



Standard Operating Procedure for e_Signature

SOP ID Number: JRO/SPON/S32/01	Effective Date: 18/03/19
Version Number & Date of Authorisation: V01, 21/02/19	Review Date: 18/03/22
eDocument kept: S:\SLMS_RSC_ALL_STAFF\CLINICAL_TRIALS\SOPs\EFFECTIVE_SOPs_Guides\Sponsor SOPs\SPON_S32_SOP for e_Signature\SPON_S32_SOP for e_Signature.doc	

Revision Chronology:			
SOP ID Number:	Effective Date:	Reason for Change:	Author:
JRO/SPON/S32/01	18/03/19	New SOP	Helen Cadiou, Keith Boland

ACRONYMS:	
JRO	Joint Research
GCP	Good Clinical Practice
SOP	Standard Operating Procedure
MHRA	Medicines and Healthcare Products Regulatory Agency
REC	Research Ethics Committee
QA	Quality Assurance

Standard Operating Procedure for e_Signature

1. PURPOSE

This Standard Operating Procedure (SOP) has been written to describe the procedure for the use of e_Signature.

2. JOINT UCLH/UCL BIOMEDICAL RESEARCH OFFICE POLICY

All SOPs produced from the JRO must be used in conjunction with local NHS Trust and UCL policies and procedures.

The JRO acts as the representative of the Sponsor and will be the official name used on all SOPs.

3. BACKGROUND

All SOPs are written in accordance with applicable GCP requirements as outlined in Directives 2001/20/EC and 2005/28/EC (in the UK, these Directives were transposed into UK law by SI 2004/1031, SI 2006/1928) and subsequent amendments and when applicable Regulation 536/2014 and subsequent relevant SIs. Where applicable it incorporates elements of ICH GCP tripartite guidelines (E6)".

All documents generated for the set up/management of clinical trials are e_documents, some of these documents will need a signature. The existing process of printing out a document, signing it as a 'wet ink', scanning it and up loading it, is antiquated/long winded/cumbersome and slows down the whole process, as it involves having access to the use of a printer. The PDF e_Signature process described in section 6 is simple and involves a security step by way of password protecting each signature.

3.1 Back in 2013, the EMA had decided to adopt a similar approach:

Regulatory information - European Medicines Agency introduces digital signatures for selected procedures, <https://www.ema.europa.eu/en/news/regulatory-information-european-medicines-agency-introduces-digital-signatures-selected-procedures>:

News 01/08/2013

From September 2013, the European Medicines Agency (EMA) will start to use digital signatures systematically in outgoing documents that currently require a legally binding signature. This will start with documents related to scientific advice for human medicines, to orphan medicines and to paediatric-medicine procedures.

The Agency will also provide certified PDF electronic application forms to allow companies to sign these forms digitally using a PDF reader application, if they wish to do so.

The steps to verify the digital signature of documents issued by the Agency and to send a digitally signed document to the Agency are described in EMA eSignature capabilities: frequently asked questions relating to practical and technical aspects of the implementation, which is available on the Agency's eSubmission website under eSignatures.

This initiative is part of the Agency's strategy to increase electronic-document-only exchanges between the Agency and the pharmaceutical industry.

The Agency expects the exchange of digitally signed electronic documents to increase the efficiency of procedures and eliminate the need to archive paper documents. It may

also bring about cost savings for companies, by removing the need to print documentation and reducing courier charges.

3.2 Extract from the Joint Statement on Seeking Consent by Electronic Methods v1.2 September 2018

file:///C:/Users/sejjhc0/Desktop/hra-mhra-econsent-statement-sept-18%20(2).pdf

Electronic signatures

What is an electronic signature?

The 'eIDAS' Regulation (EU) No 910/2014 establishes an EU-wide legal framework for electronic signatures. The Regulation, which is supplemented by the UK eIDAS Regulations (SI 2016/696), defines an electronic signature as 'data in electronic form which is attached to or logically associated with other electronic data and which is used by the signatory to sign'.

