Electronic Signature

SOP Reference: RGIT_SOP_043	
Version Number: 4.0	
Effective Date: 02 Dec 2024	Review by: 02 Dec 2027
Author: Agnese Zicari, Quality Assurance Facilitator	
Approved by: Keith Boland, Senior Clinical Trial Manager	Date: Keith Boland Digitally signed by Keith Boland Date: 2024.12.02 11:55:48 Z

Version	Date	Reason for Change
Version 1.0	21 April 2020	1st Edition
Version 2.0	19 Oct 2020	Scheduled Review Administrative changes to SOP. JRCO name change to RGIT.
Version 3.0	22 Jul 2022	Further clarification made to the process of electronic signatures
Version 4.0	02 Dec 2024	3yr SOP review

TABLE OF CONTENTS

1. PURPOSE

The purpose of this Standard Operating Procedure (SOP) is to describe the procedure of using electronic signatures (e-signature) in documents.

2. INTRODUCTION

There are several documents which are created for the set-up and management of research studies that will require a signature. The process of gaining a signature certifies that the document adds value and can be used to approve, review and validate certain events or actions that may occur throughout the duration of the research. The existing process of signing documents as 'wet ink' will be a process that will still be utilised, but for a certain number of documents. The following documents listed below can be considered as mandatory wet ink signed documents, but may also be considered on a case-by-case basis:

- Protocols and Amendments
- Consent forms
- Completed Case report forms
- CRF correction signature sheet/ signature logs

Electronic signatures can be accepted for agreements and contracts, but there may be some cases where a wet ink signature may also be required if the sponsor deems it necessary. However, if in doubt, double check with the college/trust contracts team on a case-by-case basis. As referenced in section 2.1 MHRA of this SOP any: *the use of an inserted image in place of a signature to indicate that a document has been signed electronically will not be an adequate form of the signature process, therefore inserted images should not be used for MHRA study/documents.* However, based on the risk level of studies/documentations outside MHRA (e.g. non-CTIMP studies) standard e-signatures, including insertion of an image, may still be adequate for use provided it can be verified and an adequate process is in place to ensure that changes to the documents will invalidate the signature.

The process of e-signatures can be completed using either a validated system (e.g. DocuSign) or verified e-signatures (e.g. Acrobat or Adobe reader) which are described in section 3. These capture the date, time and signee of the document and produce an audit trail of signatures.

2.1. The Medicines & Healthcare products Regulatory Agency (MHRA)

Since March 2018, also the MHRA have produced guidelines to assist in the use of electronic signatures. The MHRA guidelines stress the control that is necessary when using e-signatures within a regulated work context. It is indeed necessary to ensure that:

- the e-signature is exclusively attributable to one individual.
- 'the act of signing is recorded within the system' so that any alteration/manipulation invalidates the e-signature as well as the entry status.

- there is a verification method in place to assess that the e-signature is exclusively associated with the entry made and the entry owner.

That is, the appropriate validation of the signature will need to be demonstrated to ensure that actual control over the status of the signed records can be maintained, which means that the metadata associated with the electronic signature must be stored within the associated document to establish its formal validity. Indeed, in the MHRA guideline on e-signatures metadata have been defined as '*data that describe the attributes of other data and provide context and meaning…' as they 'describe the structure, data elements, interrelationships, and other characteristics of data…' and 'also permit data to be attributable to an individual'.* Examples of metadata needed to validate an e-signature may include: the users' name, date, and location as well as signature time.

With respect to the use of e-signatures to attain a valid e-consent, this is better detailed in the dedicated guideline by the HRA & MRA (2018).

Meanwhile, within the management context of clinical (as well as non-clinical) research, the use of advanced/qualified e-signatures is generally applied. That is, any staff involved in the management of RGIT sponsored CTIMPs and non-CTIMPS studies (alongside any staff working within the RGIT unit) should follow the below procedure.

