is decrypted at the Pharmacy using the patient's private decryption key. Access to the key pair storage requires the patient to input a secret e.g. PIN number, known only to the patient. Using two-factor authentication (e.g. possession of the smart card and knowledge of the PIN) is preferable to one factor authentication (e.g. knowledge of a PIN for accessing a secure central key storage device).

Advantages

- The system is very secure and the only way to retrieve and decode the patient's prescription is when the patient's authentication information is entered into the pharmacist's system.
- The patient has complete flexibility over which Pharmacy to go to for dispensation.
- Any pharmacist in the pharmacy can dispense the prescription.

Disadvantages (of smart card based system)

- There is a large administrative overhead in producing smart cards for everybody in the country [42,43].
- There may be public resistance to having to carry a smart card on one's person, since it may be regarded as a type of identity or entitlement card [44].
- Patients are likely to forget their smart cards when they visit their GPs.
- If the card is damaged or lost then the prescription cannot be retrieved.
- Incapacitated patients may not wish to give their smart cards to other people to collect their prescriptions on their behalf.
- If the patient forgets their PIN number, or gives their smart card to a relative or friend to act as their proxy without telling them the PIN, then the prescription cannot be retrieved.
- Management of forgotten PINs is likely to be a big overhead (compounded if patients only rarely have drugs prescribed for them, or are old with failing memory – they are much more likely to forget their PINs [45].

Disadvantages (of a central key storage facility)

- The system is less secure than individual smart cards, and the central key server is a central point of attack.
- Management of forgotten PINs is likely to be a big overhead (compounded if patients only rarely have drugs prescribed for them, or are old with failing memory – they are much more likely to forget their PINs).

Whilst this system is very secure, it has obvious disadvantages in terms of patient usability and acceptability. Consequently no one is currently suggesting using this model.

5.1.4. Provide the Symmetric Decryption Key to the patient and send the prescription to a secure central storage facility. In this model the prescriber symmetrically encrypts the electronic prescription and submits it to a secure central storage facility. The symmetric key is provided to the patient and archived by the prescriber. The symmetric key could be written onto the paper prescription form as a bar code, along with the prescribed drugs, or could be written to a smart card (the prescriber holding a stock of smart cards for this purpose). The patient takes the symmetric key to a pharmacist of his choice, and the pharmacist retrieves the encrypted prescription and decrypts it using the symmetric key provided by the patient.

Advantages

- Flexibility for patients to go to the pharmacy of their choosing, whenever they want to.
- The patient is responsible for their own data privacy and can let just the pharmacist of choice have access to the symmetric key.
- The patient can give the symmetric key to a proxy for her to pick up the prescription on his behalf.
- The prescription remains encrypted the whole time, even whilst in the central storage facility and is therefore not able to be compromised.
- Every pharmacist has the potential to be able to decrypt every prescription, but only when the patient authorizes them to do so, and the system does not need to know the pharmacist's current locations.
- Reduced administrative burden, as none of the pharmacists and patients need to have encryption key pairs.
- The central storage facility does not need to encrypt or decrypt the prescription for transfer thereby increasing its efficiency.

Disadvantages

- If the symmetric key is damaged or lost whilst in transit by the patient, then the electronic prescription cannot be decoded by the pharmacist. However, if barcodes on paper prescriptions are used, the paper script may still be readable even if the barcode is damaged. Further if 1D barcode representations are used there may still be a recovery mechanism available to the user.

- If smart cards are used rather than barcodes, the smart cards will need to be transported back to the GPs for re-use.

The authors think that this system has significant advantage over all the previous systems, and consequently they have used it in their model. A full description of symmetric key barcodes can be found in [46].

