The Secure Electronic Transfer of Prescriptions

David Chadwick, University of Salford
Darren Mundy, University of Hull

Abstract

This paper describes the information security attributes of confidentiality, integrity and availability, and then uses these to determine the security requirements for ETP. It briefly describes the four published UK ETP models (from Flexiscript, Phamacy2U, Salford and Transcript) and evaluates these from the perspectives of confidentiality, integrity and availability. Deficiencies, from a security perspective, in the 3 UK ETP pilot models (from Flexiscript, Phamacy2U, and Transcript) are described. Possible solutions to these deficiencies, as implemented in the Salford model, are described.

Introduction

Information security is traditionally viewed as providing confidentiality, integrity and availability – the CIA – of electronic data.

Data confidentiality means that only authorised people are allowed to access the electronic data. By "access" we mean any type of access to the data; not only the ability to read the data, but also the ability to update the data, delete the data or execute the data (assuming the electronic data is a program). Conversely, data confidentiality requires that unauthorised people are not allowed to access the data in an unauthorised manner. Computer security mechanisms that are used to provide data confidentiality are:

- user authentication, whereby the computer can reliability determine who the accessing user is,
- access control, whereby the computer only allows a subset of users to access the data in predefined ways, and
- encryption, whereby the data is enciphered by the computer using an encryption key, so that only people or entities with the correct decryption key are able to decipher and access the data.

Integrity refers to not only "data integrity" i.e. that the data has not been tampered with since its creation by its author, but also to "origin integrity" i.e. that the data really did originate from the person who is claiming to have created it, and did not come from an impostor. Computer security mechanisms that underpin data and origin integrity are based on calculating a cryptographic checksum that is in some way bound to the data and to the originator. Thus if the recipient can reliably recalculate the checksum, using the received data and knowledge about who the supposed originator is, then the recipient can validate the integrity of the received data.

Availability means that the electronic data is available to the authorised users whenever and wherever they need to access it. Data availability is often crucial. Unavailability can in many instances be worse than having access to partially corrupted data or providing compromised access to the data. Implicit in the concept of availability are the quality attributes of reliability, scalability and performance. Lack of availability can be due to the unreliability of the equipment storing the data, bugs in the software used to access the data, disruption of the supporting services such as

power or water needed to keep the equipment operational, or failure of humans operating the system or the supporting services. Human error is often the biggest cause of unavailability. Adequate performance is necessary when accessing the data in order to stop humans becoming frustrated with the system or unable to perform their tasks efficiently or effectively. Steadily worsening performance will eventually lead to complete unavailability of a system. If systems are not scalable to the levels required, this may lead to worsening performance as the system becomes saturated, and in the worst case, to a complete cessation of service. Denial of service attacks are specifically aimed at removing availability, by saturating a system so that it is unable to provide a normal level of service.

Finally, it should be stated that it is impossible to achieve absolute security of electronic information, just as it is impossible to guarantee that a house can never be burgled, a bank robbed, or a car stolen. Generally speaking, the more you are prepared to pay for information security, the more secure you can make your information. But it is a law of diminishing returns. Consequently, the strength of security applied to electronic information should be in proportion to its value, and to the potential cost of losing the confidentiality, integrity and availability of the information that is being secured. Ultimately, determining the level of information security to provide is a business and political decision.

Applying CIA to ETP

When we consider the implications of applying (or not applying) confidentiality, integrity and availability to the electronic transfer of prescriptions (ETP), it reveals a number of system requirements.

Considering confidentiality first, there are a number of legal and ethical obligations placed on the medical professional to protect the confidentiality of patient information. The 1998 Data Protection Act [1] requires that personal data be protected against unauthorized or unlawful processing. The NHS Confidentiality Code of Practice [2] requires that all NHS staff must keep patient information private, and physically and electronically secure. Since electronic prescriptions contain patient information, the implications of these obligations for ETP are that:

- only qualified and authorised prescribers should be allowed to create electronic prescriptions for patients,
- electronic prescriptions should be encrypted during transfer so that unauthorised people cannot view their contents, and
- only qualified and authorised dispensers should be able to retrieve electronic prescriptions ready for dispensing to patients.

However, not all authorised dispensers should be able to retrieve all genuine electronic prescriptions, since this would violate a principle of the Caldicott report [3] which states "*Access to patient identifiable information should be on a strict need to know basis.*" Thus we have another requirement:

- only the qualified dispenser chosen by the patient or his proxy should be able to access the patient's electronic prescription.

