**Understanding e-signature terminology within the GC**

# Introduction

Jurisdictions throughout the world have adopted laws and regulations that recognize the validity of electronic documents and electronic signatures. Some jurisdictions are very technology specific, others are much more general and technology neutral. In addition, the terms and definitions surrounding electronic signatures tend to differ from one jurisdiction to another and this can lead to some degree of confusion. A more thorough examination of the terms and definitions used in other jurisdictions is provided in Annex A of the [*Government of Canada Guidance on using Electronic Signatures*](https://www.canada.ca/en/government/system/digital-government/online-security-privacy/government-canada-guidance-using-electronic-signatures.html).

At the Canadian federal government level, the terms *electronic signature*, *digital signature* and *secure electronic signature* are all present in Government of Canada (GC) legislation. The purpose of this post is to help clarify these terms so that they can be used consistently throughout the GC. This post is primarily based on the [*Government of Canada Guidance on using Electronic Signatures*](https://www.canada.ca/en/government/system/digital-government/online-security-privacy/government-canada-guidance-using-electronic-signatures.html) but provides a more condensed tutorial on the terminology.

# GC e-signature legislation and terminology

Part 2 of the [*Personal Information Protection and Electronic Documents Act*](https://laws-lois.justice.gc.ca/eng/acts/p-8.6/FullText.html) (PIPEDA) defines an *electronic signature* as follows:

“a signature that consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document.”

Essentially, an electronic signature (also denoted as “e‑signature” for short[[1]](#footnote-2)) can be virtually any form of electronic representation that can be linked or attached to an electronic document or transaction. Although not intended to represent an exhaustive list, examples of e-signatures include:

* user authentication combined with a mouse click on some form of acknowledgment button to capture intent (i.e., “click to sign”)
* using a stylus on a tablet touchscreen to write a signature by hand and capture it in electronic form
* a typed name or signature block in an email
* a scanned hand-written signature on an electronic document
* a sound such as a recorded voice command (for example, a verbal confirmation in response to a question)
* a digital signature
* a secure electronic signature

Notice that both digital signatures and secure electronic signatures are considered to be a form of an e-signature.

In the context of the GC the earliest definitions for digital signature date back over two decades with the introduction of the [*Payments and Settlements Requisitioning Regulation*](https://laws-lois.justice.gc.ca/eng/regulations/sor-98-130/index.html) and the [*Electronic Payments Regulatio*n](https://laws-lois.justice.gc.ca/eng/regulations/sor-98-129/index.html).[[2]](#footnote-3) Both regulations define a digital signature exactly the same as follows:

“the result of the transformation of a message by means of a cryptosystem using keys such that a person having the initial message can determine:

* + whether the transformation was created using the key that corresponds to the signer’s key, and
  + whether the message has been altered since the transformation was made.”

The Canadian Centre for Cyber Security also provides a definition for digital signature in [*ITSP.40.111*](https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111):

“a cryptographic transformation of data which provides the service of authentication, data integrity, and signer non-repudiation.”

In essence, a *digital signature* is a type of e-signature based on asymmetric cryptography. The signer of the message, document or transaction uses their private signing key to create a digital signature and anyone with access to the signed data and the signer’s public key verification certificate can verify the digital signature.[[3]](#footnote-4)

However, not all digital signatures are created equal and some are more reliable or robust than others. For example, the manner in which a signer’s identity is verified before issuing their public key verification certificate, the type of token used to store the signer’s private signing key, the trustworthiness of the Certification Authority (CA) that issues the public key verification certificate and the digital signature algorithm and key length (among other things) collectively determine the reliability of the digital signature.

This is where the term “secure electronic signature” comes in. A secure electronic signature is also a digital signature but with specific characteristics as defined in Part 2 of PIPEDA as follows:

* the electronic signature resulting from the use by a person of the technology or process is unique to the person;
* the use of the technology or process by a person to incorporate, attach or associate the person’s electronic signature to an electronic document is under the sole control of the person;
* the technology or process can be used to identify the person using the technology or process; and
* the electronic signature can be linked with an electronic document in such a way that it can be used to determine whether the electronic document has been changed since the electronic signature was incorporated in, attached to or associated with the electronic document.

While Part 2 of PIPEDA does not actually use the term “digital signature”, the Secure Electronic Signature (SES) Regulations refine the definition using the term “digital signature”. Specifically, the SES Regulations state “a secure electronic signature in respect of data contained in an electronic document is a *digital signature* that results from completion of the following consecutive operations…” The SES Regulations also specify the technology or process that must be used to generate and verify secure electronic signatures. In addition, the SES Regulations:

* prescribe a specific asymmetric algorithm to support digital signatures[[4]](#footnote-5)
* specify that the issuing Certification Authority (CA) must be recognized by the Treasury Board of Canada Secretariat by verifying that the CA has “the capacity to issue digital signature certificates in a secure and reliable manner”
* include a presumption that, in the absence of evidence to the contrary, the electronic data has been signed by the person who is identified in the digital signature certificate or who can be identified through that certificate.

PIPEDA dates back to 2000 and the SES Regulations came into effect in 2005. It should be noted that PIPEDA Part 2 is based on an “opt-in” framework and the adoption rate of PIPEDA Part 2 within the federal government has been minimal. In addition, the SES Regulations are dated and need to be revisited. In cooperation with key stakeholders, TBS is currently exploring possible improvements to the existing federal electronic signature legislation.

# A note on e-signature implementations within the GC

Many departments are already deploying e-signature solutions to meet their business needs. A number of departments are using their GC myKEY credentials to digitally sign MS Office and PDF documents. This allows GC departments to leverage their existing investments in PKI technology and take advantage of digital signature features offered by MS Office products such as Word, PowerPoint and Excel as well as various PDF software products. SSC is one of the departments that have adopted this approach and they have shared their documentation (including getting started guides) that can help other departments enable this approach (please refer to <https://gccollab.ca/file/group/976512/all#2466578> for additional information).

Although not defined within Canadian legislation, there are some additional terms that you may encounter when deploying these solutions. For example, digitally signed MS Office documents conform to the [XML Advanced Electronic Signature[[5]](#footnote-6) (XAdES) standards](https://www.etsi.org/standards#page=1&search=XAdES&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2020-06-01&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1). When you examine the digital signature details of a digitally signed MS Office document, you may see the signature type identified as “XAdES-EPES”. This is one of the variants of the XAdES specification and according to Microsoft documentation is the default digital signature type for MS Office products. In addition, digitally signed PDF documents conform to the [PDF AdES (PAdES) standards](https://www.etsi.org/standards#page=1&search=PAdES&title=1&etsiNumber=1&content=1&version=0&onApproval=1&published=1&historical=1&startDate=1988-01-15&endDate=2020-06-01&harmonized=0&keyword=&TB=&stdType=&frequency=&mandate=&collection=&sort=1) so you may encounter variants of PAdES when working with PDF documents. However, please note that users are typically not required to understand this level of detail.

# Summary

This post addresses electronic signature definitions relevant to the GC. In summary, an “electronic signature” or “e-signature” should be thought of as an umbrella term that applies to any type of signature that can be represented electronically and associated with a document, record or transaction. A “digital signature” is a type of e-signature that is created and verified using asymmetric cryptography and supporting PKI. A “secure electronic signature” is a digital signature that meets the specific requirements defined in PIPEDA Part 2 and the SES Regulations.

The [*Government of Canada Guidance on Using Electronic Signatures*](https://www.canada.ca/en/government/system/digital-government/online-security-privacy/government-canada-guidance-using-electronic-signatures.html) document provides additional guidance regarding the use of e-signatures within the GC. Annex A of that document addresses e-signature terminology found in other jurisdictions including Provincial, the US and the European Union.

1. There are other variations including e-Signature, E-Signature and eSignature. [↑](#footnote-ref-2)
2. Both regulations came into force on 23 February 1998 and therefore pre-date PIPEDA. [↑](#footnote-ref-3)
3. There are a number of considerations that determine whether or not a digital signature is “valid” including the revocation status and validity period of the associated public key certificate. [↑](#footnote-ref-4)
4. The algorithm description in Section 2 of the SES Regulations is so specific that it is describing the Rivest-Shamir-Adleman (RSA) digital signature algorithm. [↑](#footnote-ref-5)
5. The European Union defines an Advanced Electronic Signature in their [Electronic Identification, Authentication and Trust Services (eIDAS) Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG) – it is defined almost exactly the same as the SES definition found in PIPEDA Part 2. [↑](#footnote-ref-6)