5.2. *Authorization*

Many of the ETP designs outlined above do not explicitly deal with electronic authorizations, either with patient exemptions from charges, or the rights of the professionals to prescribe or dispense various drugs. For patient exemptions, the reliance seems to be kept on the pharmacist to check the patient's paper documents (if at all); for dispensing, the PPA must still check that the pharmacists are bone fide before issuing payment; for prescribing, presumably the PPA will only issue private signing keys to authorized GPs. Then the GP's possession of a valid private signing key could be taken as his authorization to prescribe, and this can be withdrawn by the PPA revoking his corresponding public key certificate if necessary. However, in this case, the private key is serving two purposes, that of authenticating the GP and simultaneously authorizing him to issue prescriptions. It would also be possible to mark the keys as being authorized to sign different prescription pads, so as to differentiate say, between GPs and prescribing nurses, although we doubt that this is the case in the current ETP trials (even though few details have been published). This mechanism might be fine in the current ETP trials when ETP is the sole electronic application, but this becomes a problem when other electronic health care applications are introduced which also require digital signatures. The same private key cannot be used to selectively distinguish between prescribers and their various authorizations to use particular applications. Either multiple signing/authorization keys will need to be issued, which causes the user problems in choosing the correct key for any particular purpose, or an alternative mechanism needs to be found.

Is there a common solution to all the authorization issues described above, which also is extensible to serve the needs of applications in the future? We believe there is. We have been developing a Privilege Management Infrastructure (PMI) for authorization purposes, under the EC-funded PERMIS project [47]. The PERMIS PMI is a trust management infrastructure according to the definition given by Blaze [48]. 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, and all applications use the decision engine to enforce their access control decision making. 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 X.509 attribute certificates conforming to the latest version of the X.509 standard [14]. (See Appendix 1 for a description of attribute certificates). We have integrated the PERMIS PMI into our ETP infrastructure so as to provide secure authorization of the various players e.g. the GP's right to prescribe, and the patient's right to free prescriptions.

5.2.1. ETP privilege policy. 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. It need not be the Secretary of State himself who signs the policy, but could be anyone authorized by him. The system would be told who the authorized trusted person is. The actual policy can be as complex as required for the task, below is just a simple example:

- The General Medical Council is trusted to allocate the role of Doctor to qualified doctors. Anyone with the role of Doctor is allowed to prescribe any drug and submit prescriptions to the prescription store.
- The Royal Pharmaceutical Society is trusted to allocate the role of Pharmacist. Anyone with a role of Pharmacist has the privilege to retrieve prescriptions from the prescription store and to view them, and then subsequently to submit the dispensed prescription back to the prescription store.
- The Royal College of Nursing is trusted to allocate the role of Prescribing Nurse to suitably qualified nurses. Prescribing Nurses are authorized to prescribe a limited set of drugs and submit prescriptions to the prescription store.
- The Department of Social Security is trusted to allocate Exemption roles to members of the public. Anyone with an Exemption role is authorized to obtain free prescriptions.

Given the above policy, a signatory member of the General Medical Council indirectly gives any GP in the UK NHS the right to prescribe when he issues the GP with a Doctor role attribute certificate signed by himself. When the GP is generating a prescription their prescribing program calls the PERMIS decision engine to determine if the GP is authorized to prescribe 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 to prescribe and they will be allowed access to the operation to generate an electronic prescription and send it to the prescription store.

5.2.2. 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; and
- while patients are on national supported benefit they are exempt from all charges.

Using the PERMIS PMI, these exemptions would become patient roles, and the policy would state what privileges these roles conferred. The roles could either be stored within a national system or on a smart card issued to and carried by the patient. This system will alleviate the dispenser from the job of checking for proof of exemption. Approved bodies would generate and electronically sign 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 whilst on benefit an exemption certificate could be issued to a claimant quarterly or annually. The PERMIS decision engine is then called to decide on patients' exemptions from charges, thereby relieving the pharmacist of the (often embarras-

sing) task. As a fallback, for example in the case where a female is newly diagnosed as pregnant and therefore authorized to be exempt from charges before an attribute certificate has been created for her, the pharmacist is still enabled to over-ride the system and grant exemption, providing the patient signs to accept responsibility for the decision.

5.3. *Identity authentication*

All three UK pilots use digital signatures to authenticate the issuing GP. The current pilots are not using digital signatures that are legally equivalent to handwritten signatures (qualified signatures), as required by law, but a special dispensation has been granted for the duration of the trials [49]. The reason for the lower level of authentication, is that to run CAs capable of issuing qualified certificates [50], is very costly, and few of them are operational today. Further, the use of secure signing devices such as smart cards has been found to be problematical in previous trials [40], plus they are also costly compared to software based keys.

