NHS Restricted ETP Message Signing Requirements						
Programme	NHS CFH	**NPFIT-ETP-EDB-0064**				
Sub-Prog/ Project	ETP	*National Prog*	*Org*	*Prog /Proj*	*Doc*	*Seq*
Prog. Director	Tim Donohoe	**NPFIT**	**ETP**	**EDB**	**0064**	
Sub Prog/ Proj Mgr	Ian Lowry					
Author	John Whiteside	Version No		2.0		
Version Date	July 2007	Status		Approved		

Electronic Transmission of Prescriptions
Message Signing Requirements

Amendment History:

Version	Date	Amendment History	Author
1.0	Nov 2004	Initial version	Graham Jack
1.1	December 2004	Changes to remove ni structure and sign a single hash • Modified tables to remove references to ni structure • Removed references to subcomponents	Graham jack
1.2	Jan 2005	Changes in response to feedback comments: • Section 3: added column to table, documenting requirements for content commitment dialog. • Section 5: minor corrections to table	Graham Jack
1.3	May 2005	clarifications in response to feedback comments: • Section 3: signature elements author.effectiveTime changed to author.time • Section 5: sorted table on message name Changes in response to change of scope for Full ETP: • Section 3: removed entries for PS, PA and related messages – not in scope • Section 2: added scope section to list those messages not covered	Graham Jack
1.4	June 2006	Updated version number of referenced documentation to the latest versions Updated the referenced transforms to the versions to be used with MIM4.1 messages	John Whiteside
1.5	March 2007	Updated version number of referenced documentation to the latest versions And added a transform which may be used in removing superfluous whitespace from thesignedInfo element.	John Whiteside
1.6	June 2007	Clarified EPS Requirements as per TO request	John Whiteside
1.7	July 2007	Presentational Ammendments as per TD's Comments	John Whiteside

Reviewers:

This document must be reviewed by the following. Indicate any delegation for sign off.

Name	Signature	Title / Responsibility	Date	Version
Ian Lowry		ETP Programme Manager		1.6
Rob Gooch		ETP Technical Architect		1.6

Approvals:

This document requires the following approvals.

Name	Title	Signature	Version
T Donohoe	Programme Director – ETP		1.7

Document Location

This document is only valid on the day it was printed. Please contact the Document Controller for location details or printing problems.

This is a controlled document.

On receipt of a new version, please destroy all previous versions (unless a specified earlier version is in use throughout the project).

Related Documents:

These documents provide additional information.

Ref no	Doc Reference Number	Title	Version
1	NPFIT-NPO-GEN-IP-0067	Glossary of Terms Consolidated.doc	
2	NPFIT-FNT-TO-IG-0019	Digital Signing and Non-Repudiation	2.0
3	NPFIT-NDA-COM-TZ-0160	NPfIT Message Implementation Manual	4.2.00
4	NPFIT-ETP-EDB-0025	Prescribing System Compliance Specification	3.0
5	NPFIT-ETP-EDB-0024	Dispensing Systems Compliance Specification	3.0

Contents

1. Purpose

This document describes the specific requirements for implementing advanced electronic signatures within Release 2 of the EPS system for prescribing and dispensing systems.

It should be used in conjunction with the requirements for advanced electronic signatures: Digital Signing and Non-Repudiation [2]

2. Scope

This version of the document provides all of the information necessary to implement signing for the messages required for the EPS Release 2.

The following messages are out of scope for EPS Release 2 and are not covered here:

024003	Protocol Supply Notification
114002	Personal Administration Notification
142003	Protocol Supply Notification with Claim Information
114001	Personal Administration Notification with Claim Information

3. Messages without signatures

The following messages do not require a signature to be generated or checked.

Note that some of these messages include a SignatureText block – the document: Digital Signing and Non-Repudiation [2] provides guidance on how to encode the signature block in the case where no signature is required.