This later requirement poses a significant problem for ETP, namely, how should an electronic prescription be electronically protected so that any dispenser has the potential to access it, but only the dispenser chosen by the patient or his proxy can actually access it. As we will see later, the four ETP systems designed in the UK have chosen to address this critical requirement in different ways.

Turning now to consider integrity, all prescribers i.e. GPs, dentists, prescribing nurses etc. need to be unambiguously bound to the electronic prescriptions that they create. This will allow any authorised person to check who issued a particular prescription, and whether the prescription has been tampered with or not since creation. Before dispensing, pharmacists need to be confident that:

- each electronic prescription really did originate from a qualified and authorised prescriber,
- each prescription is valid i.e. it is not accidentally corrupted in any way, or even purposefully tampered with or a complete fake,
- each prescription is an original i.e. not a duplicate of a previously valid prescription, and
- each prescription has not previously been dispensed.

Prescription duplication, or multiple dispensations, especially in the case of controlled drugs, could allow a patient to obtain multiple doses of a highly restricted medication.

Unauthorised duplication of digital data poses a particular problem for computer scientists, since a binary copy cannot be distinguished from its digital original, as they both comprise the same sequence of binary digits. The method usually used to protect against data duplication during computer communications, is to uniquely identify each data message and then make the receiving software discard second and subsequent copies when it receives multiple copies of a message. Thus any ETP system should be able to detect duplicate, corrupted, fake and previously dispensed prescriptions, and not be willing to process them. Unfortunately we currently don't have any technology that is able to reliably and in all cases differentiate between maliciously altered digital data on the one hand and genuine digital data that was incorrectly created or accidentally corrupted on the other hand. Thus electronic prescribing and ETP software has to be carefully designed to both minimise the chances of users making mistakes during electronic prescription creation, and to stop corrupted, duplicate or incorrect prescriptions from being transferred and/or dispensed.

Considering availability, the ETP system obviously needs to be extremely reliable. Since people's comfort and quality of life, and in extreme cases their very life itself, may well depend upon the availability of medication when needed, availability of the ETP system is perhaps the most important of the three security elements to consider. However, no one has ever created a 100% reliable system, nor is anyone likely to in the near future. Therefore to minimise the chances of a complete system failure, ETP system designers need to ensure that their designs do not contain any single points of failure, but rather have alternate or multiple servers for all critical system components. Furthermore, there needs to be a fallback mechanism that is able to take over when (components of) the ETP system fail, either in whole or in part due to ETP hardware or software failures, or failure of the supporting services such as the power or communications networks that ETP relies upon. In addition, ETP systems designers need to ensure that their designs are scalable to national proportions, whilst maintaining adequate performance for all participants. We have found in our previous research [15] that this last factor is extremely important for busy health care professionals such as GPs, whose time is at a premium. Perhaps of less importance, but still worthy of consideration under the topic of availability, is to ensure that the ETP system does not "loose" any of the electronic prescriptions that have been

entrusted to it, or if in the rare cases when it does, we have an easy mechanism to allow prescribers to re-introduce “lost” electronic prescriptions back into the system.