Ultimately strong authentication based on qualified signatures ensures that no signer of messages within the ETP system can reasonably repudiate their signature. If questionable prescriptions are being produced or fraudulent prescriptions are found then the ETP administrators will know whose private key has been used to sign these prescriptions, and appropriate actions can be taken (not least of which could be to revoke the key thereby ensuring that no further electronic prescriptions can be signed).

The UK Government has proposed within the recent consultation paper 'Entitlement Cards and Identity Fraud' [21] the universal introduction of identity cards for every UK citizen. If these identity cards were to contain a public and private key pair then every citizen in the UK would be able to electronically sign their electronic prescriptions, to indicate that they had successfully received the drugs. This would eliminate some of the fraud today, such as prescribing for deceased patients. However, to implement such a scheme is outside the bounds of the current ETP trials.

5.4. *Audit trails*

Not many of the models detailed above provide for complete audit trails and yet these provide evidence that a patient was dispensed the drugs. If we take an example ETP scenario such as:

(1) a patient visits a GP;
(2) the patient chooses a pharmacy from which to pick up their prescription;
(3) the GP sends a direct message to that pharmacy detailing the patients prescription;
(4) the patient does not turn up at the pharmacy to claim his drugs.

What is to stop the pharmacist claiming they have dispensed the drugs and receiving payment? Worse scenarios can be constructed when the GP and pharmacist collude together.

If the patient has his own key pair e.g. on a smartcard, then he can electronically sign the transaction to say he has been given the drugs. Alternatively, if a paper prescription is still used along with a symmetric key barcode, as in the Salford design, the procedure can simply stay the same as today. The paper prescription provides the complete audit trial (after the patient has signed the back of the

prescription form to say he has been given the drugs) and the barcode controls which pharmacist has access to the electronic version. Other models would need to have similar features in place to ensure a complete audit trail is created and controls are in place to limit professional fraud. Models that have a central repository for the storage of prescriptions will also need an audit trail of access to the repository detailing who, when and what was added/retrieved. Models that don't use a central repository but rely on direct messaging, should also have an audit log that records what messages were sent to whom and when.

5.5. *Scalability, availability and reliability*

Central store models have to ensure that they are scalable, and that the central store does not become a bottleneck to performance. Direct email models do not have to worry about this issue, but they have to be concerned about the reliability of email and the potential loss of messages, for example, the patient arrives at the pharmacy but the prescription message never did. This requires positive confirmation messages to be sent to the GP's system. This is one of the reasons why the NHS is still using X.400 messaging rather than SMTP. Central store models are less concerned about communications reliability, since the connections are in real time, and the GP knows immediately whether the prescription has been stored safely or not.

The Salford model has been built with scalability in mind, since the central prescription store can be distributed into as many servers as needed. At one extreme, there could be one prescription store per GP surgery, at the other extreme there could be one central store for the whole country. This is achieved by writing the URL of the store actually used by the GP into the unique coded prescription reference barcode. Each GP system will hold the URL as a configuration parameter. The pharmacist's system can then locate the appropriate store by a simple DNS lookup after scanning in the reference barcode. Availability and reliability can be achieved by using fault tolerant hardware to host the prescription store. If a backup store is required, in case the primary store is unavailable, then each GP system can be configured with a second URL to be used if the primary store is unavailable. If prescription redundancy is required, the second URL could always be used alongside the primary one, so that two copies of the prescription are stored centrally. However, we do not believe that this is a requirement.

No matter what availability and reliability mechanisms are introduced, ETP could always be disrupted by failed communications systems or denial of service attacks, or simply failed hardware. Therefore a backup system needs to be in place for dispensing drugs to patients. All three UK pilot models described earlier will not work without a communication medium. The Salford model is the only one that can continue to work in the event of a complete or partial system failure, since patients still carry their paper prescriptions to the pharmacist, and these can be used as the ultimate fallback.

