

	<b>Secure Use of the New NHS Network (N3)</b>			
	<b>Programme</b>	NPFIT	<b>Document Record ID Key</b>	
	<b>Sub-Prog / Project</b>	Information Governance	NPFIT-FNT-TO-IG-GPG-0003.01	
	<b>Prog. Director</b>	Mark Ferrar	Status	Approved
	<b>Owner</b>	Tim Davis	Version	1.0
	<b>Author</b>	Phil Benn	Version Date	16/02/2006

## Secure Use of the New NHS Network (N3): Good Practice Guidelines

**Amendment History:**

Version	Date	Amendment History
0.1	13/09/2005	First draft for comment
0.2	20/10/2005	Second draft with additional information
0.3	10/11/2005	Third draft following review comments
0.4	29/12/2005	Minor changes to document format
1.0	16/02/2006	Approved

**Forecast Changes:**

Anticipated Change	When
Annual Review	March 2007

**Reviewers:**

This document must be reviewed by the following:

Name	Signature	Title / Responsibility	Date	Version
Malcolm McKeating		IG Security Team Manager		1.0
Tim Davis		Head of Information Governance		1.0

**Approvals:**

This document must be approved by the following:

Name	Signature	Title / Responsibility	Date	Version
Mark Ferrar		Director of Infrastructure		1.0
Tim Davis		Head of Information Governance		1.0

**Distribution:**

Information Governance Website: <http://nwww.connectingforhealth.nhs.uk/>

**Document Status:**

This is a controlled document.

Whilst this document may be printed, the electronic version maintained in FileCM is the controlled copy. Any printed copies of the document are not controlled.

**Related Documents:**

These documents will provide additional information.

Ref no	Doc Reference Number	Title	Version
1	NPFIT-SHR-QMS-PRP-0015	Glossary of Terms Consolidated.doc	12.0

---

**Contents**

1	Introduction.....	4
1.1	Aims and Objectives.....	4
1.2	Assumed Reader Knowledge.....	4
1.3	Background.....	5
2	The New NHS Network (N3) .....	5
3	Data Encryption and Privacy .....	6
3.1	Encryption Levels.....	7
3.2	Application-Level Encryption .....	7
3.2.1	Secure Sockets Layer (SSL) v3 and TLS	7
3.3	Network-Level Encryption .....	9
3.3.1	IPsec	9
4	Glossary .....	10

# 1 Introduction

This guide addresses the major security issues associated with the transmission of Patient Identifiable Data (PID) and other sensitive electronic information over the New NHS Network (N3). Detailed technical knowledge of encryption standards and techniques is not required.

It does not describe security guidelines for the transmission of sensitive information via any means other than the N3 network.

You will find guidance on ensuring the confidentiality and integrity of sensitive information transmitted across the N3 network. This includes:

- The use of encryption technologies.
- The application of encryption at different levels of the network architecture.

## 1.1 Aims and Objectives

The following information provides a knowledge-based framework that will help maintain best practice values in your own organisation. In using this guide you will be conforming to best practice and therefore avoid some of the consequences of non-compliance.

After completing this guide you should understand:

- The minimum standards applicable to the transmission of PID or other sensitive electronic information over the N3 network.
- The procedures and mechanisms for the control of PID, or other sensitive electronic information (in a NHS or other healthcare environment), when using the N3 network.

## 1.2 Assumed Reader Knowledge

- A general familiarity with the requirement to protect patient sensitive data at all times.

Further information on network security and related matters is available from the NHS Connecting for Health Information Governance website.

## 1.3 Background

N3 is a private Wide Area Network (**WAN**). Connection is therefore strictly limited to authorised endpoints. All organisations wishing to make a new connection to N3 are responsible for ensuring that their connection to the WAN does not compromise the security measures already in place.

