PKI and Digital Signature Introduction and FAQs[[1]](#endnote-1)

A Beginner’s Guide, including Frequently Asked Questions (FAQs), to Public Key Infrastructure (PKI) for Digitally Signing Documents for Publication in the Federal Register

# Introduction to PKI

## *What is PKI?*

PKI stands for Public Key Infrastructure. “A PKI establishes and maintains a trustworthy networking environment by providing key and certificate management services that enable encryption and digital signature capabilities across applications — all in a manner that is transparent and easy to use.” (Entrust website: <http://www.entrust.com/products/entrust-authority-pki/>)

## *What does PKI do as it relates to publication in the Federal Register?*

PKI allows the user to sign a Word file digitally, with no pen and ink! The system is set up in a way that the signed file can be handled (attached, etc.) without invalidating the signature. This allows for electronic submission of digitally signed documents.

# Benefits of PKI

## *Why should I use PKI?*

* PKI can reduce the time between signature and publication depending on your agency’s business process. This time savings occurs for a few reasons:
  + No package for staff to bundle (making copies, burning a CD, filling out and printing forms)
  + No mail required. File can be sent immediate via the web portal at [www.fedreg.gov](http://www.fedreg.gov).
* PKI will save Agency resources by eliminating paper, toner, CD, and time spent putting a package together.

## *How much time does digital signature save?*

This process could save some offices between 2-5 days in preparation time; in other words, it would eliminate 2-5 days between when the document is signed and when it is published. The amount of time depends on the usual method of submission (regional mailing vs. HQ hand-delivery).

## *How much money will digital signature save?*

The cost savings of digital signature can vary based on the typical length of documents for an office and your agency’s publication business process. Variations include:

* Do your regional offices mail their documents to a headquarters? If so, how does the headquarters get it to the OFR?
* Cost of toner, ink, printer maintenance.
* Staff time spent putting package together (making copies, burning CD, printing and filling out appropriate forms)

## *How much money does digital signature cost?*

There are two routes to take: the “free” route and the paid route.

**The “Free” route**

If your agency has PIV cards with PKI certificates loaded on them, then all you need is software to apply that certificate and a card reader. For the software, you can use the PKCS7Sign software, which is available free to federal agencies from the General Services Administration. The software can be downloaded at: , <http://www.idmanagement.gov/documents/pkcs-7-document-signing-tool>. Card readers may already be incorporated in your computer, or you can purchase one for around $20.

**The Paid route**

Your agency can otherwise opt for certificates from the Government Printing Office(GPO), which cost $97 per signer/per year. Only those who are signing documents require these certificates. Details on GPO’s certificates can be found here: <http://www.gpo.gov/projects/pki.htm>. The number of certificates obtained is up to your agency/office: **only signers must have the certificates**. **The signed file can be handled (attached, etc.) without a certificate.** Some offices/regions have certified a primary and a secondary signer, while others have one signer and use a paper process when someone needs to sign as “acting” for the primary signer. The cost also ensures that the Entrust software comes with technical support: GPO technicians are available to assist with installation and first-time use, and Entrust is available to support the product during later use.

Other third parties do sell digital certificates. The key is that the certificate must be a medium assurance level digital signature certificate, cross-certified by the Federal Bridge Certification Authority in PKCS#7 standard. This is being included on many PIV ID cards being distributed government wide.

## *Does embarking on the PKI digital signature program mean my office always has to use it?*

PKI digital signature does not preclude offices from submitting documents with the normal paper and CDs.

# Preparing and editing the Word file to be signed

## *Why does the file need to be submitted as a .docx?*

OFR needs to edit the document, which is one of the reasons we do not accept .pdfs, or any other file than .docx. We cannot accept .docm, as these can contain harmful macros. This rule applies not only to the document being sent for publication, but also the special handling letter, if one is needed.

## *If OFR needs to edit the document, then why do I need to digitally sign it?*

When your document arrives, with your digital signature still intact, we are able to confirm that 1) Your name matches the name printed as the signer in the document and 2) that since your signature is intact, the contents of the document have not been tampered with.

## *Can I edit the document after I have signed it? Why or Why not?*

No. Once the document has been digitally signed, you cannot edit the document. This would invalidate the digital signature and require the document to be digitally signed again.

## *How can I make sure the signed document is the one I want to send?*

We recommend that if it is necessary for your business process to do this kind of verification, that you either do it before it is signed, or if absolutely necessary, you can make a copy of the signed file and then open and view the copy for verification purposes.

## *Who needs to obtain a digital signature certificate to submit electronically?*

Anyone who is authorized to sign documents at your agency and whose name will appear in the signature block.

## *What if the only person who is authorized to sign the document is not available?*

This is a business process question that is important for agencies to consider. Remember: **no one is authorized to use someone else’s credentials to sign a document digitally on someone else’s behalf.** This applies to both PIV card digital signing and “soft certificate” use such as GPO or Entrust certificates. So the signer MUST apply their digital signature themselves. Your agency may need to look at its delegations of authority to ensure that the individuals necessary can be available to sign documents when needed. **The person whose name is in the document MUST be the person whose digital signature is applied to the document.** If the names do not match, the document will be rejected by our office.

# Sending to signed file to the OFR

## *How do I know this will work?*

We recommend to that all agencies starting their PKI program send a digitally signed test document to us for test validation at [ofrtechgroup@gpo.gov](mailto:ofrtechgroup@gpo.gov). We will work with you to test if the digital signature validates, and if it does not, we will help you fix the issue.

## *Do I need a Disk certification letter?*

Since there is no disk and no paper copy, you do not need a certification letter for digital submission.

***Can I still make special handling requests digitally?***

Yes, you can still create special handling letters and attach them to individual documents in the web portal. Remember: **the special handling letter MUST be digitally signed**, but the signer of the document and the special handling letter do not need to be the same person. For instance, a Director may sign the document, but a liaison can sign the special handling letter.

## *How do I get the signed file to the OFR?*

First, you need an account with our portal at [www.fedreg.gov](http://www.fedreg.gov) . Once you have created an account, we will verify your information and approve or reject the account set up. If you are approved, you will receive a link via e-mail to create a unique password.

Once your account has been created, you will be able to submit via the web portal. You can upload up to 20 documents at a time, as well as special handling letters, if required.

## *Do I need a digital certificate to send the document in the web portal?*

No, you do not need a digital certificate to send the document. Digital certificates are only required to sign the document or the special handling letter.

1. Portions of this document were written by staff at the Environmental Protection Agency to address questions for the agency side of the PKI program. We want to thank them for their significant contribution to this document, and to our PKI presentation. [↑](#endnote-ref-1)