6. Summary

We have reviewed all the security issues relevant to ETP, without ignoring their impacts on system usability. The issues of electronic security and the potential problems surrounding the implementation of a secure ETP infrastructure cannot be ignored if the integration of ETP into the UK NHS is going to be a success. However security decisions have to be balanced against system usability and it is

extremely difficult to design a secure system that satisfies all user groups. We have analysed how the three UK pilot ETP models have attempted to achieve this balance. Finally we have described an enhanced Salford model for ETP that provides significant improvements over the other three models, both in terms of security, reliability and usability.

The Salford ETP model provides authentication, authorization, audit measures and patient confidentiality without loss of patient flexibility, system performance or system scalability, and without requiring the patient to become familiar with a new prescribing process. Furthermore it is completely resilient to partial or total ETP system failure.

It is difficult to gauge whether ETP will ever become the sole single prescribing system within the NHS or not, and in many ways the authors believe it is preferable to have the paper prescribing system as a backup mechanism. To this end, mirroring the present paper practice will help reduce user confusion when operating with both ETP and paper prescribing systems.

Acknowledgements

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

References

1. NHS, 2002, The NHS plan – a plan for investment – a plan for reform, Presented to Parliament by the Secretary of State for Health, Available at http://www.nhs.uk/nationalplan/nhsplan.htm (February 21).
2. AllScripts, 2002, *http://www.allscripts.com/ahcs/index.htm* (November).
3. Middleton, H., 2000, Electronically transmitted prescriptions – a good idea. *The Pharmaceutical Journal*, **265**(7107), 172–176.
4. UK Government, 1998, Data protection act 1998 (c.29), Crown Copyright.
5. Information Commissioner, 2002, *Use and Disclosure of Health Data*, May, Available from http://www.dataprotection.gov.uk/dpr/dpdoc.nsf/ed1e7ff5aa6def308025663600 45bf4d/7b7d02d29c28e76d80256bb5005d7bb3/$FILE/HEALTHGU.pdf (July 2003)
6. Electronic transmission of prescriptions, *http://www.doh.gov.uk/Pharmacy/etp.htm* (June 2002).
7. Mundy, D. P. and Chadwick, D. W., 2002, 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.
8. Mundy, D. P., Chadwick, D. W., Ball, E., Marsden, P., Bell, D., Whatley, J. E., Sobreperez, P. and New, J., 2003, Towards Electronic Transfer of Prescriptions (ETP) in the United Kingdom National Health Service – Stakeholder Evaluation of ETP Pilots, *3rd International Conference on The Management of Healthcare and Medical Technology*, Warwick, 7–9 September.
9. Stallings, W., 1999, *Cryptography and network security : principles and practice Second Edition* (London: Prentice Hall).
10. National Bureau of Standards, 1977, Data encryption standard, FIPS PUB 46, January.
11. Adams, C., 1997, The CAST-128 encryption algorithm, RFC2144.
12. Advanced Encryption Standard, 2002, Available at http://csrc.nist.gov/encryption/aes/ (November).
13. Diffie, W. and Hellman, M. E., 1979, Privacy and authentication: an introduction to cryptography, *Proceedings of the IEEE*, **67**(3), 397–427.
14. ISO/ITU-T Rec., 2002, X.509 the directory: authentication framework.
15. Gritzalis, S., Gritzalis, D., Moulinos, C. and Iliadis, J., 2001, An integrated architecture for deploying a virtual private medical network over the Web. *Medical Informatics and the Internet in Medicine*, **26**(1), 49–72.