- N3 is a private network consisting of thousands of PCs, servers, printers and other items of equipment all acting as the nodes or endpoints on the network. Information is unencrypted when transmitted over the network therefore confidentiality of sensitive information within N3 is not assured. However, all National Applications encrypt data using Transport Layer Security (TLS). It is therefore advisable for Existing Systems to take the appropriate measures to ensure that sensitive data is secure before connecting to N3.
- N3 faces numerous threats to security as a result of incompletely protected partner networks or connections to uncontrolled external networks such as the internet. These threats are continually evolving in both strength and frequency: ongoing vigilance against these threats and the maintenance of strict security standards are essential to the continuing success of N3.

## 1.4 Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NHS Connecting for Health. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. NHS Connecting for Health shall also accept no responsibility for any errors or omissions contained within this document. In particular, NHS Connecting for Health shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

## 2 The New NHS Network (N3)

The N3 infrastructure connects organisations, such as non-NHS healthcare providers and approved third-party partners, to other organisations within the NHS. Currently, this infrastructure is a managed service provided and supported by a number of contractors with British Telecom (**BT**) acting as service integrator.

BT Consultancy & Systems Integration (BT C&SI) is delivering the National Application Service Provider (**NASP**) and London Local Service Provider (**LSP**). BT Exact (BT's IT and operations business) supplies the Data Centre hosting while British Telecom N3 Service Provider (**BT N3SP**) manages the N3 network.

BT provides certain guarantees regarding the protection of the network infrastructure – this makes the network a private transport medium. The N3 infrastructure is therefore suitable for consideration as a WAN.

Although the N3 is private, it is not 'secure'. The network is a transport mechanism for data and as such does not encrypt (or similarly protect) the data transmitted. Users of the network are required to apply such methods of information confidentiality and integrity as are appropriate to the data transmitted and the applications used.

Further information on suitable levels of encryption and protection is available in the *Approved Cryptographic Algorithms: Good Practice Guidelines* document.

### 3 Data Encryption and Privacy

Users of the N3 are strongly encouraged to implement a level of information confidentiality and integrity whenever transmitting sensitive data.

Data encryption allows you to create secure connections over insecure channels. Encrypting network traffic provides two useful guarantees: privacy and authentication:

- Privacy - a transmitting endpoint encrypts data. This transmitting endpoint then sends this data over an unsecured network. The receiving end-point then decrypts the data.
- Authentication - ensures that both the transmitting and receiving endpoints are able to identify each other as legitimate parties prior to (and during) communicating.

The use of Transport Layer Security (**TLS**) based encryption is the preferred method for securing applications at the transport layer.

Alternatively, the imposition of encryption at the network layer - using Internet Protocol Security (**IPSec**) - is standard practice when implementing Virtual Private Networks (**VPNs**).

Further information is available in the *Site-to-Site Virtual Private Networks (VPNs): Good Practice Guidelines* document.

## 3.1 Encryption Levels

Encryption can take place at various levels; the most common being within the application, at the network, or on the network link itself:

- **Application-level encryption** is a particularly effective approach when transmitting sensitive data on a 'one-to-many' basis. For this method the application (client and server) has the encryption solution built in. The application data payload is then encrypted making the solution network independent. An example of application-level encryption is the secure version of the Hyper Text Transport Protocol (**HTTPS**) used primarily for e-commerce and online shops.
- **Network-level encryption** takes place at the Internet Protocol (**IP**) layer and operates upon the entire data packet. It is a useful alternative when application level encryption is not an option, or when multiple streams of application data need protection between a number of separate endpoints.

It works by creating an encrypted tunnel between two endpoints. The endpoints may be any specific devices capable of supporting encryption at the IP layer, such as firewalls or routers. Alternatively, host systems are capable of performing network level encryption using client software, which again is application independent.

Sensitive data is secure whilst traversing the encrypted tunnel. However, it is important that the data remains secure when moving around the Local Area Network (**LAN**) of each endpoint.

Further information is available in the *Securing the Local Area Network (LAN): Good Practice Guidelines* document.