Electronic signatures can include signatures that are:

1. Tickbox plus declarations
2. Typewritten
3. Scanned
4. An electronic representation of a handwritten signature
5. A unique representation of characters
6. A digital representation of characteristics, for example, fingerprint or retina scan
7. A signature created by cryptographic means

Electronic signatures can be divided into three groups:

1. Simple electronic signatures – examples are a stylus or finger drawn signature, a typed name, a tick box and declaration, a unique representation of characters and a fingerprint scan.
2. Advanced electronic signatures – these are uniquely linked to the signatory, are capable of identifying the signatory, allow the signatory to retain control, and are linked to data within the signature that can detect any changes made.
3. Qualified electronic signatures – an advanced electronic signature, uniquely linked to the signatory, that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

The use of 'advanced' or 'qualified' electronic signatures provides:

1. Authentication – the signatory can be linked to the information
2. Integrity – changes to the information can be detected more easily
3. Non-repudiation – legal assurance regarding where the electronic signature has come from

Whilst any type of electronic signature is admissible as court evidence by virtue of the 'eIDAS' Regulation, some are more reliable and carry greater evidential weight and assurance than others. For example, 'qualified' electronic signatures are automatically granted the legal effect of a handwritten signature with mutual recognition in EU member states (Art. 24 (2)) but may place a disproportionate burden on both the researcher and the participant and will not always be appropriate.

4. SCOPE OF THIS SOP

This SOP relates to the use of e_Signature for documents pertaining to trials sponsored by UCL and managed by JRO.

5. RESPONSIBLE PERSONNEL

Any staff involved in the management of UCL sponsored CTIMPs managed by JRO.

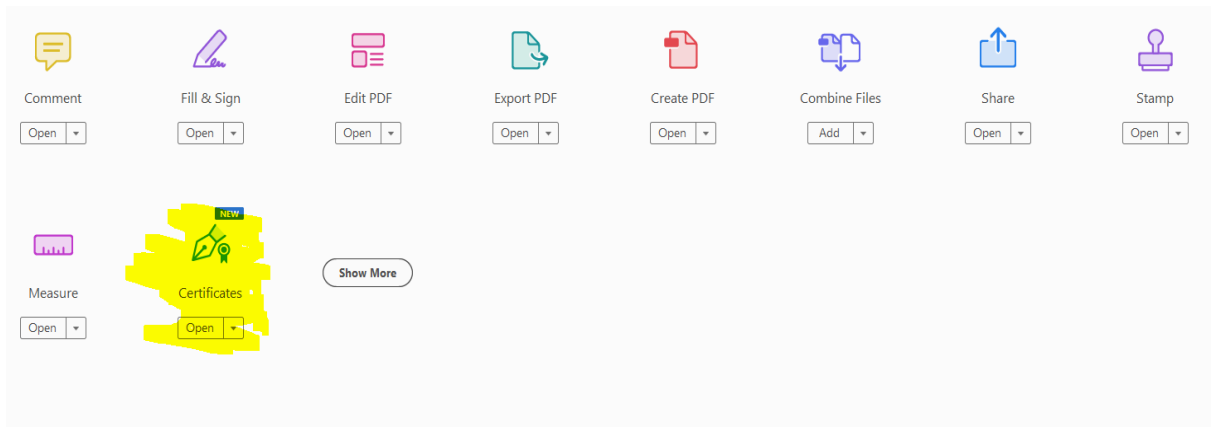
6. PROCEDURE

	Please see the screenshots below as they illustrate the following text:
	Applying the signature in a word document:
1	Open a word document needing signature
2	Save as
3	pdf
4	Open the created pdf document
5	click on "tools" on the top left, then "certificates"
6	Click on "Digitally sign"
7	Drag across the document where you want the signature
8	The "sign as" screen will show. Confirm this is correct and click "sign"
9	Then save the document to the desired location

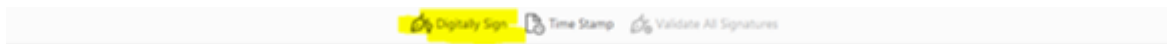
- Open document and locate area for signature.