16. NHS EXECUTIVE, 2002, The Caldicott Committee: report on the review of patient-identifiable information – December 1997, Available at http://www.doh.gov.uk/confiden/crep.htm (November).
17. SAYERS, S. 2002, Lies, damn lies ... and CVs!. *t Magazine*, March. Available at http://www.tmag.co.uk/articles/Mar00p26.html (November).
18. CARVEL, J., 2002, Checks failure could allow 'bogus' GPs to treat patients. *Guardian Unlimited*, Available at http://society.guardian.co.uk/health/news/0,8363,410289,00.html (November).
19. NATIONAL AUDIT COMMISSION, 2002, Cover story – the use of locum doctors in NHS Trusts. Available at http://www.audit-commission.gov.uk (November).
20. LOCUM GPS, 2000, *Health Which?* (December).
21. UK GOVERNMENT CM5557, 2002, Entitlement cards and identity fraud – a consultation paper, July, Available at http://www.homeoffice.gov.uk/cpd/entitlement_cards.pdf (August).
22. EUROPEAN PARLIAMENT, 2000, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. *Official Journal L 013*, **19/01/2000**, 12–20.
23. CEN WORKSHOP AGREEMENT, 2001, Secure signature-creation devices. CWA 14169.
24. DEPARTMENT OF HEALTH, 2002, Available at http://www.doh.gov.uk/Pharmacy/FAQs.htm (June).
25. PHARMED, 2002, http://www.pharmed.co.uk (June).
26. DAVIS, E., 2000, Electronic transfer of prescriptions in primary care. *The British Journal of Healthcare Computing & Information Management*, **17**(8), 29–31.
27. MOORE, J., FARRAR, K., HUGHES, D. and SPOURS, A., 1996, Electronic prescribing – the perfect prescription. *The British Journal of Healthcare Computing and Information Management*, **13**(4), 25–27.
28. MOORMAN, P. W. and BERNSTEIN, K. (editors) 1999, *The CoCo project report*. (Odense: Danish Centre for Health Telematics).
29. POCKETSCRIPT, 2002, http://www.pocketscript.com/ (November).
30. EPHYSICIAN, 2002, http://www.ephysician.com/ (November).
31. ECKSTEIN, L. and STRUIF, B., 1999, 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.
(1) 32. NHS MANAGEMENT EXECUTIVE, ????, *The care card – evaluation of the Exmouth project* (London: HMSO).
33. SONG, W. J. and AHN, B. H., 2002, A secure transmission of the prescription order communication system based on the internet and the public-key infrastructure using master smart cards, *35th Annual Hawaii International Conference on System Sciences (HICSS'02)*, Vol. 6, p.156b, January.
(2) 34. SHARPLES, S. and WOODHEAD, A., 1996, Improving security: electronic transfer of prescription data in primary care. *The British Journal of Healthcare Computing and Information Management*, **13**(1), ????–????.
(3) 35. GREETHAM, D. and FRASER, R., ????, *Explanatory guideline to PKI for patients and the public*, NHS Information Authority Guidance.
36. LOCKLEY, J., 2000, Editorial piece. Torus–Torex User Group Journal, No.42, December, Page 2.
37. IMPACT, 1999, Doctors demand encrypted NHSnet. *Pharmaceutical Journal*, **263**(7069) 697, October 30, News. Available at http://www.pharmj.com/Editorial/19991030/news/nhsnet.html (November 2002).
38. KEMBER ASSOCIATES, 2002, Research with patients. Available at http://www.pharmed.co.uk/text/reseach3.html (August 29).
(4) 39. SCHNEIER, B., 1996, *Applied Cryptography*, Second Edition (Location ????: John Wiley & Sons).
40. MCHUGH, J. and MICHAEL, J. B., 1999, Secure Group Management in Large Distributed Systems: What is a Group and What Does it Do?, *Proceedings of the 1999 workshop on new security paradigms*, Caledon Hills, Ontario, Canada, pp. 80–85.
(5) 41. ANDERSON, R., 1993, Why Cryptosystems Fail, *1st Conf.- Computer and Comm. Security '93*, Location ????: ACM.
(6) 42. FOUNDATION FOR INFORMATION POLICY RESEARCH, 1999, Framework for Smart Card Use in Government – A Consultation Response.
43. CHADWICK, D. W., 1999, Smart cards aren't always the smart choice. *IEEE Computer*, **32**(12), 142–143.
44. PRIVACY INTERNATIONAL, 2003, see http://www.privacyinternational.org/ (February).
45. YAN, J., BLACKWELL, A., ANDERSON, R. and GRANT, A., 2000, *The memorability and security of passwords – some empirical results*, University of Cambridge Technical Report, Number 500, September.
46. BALL, E., CHADWICK, D. W. and MUNDY, D. P., 2003, Patient Privacy in Electronic Prescription Transfer. *IEEE Security and Privacy*, March/April.
47. CHADWICK. D. W. and OTENKO, A., 2002, The PERMIS X.509 role based privilege management infrastructure, *Proceedings of the 7th ACM Symposium On Access Control Models And Technologies* (SACMAT 2002), Monterey, USA, June, pp 135–140.
48. BLAZE, M., FEIGENBAUM, J. and IOANNIDIS, J., 1999, The keynote trust-management system version 2, RFC 2704, September.

49. Department of Health, 2002, New legislation to facilitate electronic transmission of prescription pilot schemes, Available at http://www.doh.gov.uk/pharmacy/etpleg.htm (November).
50. Santesson, S., Polk, W., Barzin, P. and Nystrom, M., 2001, Internet X.509 public key infrastructure qualified certificates profile, RFC 3039, January.

Appendix 1. Attribute Certificates

A relatively new development in the field 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 [36], see figure 5, consists of a data structure called Attribute Certificate Information, see figure 6, which contains details about the issuer, the holder, the times of validity etc. as well as the embedded attribute(s). In our ETP design the prescription is stored as an attribute within Attribute Certificate Information, the holder is the pa-

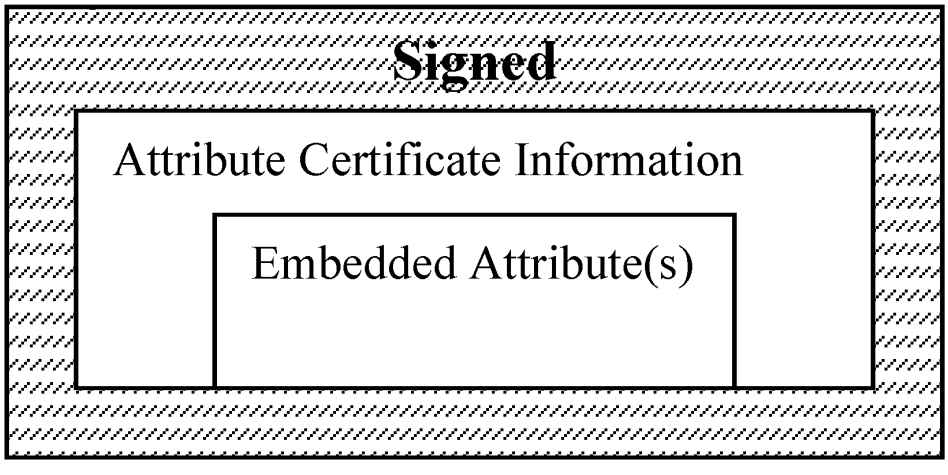


Figure 5. Attribute certificate.

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

Figure 6. Attribute certificate information.

tient and the issuer is the prescriber. The validity period is set to six months from date of issuance. 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.

When the Pharmacist receives or retrieves the electronic prescription they are able to unpackage the data structure and verify the signature. The digital signature process ensures that the prescription data has not been altered either in transit, in storage or on retrieval. Further, if qualified signatures are used, the pharmacist has the equivalent of a handwritten signature authenticating the GP who issued the prescription.

TMIF	
Manuscript No.	100292
Author	
Editor	
Master	
Publisher	

Medical Informatics & the Internet in Medicine
Typeset by Elite Typesetting for

Taylor & Francis healthsciences

ELITE TYPESETTING TECHNIQUES LTD
www.elitetypesetting.com

QUERIES: to be answered by AUTHOR

AUTHOR: The following queries have arisen during the editing of your manuscript. Please answer the queries by marking the requisite corrections at the appropriate positions in the text.

QUERY NO.	QUERY DETAILS	QUERY ANSWERED
1	Reference 32 – please supply year of publication	
2	Reference 34 – please supply page span	
3	Reference 35 – please supply year of publication	
4	Reference 39 – please supply location of publisher	
5	Reference 41 – please supply location of publisher	
6	Reference 42 – please supply any further details	