## 3.2 Application-Level Encryption

### 3.2.1 Secure Sockets Layer (SSL) v3 and TLS

SSL Version 3 is one of the most widely used security mechanisms on the Internet<sup>1</sup>. The Internet Engineering Task Force (**IETF**) has renamed SSLv3 as TLS<sup>2</sup>.

---

<sup>1</sup> Documented by The Internet Engineering Task Force (IETF) from [www.ietf.org](http://www.ietf.org).

<sup>2</sup> [RFC 2246](#) from the IETF documents the TLS protocol and identifies itself in the version field as SSL 3.1.

Web browsers make extensive use of SSL and TLS to provide a secure connection for the transfer of sensitive data such as credit card details or similarly sensitive customer information.

There are a number of subtle differences between SSLv3 and TLSv1. However, from a user perspective the protocols remain much the same in operation. For example an SSL-protected HTTP transfer (**HTTPS**) uses port 443 while a standard http transfer uses Internet Protocol (**IP**) port 80<sup>3</sup>. Thus, <https://www.nhs.uk/> causes an SSL enabled browser to open a secure SSL session to port 443 at [www.nhs.uk](https://www.nhs.uk/). The user may only notice a padlock in the bottom right hand corner of Internet Explorer, indicating a secure session.

SSL, like most modern security protocols, uses cryptography to ensure privacy. This process uses a Public Key Infrastructure (**PKI**) - PKI employs a public and a private cryptographic key pair to ensure privacy:

- A SSL session is established. The server begins by announcing a public key to the client. No encryption is in use initially, so both parties (and any eavesdropper) can read this key.
- The client encrypts a reply to the server using the server's public key which only the server can decrypt. This means that the client can transmit information to the server in a way that no one else can decode.

To initiate the encrypted session the client generates 46 bytes of random data and forms them into a single, very large number in line with Public Key Cryptography Standards (**PKCS#1**)<sup>4</sup>. The server's public key encrypts them and the results sent to the server. Only the server, with its private key, can decode the information to determine the 46 original bytes.

This shared secret is utilised to generate a set of conventional ARCFOUR (**RC4**) cipher keys to encrypt the rest of the session<sup>5</sup>. X.509 certificates (the most widely used standard for defining digital certificates) are utilised to authenticate the server and (optionally) the client.

---

<sup>3</sup> A port is a network doorway or address numbered from 0 to 65536. This number is used to transmit data to and

<sup>4</sup> See <http://www.rsasecurity.com/rsalabs/node.asp?id=2125> for further information on PKCS.

<sup>5</sup> See <http://www.rsasecurity.com/rsalabs/node.asp?id=2250> for further information on RC4.



### 3.3 Network-Level Encryption

#### 3.3.1 IPsec

IPsec is a security framework that operates at the network layer. It extends IP packet header (using additional protocol numbers - not options). It therefore has the ability to encrypt any higher layer protocol, including arbitrary Transmission Control Protocol (**TCP**) and User Datagram Protocol (**UDP**) sessions. It offers the greatest flexibility of all the existing TCP/IP cryptosystems.

A common use of IPsec is the construction of a VPN in which one or more segments of a private network link up over a public network or WAN using encrypted tunnels. This allows applications on the private network to communicate securely without any local cryptographic support because the VPN routers perform both the encryption and decryption.

IPsec is well suited for this environment, more so than tunnelling Point to Point (**PPP**) protocols over SSL or Secure Shell (**SSH**), because it operates directly on the IP packets and preserves a one-to-one correspondence between packets inside and outside the network.

Further information on the implementation of IPsec VPNs is available in the *Site-to-Site Virtual Private Networks (VPNs): Good Practice Guidelines* document.

## 4 Glossary

**ARCFOUR:** Also called RC4. A stream cipher, widely used in protocols such as Wired Equivalency Privacy (**WEP**) and Secure Sockets Layer (**SSL**). It falls short of modern cryptographic standards but is suitable for practical use in legacy or existing systems.