Message Type (PORX_MTxxxxxx)	Message Name
135001	Cancel Request
135201	Cancel Response
142001	Dispense Claim Information
024001	Dispense Notification
142004	Dispense Notification with Claim Information
121301	Dispense Proposal Return
121302	Dispense Proposal Return Rejection
142006	Dispense Reimbursement Claim
142201	Dispense Reimbursement Claim Rejection
024201	Dispense Rejection
121001	Nominated Prescription Release Request
132204	Parent Prescription Rejection
121002	Patient Prescription Release Request
014001	Personal Administration Claim Information
114002	Personal Administration Notification
114001	Personal Administration Notification with Claim Information
114003	Personal Administration Reimbursement Claim
014002	Personal Administration Reimbursement Rejection
121201	Prescription Release Rejection
142002	Protocol Supply Claim Information
024003	Protocol Supply Notification

142003	Protocol Supply Notification with Claim Information
142005	Protocol Supply Reimbursement Claim
142202	Protocol Supply Reimbursement Rejection

4. Transforms

Transforms are provided to extract the relevant parts of a message for signing. The following table lists the names of the transforms provided and the relevant version number for each message to be signed. Whenever a transform is changed in such a way that it changes the output in terms of extracted field, the version number will be incremented.

These transforms are run against the HL7 message payload before the signature is generated. The output from the transformation is what is canonicalised, hashed and signed.

Message Type	Message Name	Transform Name	Version
132004	Parent Prescription	Prescription	V0r1
122002	Prescription Release Response	Prescription	V0r1

In addition, the digital signature standards do not provide recommendations on handling superfluous whitespace between elements. As this needs to be handled consistently across all prescribing and dispensing systems it has been made a requirement that all superfluous whitespace of this nature is removed before hashing the canonicalised xml. During the process of generating (and validating) a prescription (described in depth in ref [2]), two hashes are created. The first hash is performed on the canonicalised output of the data marshalled using the above transform. This transform has been designed to remove superfluous whitespace during the marshalling step so no further actions should be required if this transform is used.
The second hash is generated on the signedInfo block prior to signing the hash (described in depth in ref[2]). In order to remove superfluous whitespace prior to this second hash, the system can either implement a proprietary mechanism or utilise a transform created by CfH. This transform is as described below.

Element	Transform Name	Version
SignedInfo	SignedInfowhitespace	V0r1

5. Requirements for Prescribing Systems

5.1. Messages sent to the SPINE

These messages are generated by prescribing or dispensing systems and sent to the ETP SPINE.

The table identifies the starting point in the schema for each of the elements which is to be included in the advanced electronic signature and the message element into which the signature should be inserted.

In addition, for each message that is signed, the table defines what information must be displayed as part of the accompanying content commitment dialog.

Message Type (MTxxxxxx)	Message Name	Signature data elements (Root classes)	Signature To Be Attached To	Content Commitment display
132004	Parent Prescription	author.time[1] pertinentPrescription.id [2] author.AgentPerson RecordTarget pertinentLineItem (exclude repeatNumber.low)	Author.signatureText	The values that are to be printed on the related PF10

[1] This time value must be set to the time at which the signing process is initiated (that is, the time at which the author enters his/her PIN)

[2] ID appears twice as part of the pertinent prescription block. The one to be included in the signature is the one containing the GUID.

5.2. Applying Advanced Electronic Signatures to prescriptions

For the requirements on when to apply an Advanced Electronic Signature to a prescription, please see [4] “Prescribing System Compliance Specification”

5.3. Requirements for non repudiation display

The Information Governance advanced electronic signature specification Ref. [2] defines the process for generating a signature.

For each message that requires a signature, a compliant system must implement a non-repudiation dialog with the signing user, displaying the information to be signed and prompting the user to confirm that he/she wishes to proceed with the signature.