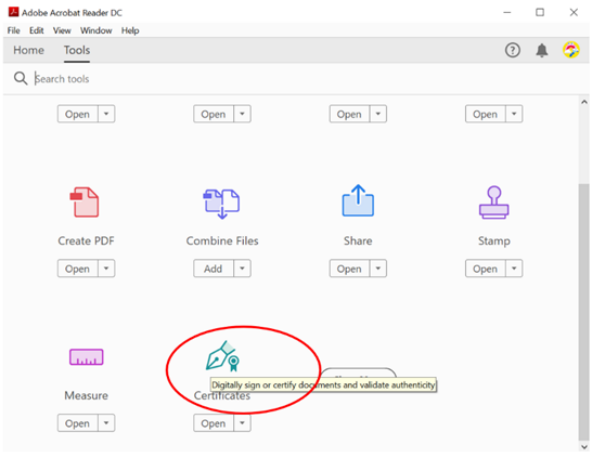
3. PROCEDURE

As explained in the previous sections, within the standard clinical research practice, the process for applying advanced/qualified e-signatures can be implemented through a broad range of validated systems that conform to the definitions reported in this SOP, such as DocuSign, Verified e-Signature, and Adobe Acrobat Digital Signature. The latter relies on the Adobe Acrobat PDF e-signature application that captures the date, time and signer's ID for a certain document. Also, for every user associated document, these applications store an activity history, and a detailed audit report may also be issued as a result. The use of the Adobe Acrobat and DocuSign to apply and validate e-signatures is described in this SOP, and more details on this are provided in the following sections.

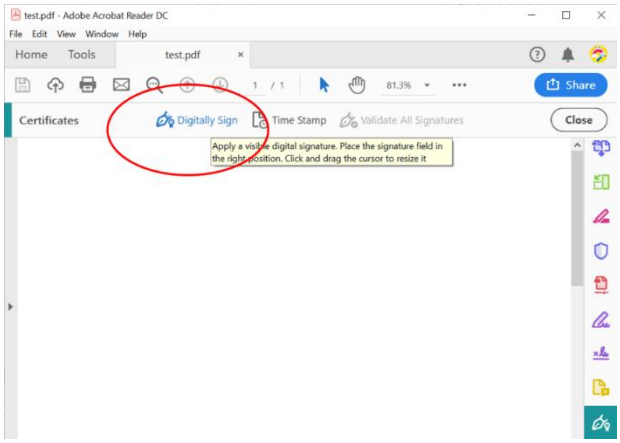
3.1. Applying e-signatures in Adobe Acrobat

In the following paragraphs there are a number of print-screen pictures to guide the user through the different steps that are required to digitally sign documents in the Adobe Acrobat application and/or create a digital identity within the same application. Also, at the end of this SOP (section 6) additional information is provided, on how to process Word or scanned documents before e-signing them in the above application. Please read carefully through the instructions and print-screen pictures.

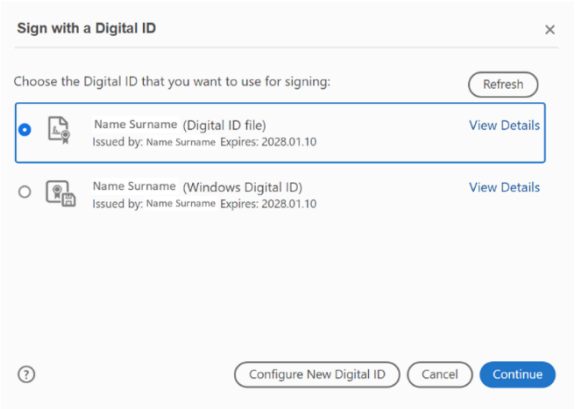
The ‘certificates’ icon should be selected:



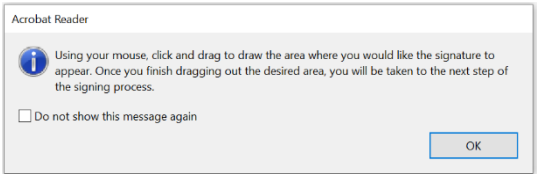
The ‘digitally sign’ icon can be then selected:



Once the correct signature option has been selected, click on the ‘continue’ icon. A preview of the signature will appear, for the user to choose the ‘signature’ option.