UK ETP Systems

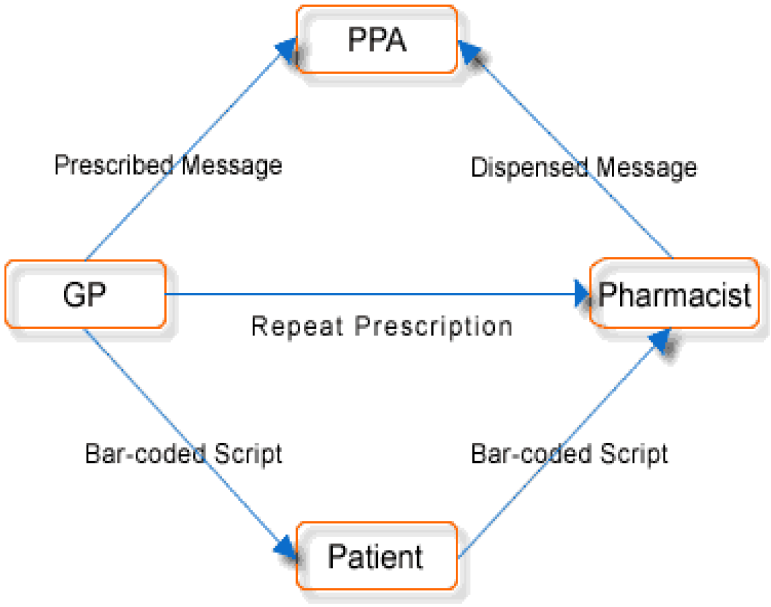
There were three different ETP pilot systems that underwent live trials by the UK NHS during 2001-3. These were provided by the Transcript Consortium, the Pharmacy 2U Consortium, and the SchlumbergerSema Consortium. A fourth system was developed at the University of Salford during 2000-3, and this underwent laboratory trials and focus group evaluation. The 3 UK ETP Pilots officially ended on the 30th June 2003 [4], and the Salford project finished in September 2003. The four ETP models are described below. Note that evaluation of the 3 UK ETP pilots [6] determined that none of the 3 pilot models was good enough to build a national system from, and that a Common Model should be developed based upon the experiences gained. Since the Common Model was not available for analysis when this paper was written, we concentrate on evaluating the 4 published models from a CIA perspective. We believe this is still valuable, and can be extended to the Common Model once it has been finalised and published.

The Transcript Consortium Model

Within the Transcript Consortium model [11] (see figure 1) a prescriber generates a prescription for her patient, digitally signs it, and prints it out as a 2-D barcode on a paper prescription. An encrypted electronic version is sent directly to the PPA.

The patient takes the 2-D barcoded prescription to any pharmacy of their choice. The pharmacist scans in the barcode, validates the digitally signed prescription, dispenses the drugs and then generates a dispensed message and sends it to the PPA.

Figure 1: Transcript consortium model



For repeat prescriptions patients are asked to nominate a pharmacy of their choice, and the prescriptions are sent directly there by email, encrypted for the pharmacy. After dispensation the pharmacist sends 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.

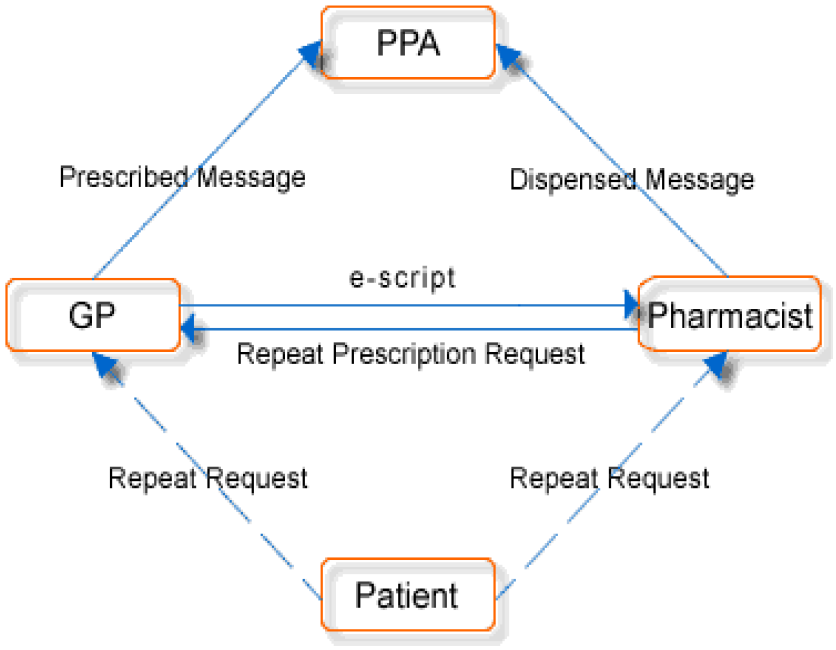
The Pharmacy2U Consortium Model

The Pharmacy2U Consortium model [12] relies solely on direct prescription messaging to patient designated Pharmacists (see figure 2). The patient visits their GP and at the end of the consultation is asked which pharmacy they wish to have dispense their prescription drugs. The GP then digitally signs the prescription, and sends it directly to the chosen pharmacy, encrypted with a key for the pharmacy. All pharmacists in the pharmacy share the same key, so any pharmacist is able to decrypt the prescription and dispense the drugs.

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.