Ref	Requirement
5.3.1	In addition to displaying the information to be signed, the system shall ensure that the following dialog is displayed when then the user is entering their pin “The system will sign the content displayed here on your behalf, by means of information stored on your smart card as an Advanced Electronic Signature. By entering your PIN here you affirm your intention to digitally sign and issue this electronic prescription. Do you wish to proceed?”
5.3.2	A compliant system may implement a “batch signing” version of any transaction to streamline commitment activities. In this case, the user is prompted to enter a PIN only once and, if correct, a signature is applied to each of the messages in the batch. The commit dialog must constructed to ensure that the user has an opportunity to review each transaction in the batch before the commit prompt is displayed and to decide which ones are to be signed and which not.

5.4. Smartcards and the Content Commitment Certificate

A minimum of two certificates will be present on a prescribers smartcard - an authentication certificate and a content commitment certificate. When creating electronic signatures only the content commitment certificate must be used (similarly, the certificate containing the prescribers public key that is placed in the prescription message must have been extracted from the content commitment certificate).

Ref	Requirement
5.4.1	Prescribing systems must use the content commitment certificate issued by the correct authority on the prescribers smartcard during the signing

	process. The authentication certificate must not be used.

5.5. XML-Signature standards (XML-DSIG)

XML-DSIG is an XML compliant syntax which can be used for the signing of message parts.

Ref	Requirement
5.5.1	Advanced electronic signatures must be created using the XML-DSIG standards defined in [2]

5.6. XML Canonicalisation

Ref	Requirement
5.6.1	The canonicalisation standard to be used is “Exclusive Canonical XML (without comments)” as defined in [2]
5.6.2	In addition to the canonicalisation, all whitespace outside of elements must be removed prior to hashing the canonical form.

5.7. Secure hashing Algorithm for use in EPS Release 2

In release 2 the agreed hashing standard to be used will be SHA-1. However in Release 3 of EPS, on the advice of CESG, prescribing systems will migrate to SHA-256

Ref	Requirement
5.7.1	In Release 2, prescribing systems shall only use the SHA-1 standard for creating hashes.

5.8. Signature Algorithm for use in EPS Release 2

Ref	Requirement
5.8.1	The SignatureMethod of *RSA-SHA1 shall be used*. This equates to the use of the RSASSA-PKCS1-v1_5 algorithm as defined in PKCS#1

5.9. Timestamp on signing

Ref	Requirement
5.9.1	The timestamp within the Author element of the parent prescription must be set immediately prior to applying the advanced electronic signature.

6. Requirements for Dispensing Systems

Within the scope of this document, validation of signatures is required within a dispensing system: a compliant system must validate the signature for each script downloaded before it is presented to the pharmacist for dispensing. In addition, a compliant system must present information about the signature to the dispenser to allow them to confirm who signed the prescription and when.

6.1. Messages sent by the SPINE

The following messages received from the SPINE have an advanced electronic signature in them that is derived from a message sent to the SPINE. The table references a message in the previous table that provides the information necessary to extract the signature and validate it.

Message Type	Message Name	Related message	Notes
122002	Prescription Release Response	132004	exclude pertinentLineItem.itemStatus

6.2. When to Check for an Advanced Electronic Signature

An advanced electronic signature should be present in every release 2 electronic prescription. As such, the dispensing system must validate the electronic signature in every release 2 prescription. Electronic signatures will not be present in release 1 prescriptions.

Ref	Requirement
6.2.1	Dispensing systems shall verify the advanced electronic signature on all release 2 electronic prescriptions.
6.2.2	Dispensing systems shall not check for the presence nor attempt to validate an advanced electronic signature on release 1 electronic prescriptions.

6.3. Secure Hashing Algorithms

Dispensing systems for the EPS Release 2 need to be able to support the verifying of signatures based on both SHA-1 and SHA-256 algorithms. Before release 3 of the electronic prescription service, the necessary infrastructure upgrades will have been put in place to accommodate SHA-256 hashing. It will be a release 3 requirement that prescribers use SHA-256 hashing within the application of advanced electronic signatures once the prescribers smartcard has been updated. If the prescribers smartcard has not been updated then a SHA-1 hash will still be applied.