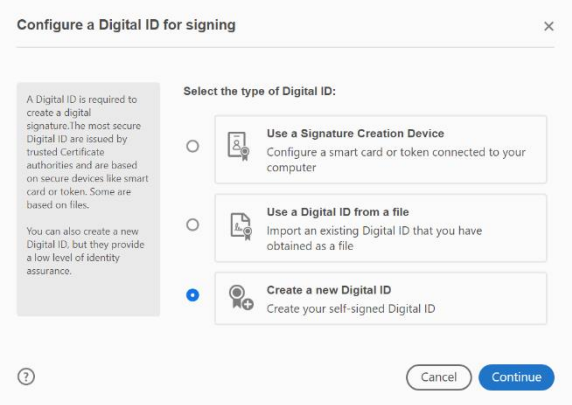


The application will then ask the user where the e-signature should be applied:

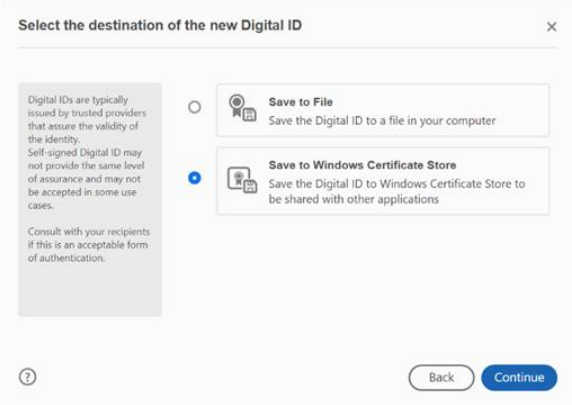


3.2. Configuring a new digital ID and applying an e-signature in Adobe Reader Acrobat

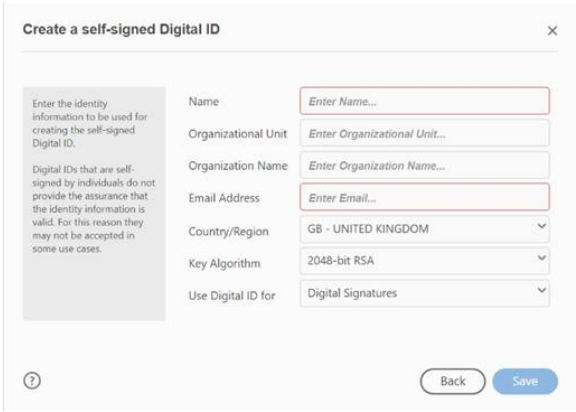
The ‘configure digital ID’ option should be selected first and the ‘create a new digital ID’ selected thereafter:



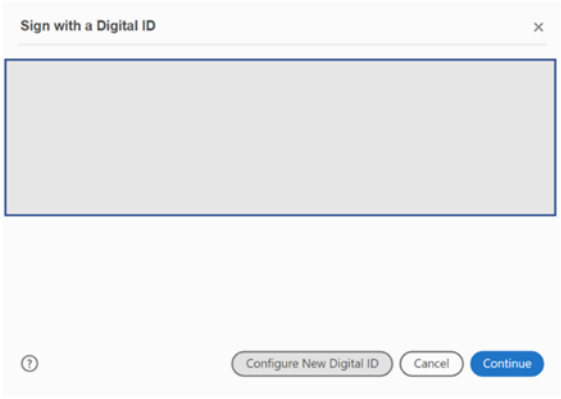
The ‘save to Windows certificate store’ option needs to be selected:



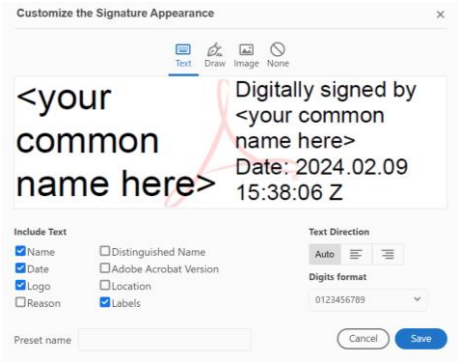
Personal information and correct Country/Region details can be this way entered, and saved:



Now that the digital ID has been created for the associated user, an ID for signature can be selected as detailed in section 3.1.



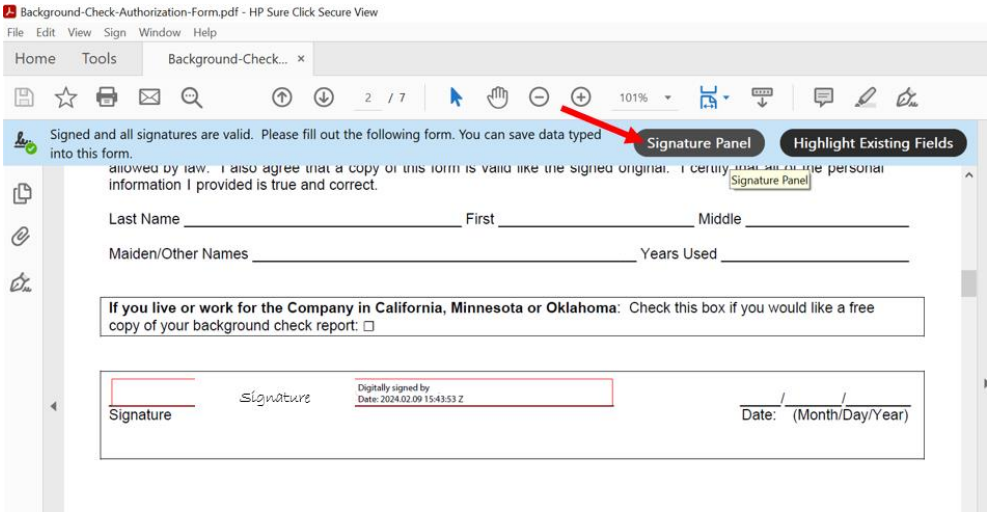
An image of the signature may also be displayed together with the digital signature by drawing and/or saving the signature image as pdf file and selecting the create option on signature.



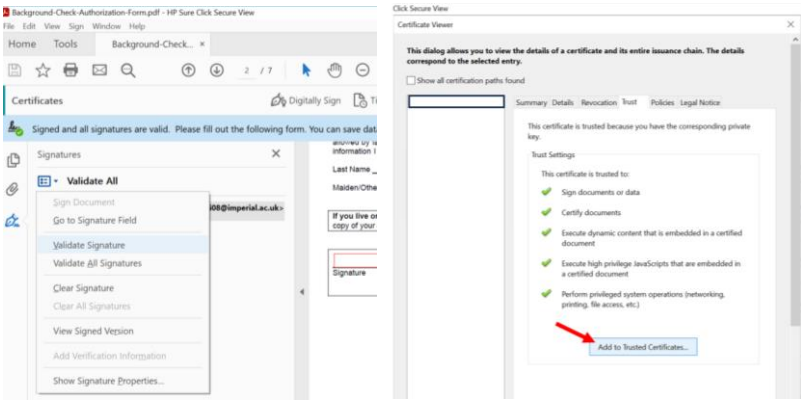
At this point the signed document can be saved in the desired location with all necessary metadata displayed and associated.