**BT:** British Telecommunications Plc. The current service provider for the N3 network.

**BT N3SP:** British Telecom N3 Service Provider. N3 is the name for the New NHS Network that will provide wide area networking services to the NHS in England. The NHS has chosen BT as the Service Provider for the N3 network. In this role BT is referred as the N3SP. BTN3SP has formulated the Internet Protocol (**IP**) addressing policy for N3.

**HTTPS:** Hypertext Transfer Protocol over Secure Socket Layer. A method of using HTTP which moves information using SSL or TLS. It is not a separate protocol but a URI scheme that allows a system to know that HTTP is to be used but with additional security measures applied to the transactions.

**IETF:** The Internet Engineering Task Force. A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

**IP:** Internet Protocol. A data oriented communications protocol. IP version 4 is the common element found in today's internet.

**IPSec:** Internet Protocol Security. A method of securing IP communications for security that takes place at the network or packet processing layer of network communication.

**LAN:** Local Area Network. A local computer network for communication between computers; especially a network connecting computers and word processors and other electronic office equipment to create a communication system between offices.

- LSP:** Local Service Provider. A provider of LSP Services which has been appointed by the Authority for a Cluster. Responsible for making sure the new systems and services delivered through the NPfIT meet local requirements and are implemented efficiently.
- N3:** The New NHS Network. A private Wide Area Network consisting of thousands of PCs, servers, printers and other items of equipment. Information is unencrypted when transmitted over the network therefore confidentiality of sensitive information within N3 is not assured.
- NASP:** National Application Service Provider. A supplier selected to provide one of the NPfIT national solution services.
- PID:** Patient Identifiable Data. Key identifiable information includes: patient's name, address, full post code, date of birth, pictures, photographs, videos, audio-tapes or other images of patients. PID also encompasses NHS local patient identifiable codes or anything else that could identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within small population may allow the identification of individuals.
- PKCS#1:** Public Key Cryptography Standards. PKCS#1 defines the format of RSA encryption.
- PKI:** Public Key Infrastructure. Enables users of a basically unsecured public network (such as the internet) to securely and privately exchange data through the use of a public and a private cryptographic key pair, obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.
- PPP:** Point to Point Protocol. A data transfer protocol which operates at the Data Link Layer.
- RC4:** See ARCFOUR (above).
- SSH:** Secure Shell protocol. Using SSH, a user can log into a server and all of their interactions are tunnelled through an encrypted session so that even if someone intercepts the data, all they will encounter is gibberish.

- SSL:** Secure Sockets Layer. A protocol designed to provide secure communications across the Internet.
- TCP:** Transmission Control Protocol. A protocol which works with IP to ensure that packets travel safely on the Internet. This is the method by which most Internet activity takes place.
- TLS:** Transport Layer Security. A protocol designed to provide secure communications across the Internet designed as a successor to SSL. It uses the same cryptographic methods but supports more cryptographic algorithms.
- UDP:** User Datagram Protocol. A protocol which allows the transfer of information to be transferred across IP networks. It is similar in operation to TCP; however it lacks the reliability and ordering guarantees, and is stateless. It offers higher performance due to lower overheads in processing and delivery.
- VPN:** Virtual Private Network. A private data network that makes use of the public telecommunication infrastructure; privacy is maintained through the use of a tunnelling protocol and security procedures.
- WAN:** Wide Area Network. A computer network that spans a relatively large geographical area, typically a WAN consists of two or more local-area networks (**LANs**). The largest WAN in existence is the internet.
- WEP:** Wired Equivalency Privacy. A security system that uses a series of keys on both sides of a wireless transmission to encrypt data for secure transmission. WEP is not considered secure and there is a range of freely available, pre-existing software programs designed to break its encryption.
- X.509:** The ITU-T standard for Public Key Infrastructure (**PKI**). It specifies information and attributes required for the identification of a person or a computer system.