Figure 2: Pharmacy 2U Consortium model

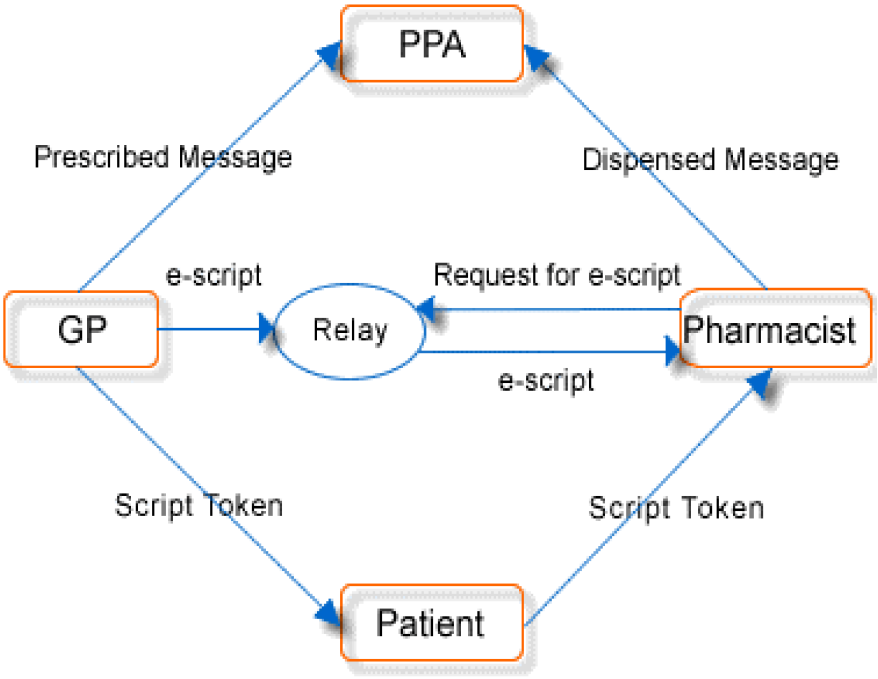


The SchlumbergerSema Consortium (Flexiscript) Model

The Schlumberger/Sema Consortium has settled for a relay model (see figure 3) [10] called Flexiscript. Prescriber's send digitally signed electronic prescriptions to a prescription data store, encrypted for the data store. An encrypted copy is sent directly

to the PPA. The system also generates a paper prescription containing a unique data store identification number for the patient and a barcode representation of the digitally signed prescription. The patient takes the prescription to any pharmacy and the pharmacist uses the identification number to retrieve the electronic prescription from the data store. The data store decrypts the prescription (this may happen upon arrival or when the prescription is requested), and re-encrypts it for the pharmacist upon demand.

Figure 3: SchlumbergerSema Consortium model



Patients may 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.