3.3. Verifying e-signatures in Adobe Reader

It is recommended that all signatures on a PDF document be verified as follows. First, the signature panel should be selected.



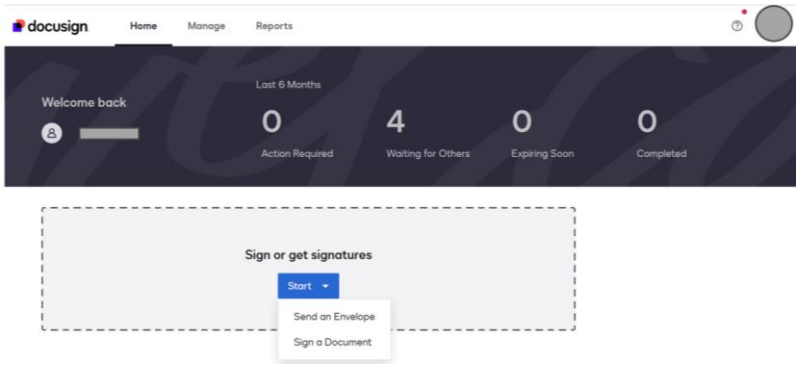
Once the signature(s) show(s) in the panel list beside the document, the signature validation option may be chosen from the dropdown list, by right clicking on each individual signature (see the left picture below). In the signature properties window, the icon 'show signer's certificate' can be this way selected, and the 'add to trusted certificates' option should be chosen (in the dynamic mode) in the related 'trust' tab (see the right picture below).



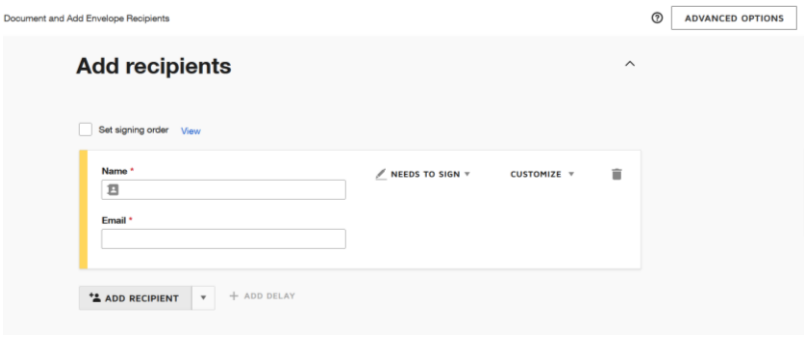
3.4. Sending an envelope in DocuSign

In this section as well as the following section, simple instructions on how to apply e-signatures on documents in DocuSign have been listed.

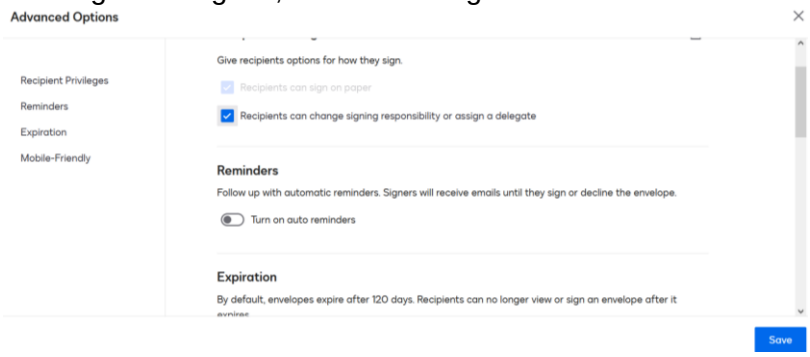
In the DocuSign home tab window, the send envelope option should be selected and the file to be signed uploaded.



After that the file has been uploaded the recipients (i.e. the signatories) can be added to the envelope.



The advanced option section on the top right corner of the above window should be selected and opened to untick the option ‘recipients can change signing responsibility or assign a delegate’, and this change should be saved.