Signature

- Click Tools
- Open Certificates

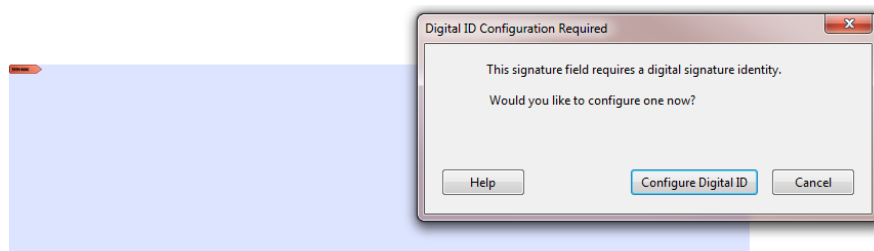


- Click Digitally sign



Signature

- Drag across document where you want signature to be and click configure digital ID



Signature

- Choose Create Digital ID option

Configure a Digital ID for signing

A Digital ID is required to create a digital signature. The most secure Digital ID are issued by trusted Certificate authorities and are based on secure devices like smart card or token. Some are based on files.

You can also create a new Digital ID, but they provide a low level of identity assurance.

Select the type of Digital ID:

- Use a Signature Creation Device**
Configure a smart card or token connected to your computer
- Use a Digital ID from a file**
Import an existing Digital ID that you have obtained as a file
- Create a new Digital ID**
Create your self-signed Digital ID

Cancel Continue

- Save digital ID to windows certificate store

Select the destination of the new Digital ID

Digital IDs are typically issued by trusted providers that assure the validity of the identity. Self-signed Digital ID may not provide the same level of assurance and may not be accepted in some use cases.

Consult with your recipients if this is an acceptable form of authentication.

- Save to File**
Save the Digital ID to a file in your computer
- Save to Windows Certificate Store**
Save the Digital ID to Windows Certificate Store to be shared with other applications

Back Continue

- Input details of UCL account

Create a self-signed Digital ID ✕

Enter the identity information to be used for creating the self-signed Digital ID.

Digital IDs that are self-signed by individuals do not provide the assurance that the identity information is valid. For this reason they may not be accepted in some use cases.

Name	Keith Boland
Organizational Unit	UCL
Organization Name	UCL
Email Address	k.boland@ucl.ac.uk
Country/Region	GB - UNITED KINGDOM
Key Algorithm	2048-bit RSA
Use Digital ID for	Digital Signatures

? Back Save

- Sign document electronically

Sign as "Keith Boland" ✕

Appearance Standard Text ▼ Create

Keith Boland Digitally signed by Keith Boland
Date: 2019.01.23 17:07:00 Z

Lock document after signing [View Certificate Details](#)

Review document content that may affect signing Review

Back Sign

7. REFERENCES NA

8. APPENDICES NA

9. TEMPLATES/LOGS ASSOCIATED TO THIS SOP NA

10. SOP DISSEMINATION AND TRAINING

SOPs will be distributed to the concerned staff.

11. SIGNATURE PAGE

Author and Job Title:	Keith Boland, Sponsor Regulatory Advisor
Signature:	
Date:	
Authorised by: Name and Job Title	Helen, Cadiou, Head of QA
Signature:	
Date:	

12. SOP TRAINING LOG

	Name of Staff (Capital letters)	Job Title: Department:	Training Date	I confirm that I understand & agree to work to this SOP SIGNATURE	Name of Trainer (if training required)	Signature	Date
1							
2							
3							
4							
5							
6							
7							

	Name of Staff (Capital letters)	Job Title: Department:	Training Date	I confirm that I understand & agree to work to this SOP SIGNATURE	Name of Trainer (if training required)	Signature	Date
8							
9							
10							
11							
12							
13							
14							

	Name of Staff (Capital letters)	Job Title: Department:	Training Date	I confirm that I understand & agree to work to this SOP SIGNATURE	Name of Trainer (if training required)	Signature	Date
15							
16							
17							
18							
19							
20							