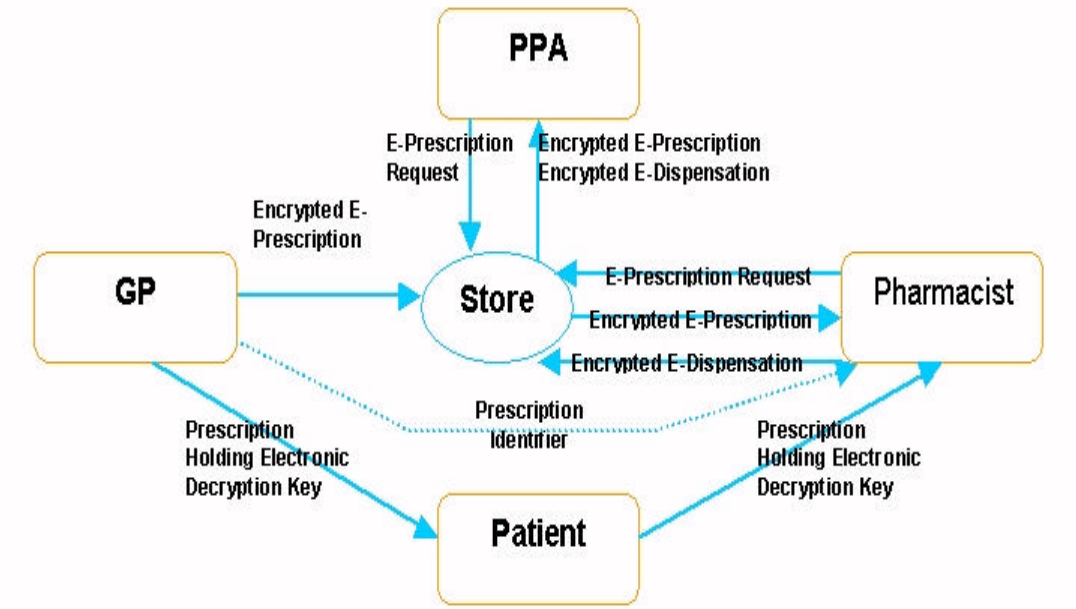
The Salford Model

The Salford model [16] is also a relay model (see figure 4). The GP digitally signs the electronic prescription and then the prescription is symmetrically encrypted and sent to the prescription store. The electronic prescription contains a copy of the symmetric key encrypted for the PPA, to allow the PPA to subsequently retrieve and decrypt the prescription. The patient is provided with a printed paper copy of the prescription containing in addition to the standard contents a reference barcode (which allows fast access to the prescription in the prescription store) and a symmetric key barcode (which is needed to decrypt the prescription in the store). The patient then goes to his pharmacy of choice and hands over his prescription, which allows the pharmacist to retrieve and decrypt the electronic prescription from the prescription store. The dispensed prescription (which may be endorsed) is encrypted for the PPA by the

pharmacist and returned to the prescription store. Periodically the PPA will retrieve dispensed and expired un-dispensed prescriptions from the prescription store.

If a patient has a preferred pharmacy and informs the GP about this, then an email message is sent to this pharmacy, encrypted for the pharmacy, containing the reference barcode and symmetric key barcode. This allows the pharmacy to retrieve the prescription from the prescription store prior to the patient's arrival, and to dispense the drugs ready for collection. This process can be applied to repeat prescriptions as well as acute prescriptions.

Figure 4: University of Salford ETP model



Prescribers' authorisations to prescribe, and pharmacists' authorisations to dispense are checked automatically by the Salford ETP system [17] before allowing the health care professionals to access the ETP system. Similarly patients' entitlements to free prescriptions are similarly checked on behalf of the pharmacist, thus relieving them of this burden for the majority of patients.

Analysing the Four ETP Models

We now analyse each of the four ETP models from the security perspectives of confidentiality, integrity and availability.

There are three aspects of confidentiality that need to be considered, namely: only authorised health care professionals should be able to participate in ETP, electronic prescriptions should be encrypted during transfer and only the dispenser chosen by the patient or his proxy should be able to access the patient's prescription. None of the three UK ETP pilots have an electronic authorisation system built into their models, and this is one of the requirements arising from the ETP evaluation report [6],

> *"Satisfactory mechanism(s) should be developed for the secure accreditation of GPs, registrars, locums, and pharmacies to prevent unauthorised use of the system"*

The Salford model does have a high security authorisation system built into its model. Authorisations are implemented using the X.509 authorisation framework [7] and the

PERMIS authorisation infrastructure [5]. X.509 is an international standard, which besides specifying an authorisation framework also standardises the authentication framework (public key certificates, certification authorities etc.) used by all four ETP models. We thus believe that it is the perfect framework to use for ETP authorisation, since ETP is already using the same standard for the authentication and integrity of its electronic prescriptions. PERMIS is an implementation of the X.509 authorisation framework, and is internationally distributed as part of the US National Science Foundation's Middleware Initiative software release [8]. PERMIS is shortly to be piloted as a national authorisation infrastructure for the UK academic community, and therefore we believe it is highly suitable for use in ETP [17].

Encrypting the electronic prescriptions during transfer is especially difficult to achieve if the ETP system is to preserve the confidentiality of the electronic prescription and the patient's freedom of choice to choose a pharmacy right up to the point of dispensation. This is because the prescribing GP will not know at the time of prescription creation who the final recipient pharmacist is to be, and therefore cannot encrypt the prescription for the pharmacist. Consequently the four models have addressed this dual problem in different ways.