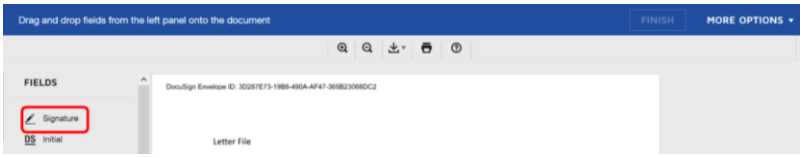


A message can be added too in the envelope before sending the envelope for signature. At this point the envelope can be sent out for signature either immediately or on a specific date/time (by choosing the option send it later).

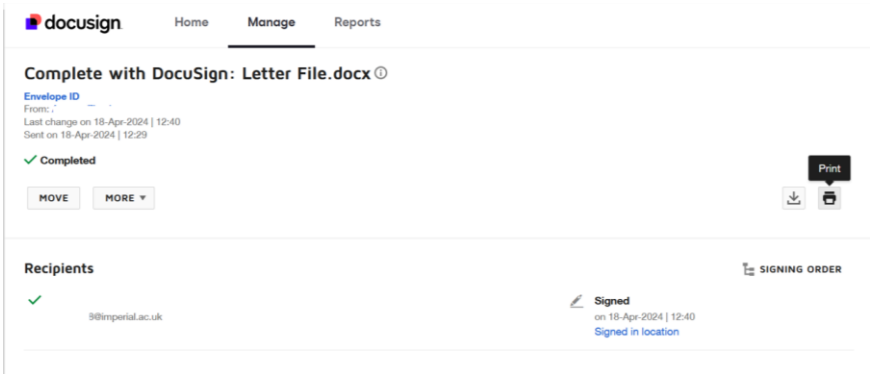
3.5. Applying e-signatures in DocuSign

DocuSign will send an email to all signatories selected when drafting the envelope, and they will need to click on the review document icon in the email to apply the signature.

In order to apply the signature, the signature icon in the left panel needs to be dragged and dropped into the document signature placeholder.



Once the document is complete, this can be downloaded together with the audit certificate. Also, the audit report can be printed out and attached to the document, in hardcopy.



4. REFERENCES

Regulation (EU) N.910 of the EU parliament and council (2014).

EMA technical guidance on e-submissions (cited on 30 Mar 2023).

UK Statutory Instrument N.89 (2019) Electronic execution of documents - Low Com No. 386, (UK Law Commission, 2019) (cited on 30 Mar 2023).

MHRA 'GXP' Data Integrity Guidance and Definitions – Rev.1
(cited on 30 Mar 2023).

Joint Statement on Seeking Consent by Electronic Methods v1.2 September 2018
(cited on 31 Mar 2023).

MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015 (cited on 31 Mar 2023).

5. APPENDICES

6.1 Applying an e-signature to a PDF from a Word document

1. *Open the desired word document, click 'file' and then 'save as' icons.*
2. *Change the file format from Word to 'PDF' document.*
3. *Ensure that the document name is correct and click the 'save' icon.*
4. *Navigate to the location of the saved PDF and open the document.*

5. *Click the 'tools' tab on the top left tab and then click the 'certificates' icon.*
6. *Click the 'digitally sign' option and highlight an area to place the e-signature.*
7. *After completing the section 4.1 steps a digital ID signature can be chosen/applied.*
8. *All visible metadata (name and date/time stamp) should be assessed for correctness.*
9. *The e-signature should be applied and saved.*
10. *Renaming the signed document may be required to ensure the metadata within the document have been saved.*

6.2 Applying an e-signature to a PDF from a scanned document

1. *Locate the scanned document that has been saved as a PDF formatted document.*
2. *Otherwise, right click the document and click 'open with', navigate to the Adobe application icon and proceed to open the document.*
3. *Save a copy of the document as a PDF.*
4. *Once the document has been saved correctly, it can be signed as per the instructions in section 4.1.*