Digital

signATURES

Guidance for Form Owners

Contents

[Introduction 3](#_Toc19867793)

[Can I use Digital Signature? 3](#_Toc19867794)

[Benefits of Digital Signature 3](#_Toc19867795)

[Types of Digital Signature 4](#_Toc19867796)

[Appropriate Software to Use 5](#_Toc19867797)

[Digital Signature Scenarios 5](#_Toc19867798)

[Additional Guidance For Form Owners 6](#_Toc19867799)

[Conclusion 7](#_Toc19867800)

[APPENDIX A: Definitions 8](#_Toc19867801)

[APPENDIX B: Steps Signing Forms in MS Word That Contain Multiple Signature Fields 9](#_Toc19867802)

[APPENDIX C: Related Guidance 11](#_Toc19867803)

# Introduction

Digital signature is the umbrella term used to talk about secure signature or simple signature and the term also includes offline and online signatures. In its most basic format, a “picture” is intended to make both the signer and recipient of a signed document “feel” like the ritual they are undergoing is equivalent to that of the traditional paper process. Digital Signatures can also be encrypted and secured using Public Key Infrastructure (PKI), also known as myKEY.

This document is intended to provide Transport Canada employees with the necessary information to help ensure an efficient and secure transformation to Digital Signature throughout the department. This guide will:

* Identify some of the benefits of Digital Signature
* Determine whether moving to Digital Signature is a suitable option
* Determine what type of Digital Signature is most appropriate
* Determine how to proceed with implementation of Digital Signature

# Can I use Digital Signature?

In June 2019, Bill C-97 received royal assent and amended Transport Canada’s authorities and gave the department wider authority over the administration and enforcement of the Act and can now use electronic means. The new sections 6.3, 6.4 and 6.5 now provides Transport Canada with the legal footing to request and/or accept digital signature in lieu of paper-based signatures.

While most documents and forms can be signed digitally, it’s unfortunately not appropriate in all scenarios and you should be aware of when it is appropriate to do so or not. Generally, if your document is internal to the department or required by internal policy then digital signatures are acceptable. If a signature is required by legislation or regulation, you may need to seek additional guidance from Legal Services.

|  |  |
| --- | --- |
| Appropriate usage | Will require additional guidance |
| Mandatory Rules form | Signature required by law |
| Consultant timesheets | External individual is required to sign |
| Access Control form | Signature is required from a Minister’s delegate |
|  |  |

# Benefits of Digital Signature

In the past there have been some users who have had a preference for traditional written “wet ink” signatures, and some business preferences continue to reinforce a paper based bias. However, with the introduction of digital signature technology, the process of submitting documentation has changed significantly and many forms are now being signed safely and efficiently using digital signature.

The following are the main benefits of using digital signatures:

1. Speed: Businesses no longer have to wait for paper documents to be sent by courier. Documents are easily written, completed, and signed by all concerned parties in a little amount of time no matter how far the parties are geographically.
2. Costs: Using postal or courier services for paper documents is much more expensive compared to using digital signatures on electronic documents.
3. Security: The use of digital signatures and electronic documents reduces risks of documents being intercepted, read, destroyed, or altered while in transit.
4. Authenticity: An electronic document signed with a secure digital signature will provide more confidence to the recipient that the signature has not been forged.
5. Non-Repudiation: Signing an electronic document digitally identifies you as the signatory and that cannot be later denied.
6. Imposter prevention: No one else can forge your digital signature or submit an electronic document falsely claiming it was signed by you.
7. Time-Stamp: By time-stamping your digital signatures, you will clearly know when the document was signed.

# Types of Digital Signature

Digital Signatures are the evolution of the traditional wet ink signature and can be used in a variety of contexts. These signatures are produced electronically and most commonly try to look as much like a wet signature as possible. Many forms that previously existed only in paper format at Transport Canada are now being transferred to electronic format and this has increased the need to have better guidelines and standards for the use of digital signature.

The type of signature that is required is directly linked to the type of document you are signing and its associated risk level. As some types of signatures are more secure than others you’ll need to choose a signature that meets the security requirement of the document and/or process and instruct your users appropriately. You should ask yourself the following questions:

* How sure do I need to be that the right individual has signed the document?
* Will the individual provide me with the document in another, more secure way?

There are several different types and uses for digital signature. To start with, digital signatures can be online or offline:

* Offline signatures: Defined as signatures in documents such as Word or PDFs that are shared via emails or other mechanisms
* Online signatures: Used or developed in solutions and can take the form of checkboxes or buttons, in combination with the capture of appropriate metadata.

Digital Signatures can also be distinguished by the level of security provided by the signature. There are several different types and styles of digital signature:

* Secure signature: Signatures applied to a document using a personal certificate and is coupled to an identity that has been proven to a higher level of assurance.
  + Signature applied with your myKey
* Simple signature**:** A stylus captured, typed or image based signature that is applied to a document with little or no identity validation. This is the most basic type of signature and is appropriate for low risk transactions and in some cases, will need to be coupled with an offline identity verification.
  + Scan of your signature
  + Signature captured by stylus
  + Signature typed on a document

Early adopters of digital signatures will be primarily focused on offline signatures. Those are considered to be both less risky and easiest to implement. Early adopters will primarily use Digital Signature for Level of Assurance 1 & 2 documents and/or process, therefore simple signatures will be more common during this phase.

# Appropriate Software to Use

It will be necessary to determine the appropriate type of software you will be using to create and sign the form using a Digital Signature, The following solutions are currently permitted at TC and their corresponding user instructions are described in Appendix B:

|  |  |  |  |
| --- | --- | --- | --- |
| Software | Use to Create Digital Signature Forms | Use to Sign Digital Signature Forms | Notes |
| Adobe Reader | Yes | Yes |  |
| Microsoft Office | Yes | Yes |  |
| Foxit PhantomPDF | Yes | Yes |  |

# Digital Signature Scenarios

**Scenario 1**

Mary is a consultant and works for Jon, a team lead. At the end of the month, Mary emails him with a completed timesheet and asks for Jon’s signature prior to sending it to her consulting company.

* Can Jon sign digitally?
  + Yes. This is a document that is not required by law, but rather by internal policy.
* Which signature type should Jon use?
  + Since Jon will email it back to Mary, Mary will have a good certainty that it is indeed Jon that signed her timesheet. Therefore, Jon can simply apply a scan of his signature on the timesheet.

**Scenario 2**

Arya is a Marine Safety Inspector and will sign a detention order against a vessel as per the Canada Shipping Act.

* Can Arya sign digitally?
  + It’s unclear as the signature of the detention order is required by legislation. Arya and her directorate should seek further guidance from Legal Services before proceeding.

# Additional Guidance For Form Owners

It is very important that this transformation be coordinated in a secure and stable way and a certain amount of employee awareness and training will be required. If you are the functional owner of a document, a form or a process, it may be beneficial to rethink its design from start to finish:

1. Do you really need a signature?
   * Signatures should be challenged in many situations.
     + Sometimes a form unnecessarily requires multiple signatures and this causes extra time and effort from various stakeholders.
   * Do other actions the individual takes fulfill the requirement of acceptance for its content?
     + For example, if you email a document you have completed an action that objectively speaking, replaces a signature.
   * Could a fully data/digital drive approach be used to store digitally signed documents?
     + Is it possible to use the process to represent digital signature rather than working from a document based approach to collecting data
2. Determine whether the Digital Signature is a good candidate for the Early Adopter Phase:
   * The Early Adopter phase will focus on the following types of forms:
     + Offline Digital Signatures that are shared by email and not contained on a page of a web application.
     + Forms intended solely for internal use that will not be shared outside of Transport Canada
     + Forms that require a Level of Assurance of 1 or 2
   * Some examples of forms that meet the aforementioned criteria would include NSRs, Timesheets and Letters of Offer.
3. Determine the type of software you will be using to create and sign the form using a Digital Signature and be familiar with the associated User Guides. The following solutions are currently permitted at TC and their corresponding user instructions are described in Appendix B:
   * Adobe Reader: Used employees who may be signing forms created by others.
   * Microsoft Office: Used employees who may be signing forms created by others.
   * Foxit PhantomPDF: Used by about 500 employees who may be creating or editing forms.
4. Determine the LOA Requirements of the form:
   * Everything can be signed, but we need to decide what LOA and hence what type of signature to use.
5. Determine the right type of digital signature to use:
   * Understand risks of choosing wrong type of digital signature
6. Determine where digital signature should be housed once signed:
7. In cases when multiple signatures are required it is necessary for signers to be familiar with the proper signing process using RDIMS:
   * See Appendix B for steps
8. In cases where there are date fields alongside signature fields it is necessary for signers to be familiar with the proper signing process:
   * See Appendix C for steps
9. Audit your Implementation of Digital Signatures
   * Ensure that Digital Signatures implemented remain at least as secure and efficient as “Wet Signatures” and report any issues.
10. Report Success and Lessons Learned
    * Examples of Recent Successes at TC include:
      + Pilots are now happening at Civil Aviation for pilots and HR is beginning to use Digital Signature for Letters of Offer and Performance Measurement

# Conclusion

Digital Signatures are a great way to save time and gain efficiencies in your process as well as reducing the use of paper and printers. Not all processes and documents lend themselves well to digital signatures, but if they do, the standard Transport Canada tools technology offers different types of digital signatures that allows you to do so quickly and easily. We recommend reviewing the related guidance in Appendix B and following our GC Wiki page ([TC Digital Signature Pilots](https://wiki.gccollab.ca/Transport_Canada_Digital_Signature_Pilots_-_Pilotes_de_signatures_num%C3%A9rique_%C3%A0_Transports_Canada)) to get started with digital signatures today!

# APPENDIX A: Definitions

To facilitate the understanding of this document, some definitions are provided below:

**Offline Signature**: Defined as signatures in documents such as Word or PDFs that are shared via emails or other mechanisms

**Online Signature**: Used or developed in solutions and can take the form of checkboxes or buttons, in combination with the capture of appropriate metadata.

**Secure Signature:** Signatures applied to a document using a personal certificate and is coupled to an identity that has been proven to a higher level of assurance.

* Signature applied with your myKey

**Simple Signature**: A stylus captured, typed or image based signature that is applied to a document with little or no identity validation. This is the most basic type of signature and is appropriate for low risk transactions and in some cases, will need to be coupled with an offline identity verification.

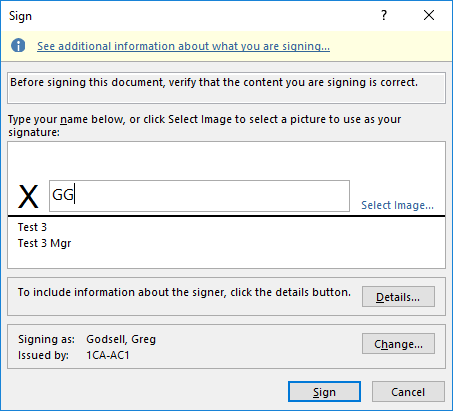
* Scan of your signature
* Signature captured by stylus
* Signature typed on a document

**Public Key Infrastructure (PKI)**: A set of requirements that allow (among other things) the creation of secure digital signatures. Through PKI, each digital signature transaction includes a pair of keys: a private key and a public key. The private key is not shared and is used only by the signer to electronically sign documents and the public key is openly available and used by those who need to validate the signer’s electronic signature.

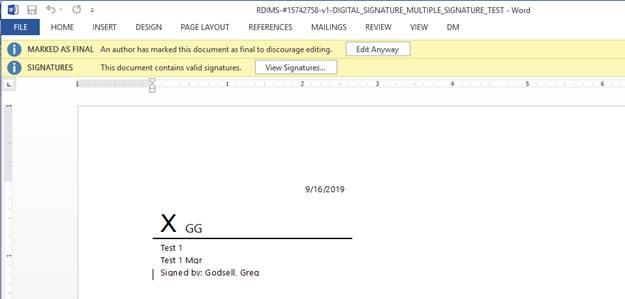
**Certificate Authority (CA)**: Digital signatures rely on public and private keys. Those keys have to be protected in order to ensure safety and to avoid forgery or malicious use. Third-party organizations that have been widely accepted as reliable for ensuring key security and that can provide the necessary digital certificates. Both the entity sending the document and the recipient signing it must agree to use a given CA.

# APPENDIX B: Steps Signing Forms in MS Word That Contain Multiple Signature Fields

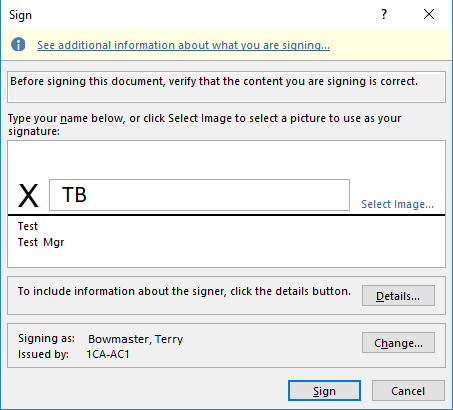
1. Open RDIMS Document that you wish to sign
2. Signer 1 adds a Signature to the Document:
   1. Right Click on Signature Field and Select “Sign…”
   2. Type Your Signature or Choose “Select Image…” to add image of your signature and then click Sign



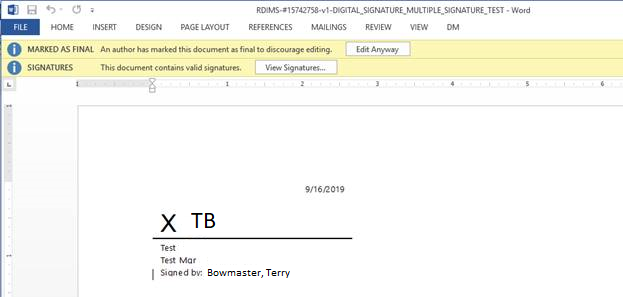
1. Check that Signature was Added Successfully



1. Right click on the document in RDIMS and click on Save e-Signature
2. Close document
3. Signer 2 adds a Signature to the Document:
   1. Right Click on Signature Field and Select “Sign…”
   2. Type Your Signature or Choose “Select Image…” to add image of your signature and then click Sign



1. Check that Signature was Added Successfully



1. Right click on the document in RDIMS and click on Save e-Signature
2. Close document

# APPENDIX C: Related Guidance

* [RDIMS-#15397429-SI - EA - DIGITAL SIGNATURES - TECHNICAL USER GUIDE (ENGLISH)](pcdocs://RDIMS/15717046/3)
* [RDIMS-#15398723- SI-EA - DIGITAL SIGNATURES - FREQUENTLY ASKED QUESTIONS (ENGLISH)](pcdocs://RDIMS/15398723/R)