The Pharmacy2U consortium has chosen to remove patient's freedom of choice at the time of prescribing, and the GP encrypts and emails the prescription to the patient's chosen pharmacy. Thus the patient cannot change their mind after leaving the prescriber's surgery. The SchlumbergerSema (Flexiscript) consortium retains patient freedom of choice up to the point of dispensation, but with a small loss of confidentiality. The electronic prescription is first encrypted for the central prescription store, but is then decrypted by the store, and re-encrypted for the pharmacy after the patient has chosen which pharmacy to go to. Thus anyone with access to the central store has the potential to view all prescriptions, plus any pharmacist has the potential ability to retrieve any and all prescriptions by searching for them in the store by trial and error. The Flexiscript implementation has limited this last weakness by only giving pharmacists a pre-configured number of erroneous attempts before blocking their access to the prescription store [13]. The Transcript consortium model is a hybrid. It preserves patient freedom of choice for acute prescriptions, by removing the requirement to encrypt them since they are not transferred electronically over the network. This model writes the prescription unencrypted to a 2-D barcode on the paper script, and anyone with access to the paper script can read the contents of the prescription, in much the same way as today. For repeat prescriptions the Transcript model removes the patient's freedom of choice at the time of prescribing, by encrypting the prescriptions for the chosen pharmacy (in much the same way as the Pharmacy2U model). Only the Salford model preserves patient freedom of choice up to the point of dispensation, whilst not compromising the confidentiality of the electronic prescription. This is because the electronic prescription is symmetrically encrypted using a one off symmetric key, and is sent to the prescription store encrypted. Neither the prescription store nor any pharmacist are able to decrypt the prescription, as they do not know the key. The key is written (within a barcode) to the paper prescription given to the patient, thus only the pharmacy chosen by the patient has the ability to decrypt the electronic prescription after the patient arrives [9]. For patients who prefer to pre-select a pharmacy, an encrypted email is sent to the pharmacy containing the decryption key.

Turning now to consider integrity, all four models use digital signatures. A digital signature provides a unique cryptographic binding of the contents of an electronic document to the private key used to create the digital signature. Thus digital signatures provide data integrity and originator integrity, providing the private key used to create the digital signature remains in the sole possession of the document originator. Originator integrity for a digital signature is thus not quite the same as that of a hand written signature, since it is not possible to lend someone your hand, but it is possible to lend someone your private key. Originator integrity for a digital signature is more akin to that of a bank claiming that money retrieved from a bank account by an ATM card must have been withdrawn by the account holder, since the latter should have been the only person in possession of the ATM card and the PIN used to activate it. Of course, we now know that this is not always the case, due to well publicised court cases of ATM withdrawals being made by non-account holders. Thus if prescription creators keep their private keys and PINs solely for their own use, we will have originator integrity. But if prescribers lend their private keys and PINs to colleagues, or they are stolen by someone else, we will not have originator integrity (although we should have accountability).

Digital signatures also have the ability to prevent the duplication of electronic prescriptions, providing each signed prescription contains a unique number and a validity time, and the ETP system ensures that no two identical prescriptions with the same unique number can exist during the validity time (note that repeat prescriptions are not duplicates and will have different unique numbers). The models that rely on relays (the Flexiscript and Salford models) can simply ensure that duplicate prescriptions with the same unique number are rejected by the relay. The acute Transcript model relies on detection of paper prescription duplication by the pharmacy, but it is very difficult to detect duplicates sent to different pharmacies. The Pharmacy2U and Transcript repeat prescription models will have to rely on the prescription generation software not to generate duplicate prescription messages, but as we all know this is extremely difficult to achieve in practice, since we all do occasionally receive duplicate email messages.

Equally as important is the detection of concurrent duplicate dispensations and fraudulent claims after dispensation that prescriptions have been lost and never dispensed. The Salford system has mechanisms to prevent both of these scenarios. Once a pharmacist retrieves a prescription from the relay, a lock is placed on that prescription record, which prevents any other pharmacist from being able to dispense the same prescription. After dispensation a message is sent from the pharmacist to the prescriber stating that the prescription has been dispensed preventing a patient fraudulently claiming a lost prescription. The Flexiscript model should also be able to enforce a lock to prevent concurrent dispensations, but in the pilot service only 2 out of the 3 pharmacy systems actually did this [13]. There is insufficient documentation in the public domain to determine how the Flexiscript model protects against fraudulent claims of lost prescriptions. The Pharmacy2U and Transcript repeat prescription models are (at least partially) protected against fraudulent claims of lost prescriptions, since the patient is never given the prescription (although this might not stop some patients from claiming that the system has lost their prescriptions). These models also rely on the prescription generation and messaging software not to generate duplicate prescription messages, thus eliminating the chance of duplicate dispensations. Nevertheless, we believe it would still be a sensible precaution to build

duplication checking into the pharmacy software, to ensure that if/when duplicate prescription messages are received the duplicates are not dispensed.