In assembling the signature in the XML, the relevant uri's (dependent on the algorithm used) will be embedded into the relevant place in the signature block so that a dispensing system can identify the algorithms used within the signing process and hence apply the correct algorithms during verification.

In order to allow a seamless transition from SHA-1 to SHA-256 it is a requirement that dispensing systems have the capability of validating signatures created with SHA-256 now so that SHA-256 can be introduced without having to upgrade all dispensing systems across England at that time.

Ref	Requirement
6.3.1	Dispensing systems must be capable of validating electronic signatures which were created using SHA-1 or SHA-256.
6.3.2	Dispensing systems shall identify which hashing algorithm was used during creation of the signature by inspecting the algorithm attribute within the DigestMethod of the signature block in the prescription release response.
6.3.3	Dispensing systems shall apply the same algorithm during the validation of the signature as was during the creation of the signature.

6.4. Signature Algorithms

Ref	Requirement
6.4.1	Dispensing systems must be capable of validating electronic signatures which were created using either *RSA-SHA1 or RSA-SHA256 signature methods*.
6.4.2	Dispensing systems shall identify which signing algorithm was used during creation of the signature by inspecting the algorithm attribute within the SignatureMethod of the signature block in the prescription release response.

6.5. System Signature Validation Requirements

Compliant dispensing systems must use the digital certificate received to validate the signature as follows:

- the relevant contents of the message have not been changed since the signature was applied,
- the message was signed by the owner of the received certificate,
- the received digital certificate was issued by the CfH certificate authority set up to issue signing certificates,
    - Uses cached certificate of the Content Commitment Sub-CA
- the signature was applied during the validity period for the received certificate.

Referring to the signature validation steps defined in the Information Governance advanced electronic signature specification, Ref. [2], EPS, compliant dispensing systems must validate the signature as follows:

Ref	Requirement
6.5.1	**Hash comparison –** dispensing systems must confirm that the message contents match the hash value received.
6.5.2	**Signature comparison –** dispensing systems must confirm that the hash value calculated from the signature block matches that which was signed
6.5.3	**Certificate validation** – dispensing systems must confirm the identity of the person who created the signature, by implementing the following checks: • **Certificate chain/signature** – confirm that the received digital certificate was issued by the NPfIT certificate authority set up to issue signing certificates, • **Validity date –** confirm that the electronic signature was applied during the validity period for the received certificate.

If any one of the above checks fail then the signature is invalid. If the signature is invalid then the message must be returned to the SPINE and the medication must not be dispensed.

Message	*Dispense Proposal Return*
Message Code	0005
Description (Text)	Invalid digital signature

Ref	Requirement
6.5.4	The dispensing system must prevent the user from dispensing a prescription with an invalid digital signature.
6.5.5	On identifying an invalid advanced electronic signature the prescription must be returned to the spine via a dispense proposal return with the reason “invalid digital signature”
6.5.6	Dispensing systems must provide some form of indication to the system user that a prescription has been returned, to allow patients to be kept informed, and to allow a pharmacist to make proactive enquiries as to the cause of the failure.

6.6. Signature Display Requirements

When a prescription is presented for dispensing, a compliant system must display details relating to the signature received for the dispenser to review, and provide an optional button to invoke a certificate revocation check:

“signed by” – subject/common name attribute value from the *X509Certificate* element in the *SignatureText* block

“signature date/time” – *Author.time*

Ref	Requirement
6.6.1	The dispensing system must display to the user the “signed by” and “signature date/time” details retrieved from the certificate within the prescription message.
6.6.2	A compliant system must allow the dispenser to cancel a dispensing operation if not satisfied with any of the displayed information.