Finally we review all four models from the aspect of availability. Factors that need to be considered are the existence of single points of failure, how the models cater for any failures, and the scalability and performance of the different systems. The Flexiscript model has a single prescription store through which all prescriptions are relayed. If this fails then the whole ETP system fails [13]. Flexiscript also uses a single private key server from which prescribers must download their signing keys prior to prescription creation. If this is unavailable then no-one is able to sign and send an electronic prescription [13]. Whilst the Salford model also uses a prescription store, it has been designed to be configurable, so that any number of prescription stores can be used, up to one per prescribing surgery if required. Thus there is no reason to have a single point of failure in the Salford model. The Pharmacy2U model uses a single directory server to hold all users' public key certificates, for both encrypting messages and validating signatures. If this fails, then new prescriptions cannot be sent, and those that have already been sent cannot be validated [13]. The Transcript model does not appear to have a single point of failure that would stop the whole ETP system from working [13].

How do the models cope with failures in the ETP system or its supporting infrastructures? The Flexiscript and Salford models both print additional information onto an existing FP10 prescription form. The Transcript model does so for acute prescriptions, but not for repeat prescriptions, which are sent directly to the pharmacy by email. The Pharmacy2U model always sends prescriptions directly by email.

Any failures occurring in the email system or in the pharmacy end systems of the Pharmacy2U or Transcript repeat prescription models will cause the pharmacies to be disabled from participating in the prescription process. The pharmacies will not have a failsafe system to fall back to. In the case of the Transcript repeat prescriptions model, the patients and the prescribers could fall back to the paper based acute prescription model, but at some inconvenience to the patient if the failure occurs after the repeat prescription has been sent (but not received) electronically.

Those models that use supplemented FP10 prescription forms (Transcript acute, Flexiscript and Salford) do have a failsafe fallback procedure in the case of any and all ETP failures – they simply revert to paper based processing. However the Transcript and Flexiscript consortia have stated that the use of supplemented FP10 forms is a short term expedient measure to allow the patient to take his prescription to either a pharmacy participating in the ETP pilot or one that is not, and they expect the forms to be phased out once ETP is implemented nationally [6, 10,11]. In the case of the Salford model, the use of the FP10 form is an explicit permanent design feature made for several reasons:

- firstly the patient sees no difference in procedure when ETP is introduced,
- secondly, GPs said they liked giving the patient a paper prescription as it signalled the end of their session with them [14],
- thirdly, the enhanced paper prescription can be used throughout the transition to ETP, without inconveniencing any of the participants,
- fourthly, the patient remains free to choose the pharmacist right up to the moment of dispensing, and

- lastly, the system is resilient to all technology failures since the paper prescription provides the ultimate fallback, even in the case of a power cut.

The authors believe the last two points are important from the perspective of availability, since the paper prescription provides for permanent availability of the prescription service and flexibility even in the case of complete ETP technology or pharmacy failures.

Finally we consider scalability and performance. The performance of the 3 UK pilots has been inadequate "*The evaluation reports describe shortcomings in performance and usability that appear to be caused by inadequate system design or faulty implementation*" [6]. We recognised very early on that performance would be a critical success factor for ETP. We also suspected that the use of XML transfer syntax, as mandated by the Department of Health in its ETP XML message DTDs, would not be optimal from a performance perspective. Consequently we performed some comparative performance tests for XML and ASN.1 BER [21, 22]. ASN.1 is a mature international standard used by X.509 public key certificates, encrypted email (S/MIME), and mobile phones etc. We found that ASN.1 BER would outperform XML by approximately an order of magnitude [18]. Subsequent to this, Sun have also published a paper about Fast Web Services [19] that supports our findings. We thus believe that the DoH would do well to reconsider the use of XML as the transfer syntax for electronic prescriptions.

We are not aware of any scalability tests that have been published by the 3 UK ETP pilots. The Flexiscript consortia are the only UK ETP pilot to say that scalability tests have been performed, but they would not release these results to the ETP evaluators [20]. Salford has performed scalability tests for its central relay, and demonstrated that 10 million prescriptions can easily be stored on a modest PC. Additional performance results are currently being prepared. The Salford model has been designed with scalability in mind, by allowing any number of prescription stores to be used, ranging from one central national store to one store per GP surgery. Thus we believe that it is infinitely scalable.

Conclusions

In this paper we have looked at the security requirements for ETP, from the perspectives of confidentiality, integrity and availability. We have then described and evaluated the four published UK ETP models from these perspectives. We have shown that each of the 3 UK ETP pilot models are deficient in one way or another, and have shown how the Salford model has attempted to address all the security requirements for ETP. We believe that this paper will be valuable as a basis for a future evaluation of the Common Model, once it has been finalised and published, so as to ensure that it does not suffer from the same deficiencies as the 3 UK ETP pilot models.

References

[1] UK Government, "Data protection act 1998 (c.29)", Crown Copyright 1998
[2] Department of Health "Confidentiality, the NHS Code of Practice", November 2003. Available at http://www.doh.gov.uk/ipu/confiden/protect/ (December 2003)
[3] Department of Health, The Caldicott Committee "Report on the review of patient-identifiable information", December 1997, Available at http://www.doh.gov.uk/ipu/confiden/report/ (December 2003)
[4] See http://www.ppa.org.uk/news/etp.htm (December 2003)

[5] D.W.Chadwick, A. Otenko, E.Ball. “Implementing Role Based Access Controls Using X.509 Attribute Certificates”, IEEE Internet Computing, March-April 2003, pp. 62-69.
[6] Sowerby Centre for Health Informatics at Newcastle. “Electronic Transmission of Prescriptions Evaluation of Pilots *Summary Report”*. Dept of Health, July 2003
[7] ISO/ITU-T Rec. “X.509 (2000) The directory: Public Key and Attribute Certificate Frameworks”
[8] See http://www.nsf-middleware.org/ (December 2003)
[9] E.Ball, D.W.Chadwick, D.Mundy, “Patient Privacy in Electronic Prescription Transfer”, IEEE Security & Privacy magazine, March-April 2003, pp77-80
[10] See http://www.flexiscript.co.uk/etp/htm/ (December 2003)
[11] See http://www.pharmed.org.uk/pages%20Jan%202002/pilot2.htm (December 2003)
[12] See http://www.ppa.org.uk/news/etp-consortia/pharmacy2u.htm (December 2003)
[13] QinetiQ. “Report on Security Assessment of the ETP Pilots”. Version 6, 14 July 2003, produced for the Department of Health.
[14] Mundy, D.P, Chadwick, D.W, Ball, E, Marsden, P, Bell, D, Whatley, J.E, Sobreperez, P, New, J, "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 2003
[15] 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) Ed. Ralph H. Sprague, Jr. Abstract p 156. Main paper on accompanying CD-Rom. Also available from http://www.hicss.hawaii.edu/HICSS_35/HICSSpapers/PDFdocuments/HCTHC01.pdf
[16] Mundy, D.P. and Chadwick, D.W. “A system for secure electronic prescription handling”, Second International Conference On The Management Of Healthcare And Medical Technology On: The Hospital of the Future Bringing Together Technology, Health Care and Management. Abstract and Main Paper on accompanying CD-Rom, Stuart Graduate School of Business, Center for the Management of Medical Technology, Illinois Institute of Technology, Chicago, Illinois, USA, July 28-30, 2002. Paper also available from http://sec.isi.salford.ac.uk/download/HospitalFutureConf.pdf
[17] D.W.Chadwick, D.Mundy. "Policy Based Electronic Transmission of Prescriptions". Proc of Fourth IEEE Int Workshop on Policies for Distributed Systems and Networks, Lake Como, Italy, 4-6 June 2003, p197-206
[18] D.Mundy, D.W.Chadwick, A.Smith, “ASN.1: An XML Alternative for Performance and Security”, IT Professional magazine, Jan/Feb 2004
[19] P. Sandoz, S. Pericas-Geertsen, K. Kawaguchi, M. Hadley, and E. Pelegri-Llopart. “Fast Web Services”, Aug 2003, Available from: http://java.sun.com/developer/technicalArticles/WebServices/fastWS/
[20] QuinetQ. “Final Technical Evaluation Report”, Version 6, 14 July 2003, produced for the Department of Health
[21] ITU-T Recommendation X.680 (1997) | ISO/IEC 8824-1:1998, Information Technology - Abstract Syntax Notation One (ASN.1): Specification of Basic Notation
[22] ITU-T Recommendation X.690 (1997) | ISO/IEC 8825-1,2,3:1998 Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER)