



# LAWS OF eSIGN

India's first authoritative book on the  
legal and technical framework of eSign

FOREWORDS BY  
SR. ADV. GOURAB BANERJI & SR. ADV. SAJAN POOVAYYA

[www.leegality.com](http://www.leegality.com)

# ACKNOWLEDGEMENTS

## AUTHORS

**Name:**

**Contact:**

**Ancha Venkata Samarth**

(Content Specialist @ Leegality | previously Associate @ IndusLaw)

avs@leegality.com

**Aditya Patel**

(Director - Growth @ Leegality | previously Advocate, Karnataka High Court)

aditya@leegality.com

**Vinodini Srinivasan**

(Counsel, Bombay High Court)

vinodinisrinivasan@gmail.com

## EDITORS

**Name:**

**Contact:**

**Suswagata Roy**

(Partner @ NKR Law Offices)

sroy@nkrlaw.com

**Ancha Venkata Samarth**

(Content Specialist @ Leegality | previously Associate @ IndusLaw)

avs@leegality.com

**Aditya Patel**

(Director - Growth @ Leegality | previously Advocate, Karnataka High Court)

aditya@leegality.com

We would also like to thank **Senior Advocates Gourab Banerji and Sajan Poovayya** for writing very thoughtful forewords for this book.



# FOREWORD

Companies in India are increasingly looking to eSign as a critical first step in digitally transforming their paperwork processes. In this book, which is arguably the first of its kind, Leegality discusses the validity and enforceability of electronic signatures and the associated technical and legal framework in India.

The increase in digitalisation has witnessed a shift from the use of wet-ink signatures to E-signatures. While the trend has been towards all things digital since the turn of the century, the COVID-19 pandemic has acted as a catalyst in this change. It is no longer beyond the bounds of possibility for Leegality to envisage a market where electronic signatures have started substituting the classic “pen” signature. I believe that the digital transformation brought about the COVID-19 pandemic is here to stay. Thus, it is vital that we develop a deeper understanding of electronic signatures.

The pandemic has drastically reduced face-to-face interactions due to the restrictions imposed by governments on the movement of people in order to curb the spread of the virus. Adapting to these changes has greatly impacted the way we conduct our personal and business transactions. Necessarily, the remote work environment has reduced wet-ink signatures and increased the use of electronic signatures for contracts. Now parties have various options to conclude a contract. They can click a button to sign an electronic document, add their signature at the end of an email, or upload a picture of their signature. In this changing environment, this book highlights the nuances of electronic signatures.

Different types of electronic signature techniques have been developed over the years. Those can be broadly classified into four categories:

- 1) Those based on the knowledge of the user or the recipient, such as passwords and personal identification numbers;
- 2) Those based on the physical features of the user, such as biometrics and facial recognition;

- 3) Those based on the possession of an object by the user, such as codes and magnetic cards.
- 4) Those that indicate the originator of the electronic communication, such as the facsimile of a handwritten signature or a name typed at the bottom of an electronic message.

Based on the principle of technological neutrality, many jurisdictions, including India, have deliberately kept the definition of electronic signature broad. The aim is to accommodate all forms of electronic signatures by encompassing all existing and future electronic signature methods. As long as the methods used are reliable and appropriate for the purposes for which the data message was generated or communicated, such signatures would be regarded as meeting the legal signature requirements. Accordingly, electronic signatures would cover the entire spectrum of electronic signature techniques from higher-level security, such as cryptographically based signatures to lower levels of security, such as the author's name at the end of an email message.

Digital signatures are a sub-set of an electronic signatures. It is a name for technological applications that use asymmetric cryptography ensuring the authenticity of electronic messages and guaranteeing the integrity of the contents of those messages. There are various reasons why this book, which dives deep into the world of electronic signatures, is being published at an opportune moment and provides valuable insights to the reader.

Firstly, with the world reeling from the pandemic and businesses increasingly "going virtual", there is a lack of information about the validity and legality of most things digital; the act of electronic signing is not an exception.

Secondly, there is, to the best of my knowledge, no single book dedicated to explaining the first principles of the meaning of a "signature" itself, and then tying it up with the "electronic" version thereof. I particularly liked the comment by the authors that a signature is "an anchor of security and integrity".

Thirdly, with any progress in technology, there is usually always a "Luddite" pushback to the innovation. To engage with the scepticism or doubt relating to electronic signatures, the authors have dedicated Part I and II of the book to the validity and kinds of electronic signatures themselves. The techno-legal frame-

work is explained in the layperson's vocabulary, without missing out on the legal niceties. Part II is a commendable piece of research dedicated to explaining as to why businesses and industry, and, indeed, we have nothing to fear about the validity of the electronic signature.

Fourthly, the present authors are rooted in the industry about which they seek to inform the public. The book, essentially, distils the knowledge that they have acquired through their experience over the years. This is supplemented and complemented by the expertise of various clients.

Lastly, it is rather ironic that in today's day and age, with billions of dollars' worth of investment, investors and banks still rely on the classical pen signature. What could be a better reason for this book than the example of an Indian multinational technology company specialising in digital payment system entering into a contract with its venture capitalists by way of the good old signature?

This book is the perfect companion for Indian lawyers looking to gain an in-depth understanding about the laws governing eSign in India. Whether you are part of a law firm that is advising its clients or an inhouse counsel who has received a request to scrutinize a new digital onboarding process, or even an interested member of the public- this book is for you.



**GOURAB BANERJI**

Senior Advocate, Supreme Court of India

Sitting in my chambers, I'm looking at the voluminous paperwork involved in legal proceedings. Case briefs relating to disputes argued over decades, stored away in numerous cupboards, with more coming in every day. This got me thinking. If this is how it is at a lawyer's chambers, storing thousands of paper based agreements must be a nightmare for businesses. This begs the question - why are critical legal documents, which codify and specify commercial legal relationships, documented and reproduced on paper anyway?

To answer the question, we should take a step back. Maybe even get a little philosophical. To understand why agreements are produced on paper, we need to understand how and when agreements transform from negotiated set of terms and conditions to actionable legal reality. In our times, drafts of all agreements are created on computers. The genesis is therefore electronic. Why then do we convert the agreement into physical form and have parties endorsed their acceptance by physically signing the paper on which the agreement is reproduced? With more efficient electronic means at our disposal why should we tread the physical path?

There are numerous operational difficulties with a physical signature. One has to spend time, money and effort to print paper, physically dispatched documents, gather people and have them append their elusive signatures. As a lawyer I can't help but worry about the security aspects of paper based agreements. Paper based agreements, the traditional storehouse of parties' legal rights and duties, are highly prone not just to wear and tear, but also to interpolations and superimpositions. Once anyone signs a physical agreement, it is easy to just take a page out from the document or insert one - or simply raise such contention in Court. Replicating a physical signature is rather easy.

One lived with these problems for there were no real alternatives to the classic wet-ink signature. The Information Technology Act changed it all by ushering more efficient alternatives. The technical superiority of electronic signatures or eSigns over physical signatures, in fulfilling the functions of legal and documentary certainty, really leaves one with no option but to switch over. It is extremely difficult for an author to repudiate her electronic signature at a later point in time. It is equally difficult for a third party to replicate the author's electronic signature. A document executed through electronic signatures cannot be easily tampered and

such safeguard is by design. There are hundreds of benefits that convince a lawyer to switch to eSigns. The icing on the cake is that such benefits are not only technologically assured, but also legally recognised.

The Information Technology Act confers on electronic signatures legal validity, whilst the Evidence Act works in tandem to make electronically executed documents easily enforceable in Courts of law. The numerous presumptions in favour of eSigns contained in the Evidence Act make a litigator's life so much easier, while having to prove an agreement in Court.

With any big change, such as the switch to electronic signatures, there is bound to be initial hesitation. With technology and legal ecosystem available to secure the terms and conditions of a legal relationship between parties, why should mindsets and lack of information become predominant hurdles to their adoption? This book puts all uncertainties to rest by consolidating and simplifying the body of laws on electronic signatures in India, whilst also offering a comprehensive overview of the technological architecture behind it. It does not just explain the law but goes on to explain why the law exists in its current form.

Building a complete ecosystem for digital execution of legal documents, digital registration of compulsorily registrable ones, digital notarization or authentication, digitally secure storage and digital production of evidence in courts of law will require many additional steps towards interoperability, electronic signature is a critical and essential first step in spurring this transformation. Therefore, it is imperative for lawyers to understand the legal and regulatory framework that help make eSigns valid and enforceable in India. This book enormously helps lawyers in the endeavour.



**SAJAN POOVAYYA**

Senior Advocate, Supreme Court of India



# TABLE OF CONTENTS



## **Prologue: What is a signature.....01**

Explore the 3 essential functions performed by signatures to understand why we need them at all

## **Introduction: A framework for evaluating electronic signatures.....09**

We lay down a practical framework to examine the legality of electronic signatures through the prism of 2 concepts: Validity and Enforceability

## **PART I: VALIDITY**



## **Chapter 1: Introduction to validity of eSign.....15**

Before we deep dive into the world of eSign, let's take a look at where it cannot be used

## **Chapter 2: The foundation of eSign in India - Section 5 of the IT Act.....18**

Breaking down Section 5 of the IT Act - the provision which makes eSigns the legal equivalent of traditional wet-ink signatures

## **Chapter 3: Digital Signatures under Section 3 of the IT Act.....21**

Deep dive into the legal and technical framework behind Digital Signatures

## **Chapter 4: Schedule 2 Electronic Signatures.....38**

### **Part 1 - Legal and Technical Framework**

An analysis of the legal provisions that introduced the concept of electronic signatures in India:

The 2008 amendments to the IT Act

### **Part 2-Schedule 2 of the IT Act and the regulatory framework for electronic signatures.....44**

A comprehensive overview of the regulatory framework behind electronic signatures listed under the Second Schedule of the IT Act - Aadhaar eSign and PAN eSign.

**Chapter 5: Other modes of electronic execution.....58**

Explore the other commonly used methods of electronically executing documents

**Chapter 6: Validity Matrix.....68**

In this chapter we give you a matrix that you can use to determine if a particular signing type is valid for the document that you want to get signed

**PART II: ENFORCEABILITY**



**Chapter 7: The Enforceability of eSigned documents.....72**

To understand why someone would choose a certain method of electronic execution when there may be multiple legally valid methods, we plot the different methods of execution discussed so far against how well they meet the end goals of the signing process.

**Chapter 8: Legal Presumptions in favour of eSigns under the Evidence Act.....89**

In this chapter we list out various provisions of the Indian Evidence Act, 1872 that make eSigns the most easily enforceable form of executing documents

**Chapter 9: Producing electronic agreements as evidence in Court.....101**

An overview of the law on Section 65B of the Indian Evidence Act, 1872 to understand how one can produce electronic agreements as evidence in Court

**ANNEXURES**



**Is reliability alone not a sufficient criteria?.....110**

Here we put to rest any debate about whether a type of eSign can be classified as an electronic signature under the IT Act without it being specified in the Second Schedule of the IT Act.

**Compendium of legal provisions and case laws.....114**

A ready referencer of all the relevant legal provisions and Supreme Court judgments.

**Sample 65B Certificate.....135**

An indicative Section 65B certificate that you can use to tender electronic agreements as evidence in Court.

# PROLOGUE



## WHAT IS A SIGNATURE?

Before we deep-dive into the world of electronic signatures it's important to understand the function of signatures in the first place.

*But first, a small story.*



# AKANKSHA'S STORY



Akanksha was happy and relieved.

Her application for a two wheeler loan had just been approved by her Bank.

Her office was commencing work-from-office for 3 days a week - but taking the metro was out of the question now.

So she really needed this two wheeler loan to come through - to give her mobility and freedom.



Now that it was approved, she could finally purchase that Bajaj Chetak that she had been eyeing since the end of the lockdown.

An agent from her Bank visited her house with the loan documentation.

The Loan Documents record the terms and conditions for the loan. Some key ones:

- (a) Disbursal amount.
- (b) Repayment Schedule.
- (c) Rights of Bank X in the event of default by Akanksha.
- (d) Rights of Akanksha.

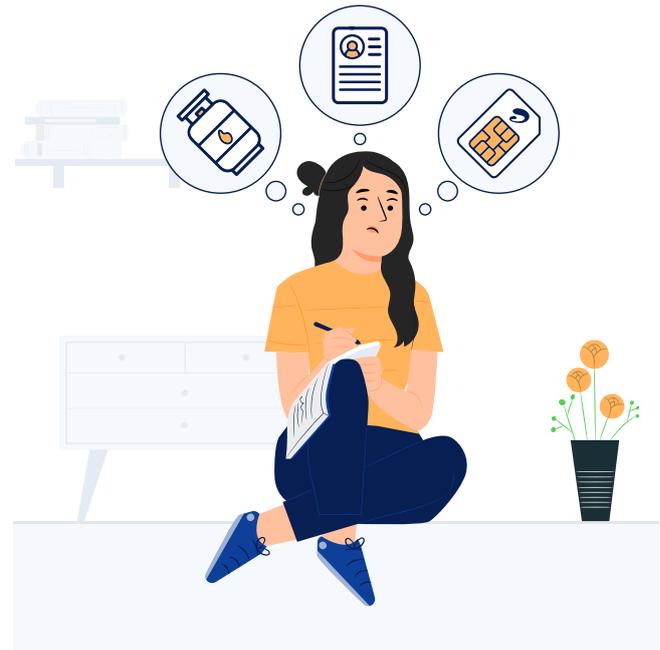
Akanksha has already seen these terms, the Bank had sent them to her via email earlier - and she was okay with them.

But despite this the agreement is not complete.

Akanksha takes a blue ball-point pen out of her pocket and goes through the voluminous sheaf of papers in front of her.

On each page, she scribbles her signature in the designated spots on each page of the 40 page loan booklet. This process of signing is something she is intimately familiar with. She's done it for many things - for getting a gas connection, for starting her new job, for her new Airtel SIM and even for getting her marriage registered.

After flipping through the Bank's loan booklet once more - she realises she has missed a spot. She makes her trademark wavy flourish signature in the vacant box.



45 minutes since Akanksha entered the branch, the Agreement is now complete.

A week after she signed the documents, the Bank disbursed the loan directly to Akanksha's bank account. And she immediately purchased her cherished "Bajaj Chetak".

There is something that sticks out above. The Agreement was finalized even before the Bank agent walked into Akanksha's house. Both Akanksha and the Bank were aware - and had accepted - the terms of the agreement.

Why did the Bank put in so much effort in sending an agent to Akanksha simply to collect her signature?

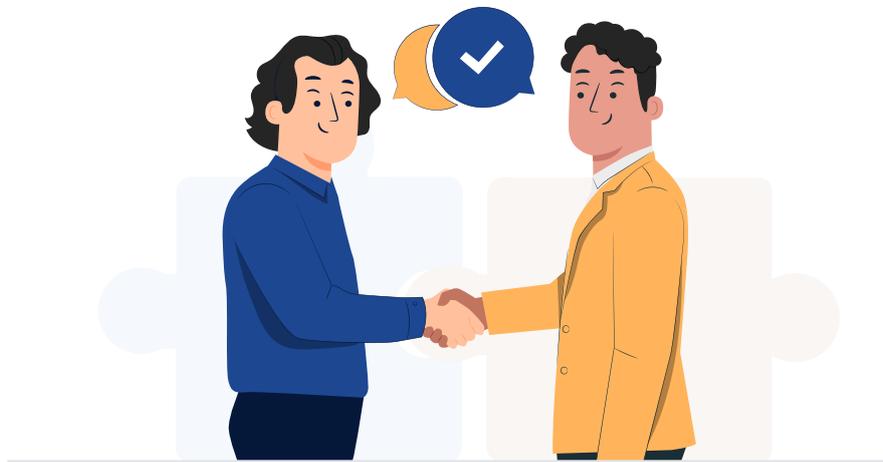
## WHY DID THE BANK NEED AKANKSHA'S SIGNATURE?

Contracts/agreements - such as the loan agreement between Akanksha and her Bank - codify, specify and clarify commercial business transactions and relationships.

Without a contract/agreement, a commercial transaction cannot move forward.

Even though any party can type and print out a draft contract; there is still a need for all parties to signal acceptance to the contract's terms.

In the case of oral agreements, the handshake is often used as a signal of acceptance.



In the case of written contracts, handshakes are not enough.

Parties need a written signal of acceptance for written agreements. For millennia, the signature has fulfilled this role for written contracts.



# THE SIGNATURE IS AN ANCHOR OF SECURITY AND EVIDENCE

An agreement without a signature is open, floating, ambiguous and extremely hard to enforce. The signature anchors the agreement to a legally binding, enforceable, actionable reality.

A signature ensures authentication, integrity and non-repudiation of a document:

 <p><b>AUTHENTICATION</b></p> <p>The identity of the parties signing the document is clear</p>	 <p><b>INTEGRITY</b></p> <p>The document cannot be changed unilaterally after the signatures are affixed</p>	 <p><b>NON-REPUDIATION</b></p> <p>The parties cannot “deny” their acceptance of the terms and conditions of a document at a later stage</p>
---	---	--

Let’s unpack each of these layers a bit.

## AUTHENTICATION

When parties “sign” a document, they convey:

- (a) - The identity of the parties entering into a contract.
- (b) - The personal involvement of the parties in the actual act of “authenticating” or “accepting” the contract.
- (c) - The acceptance, by the parties, of the terms and conditions contained on the document they are signing.

Thus, parties are authenticating the document and its contents with their identity.

## INTEGRITY

The act of signing intends to “capture” or “preserve” the contents of the document at the time of signing.

That’s why, for revisions, parties often have to attest to the revision with a fresh signature. Without the fresh signature - revisions are often “not counted”.

Therefore signatures are like a security feature - playing a vital role in preserving the integrity of the final version of a document and its subsequent modifications.

## NON-REPUDIATION

The act of signing lends immense **trust and credibility** to the contract in two ways:

**(A) Commercial Security:** By making a tangible, preservable mark on a document, parties signal to each other that they are serious about honoring their commitments detailed in the document. It's a tangible, visual representation of the honour-bound handshake.

**(B) Legal Security:** It is extremely hard to prove to a Court that a handshake or oral agreement actually happened. Courts find it significantly easier to rely on the presence of the parties' actual signatures on a document to treat that document as legally valid and binding on those parties.

The above details are also an invaluable source of evidence.

Since Akanksha signed the loan agreement, her Bank now has a written commitment they can enforce in a Court of law if Akanksha defaults.

The Bank's authorized signatory's sign on the loan booklet has immense value for Akanksha as well - it ensures that Akanksha can hold the Bank to its commitment to disburse the loan in the manner promised - ensuring she gets the funds to buy her Bajaj Chetak and attains the mobility and freedom she has long pined for.

## MOVING AWAY FROM THE TRADITIONAL UNDERSTANDING OF THE SIGNATURE

We often define a signature as a handwritten, usually personalised, depiction of a person's name, marked on a paper with ink.

However, this definition is simply a holdover from the physical document execution process that drove contract formation and legal procedures for millennia. We think a signature means a physical mark made with ink simply because that is the only way humans have been signing for thousands of years!

The advent of electronic signatures forces us to re-examine this understanding.



Electronic signatures are not physical and they aren't marked with ink.

In countries like India, electronic signatures don't even have a unique physical form and are merely the product of a complicated hash function and asymmetric crypto function (more on this in subsequent chapters).

## SO THEN WHAT EXACTLY IS A SIGNATURE?

The following definition in C. Reed's Article in the Journal of Information, Law and Technology puts it in better words than we could:

"A signature, as a legal concept, bears no relationship to the popular conception of a name, on paper, in the signatory's own handwriting. A signature is not a 'thing', but a process. If that process produces sufficient evidence that a person has adopted a document as his own, and that the document before the Court is the same document to which the process was applied, then the document has been signed. It is irrelevant whether the result of the process is a visible name, a symbol, or a logical alteration of information content. To the question 'what is a signature', the answer is now a single word - 'evidence'." (emphasis supplied)



The United Nations Commission on International Trade Law (UNCITRAL) adopts a similar definition:

"Signatures, in turn, perform three main functions in the paper based environment: signatures make it possible to identify the signatory (identification function); signatures provide certainty as to the personal involvement of that person in the act of signing (evidential function); and signatures associate the signatory with the content of a document (attribution function).

Signatures can be said to perform various other functions as well, depending on the nature of the document that was signed. For example, a signature might attest to the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text (thus displaying awareness of the fact that legal consequences might possibly flow from the act of signing); the intent of a person to associate him or herself with the content of a document written by someone else; and the fact that, and the time when, a person has been at a given place." (emphasis supplied)



If you notice, both the above definitions are in perfect sync with the initial definition of signature that we offered - a signature is a process which ensures authentication, integrity and non-repudiation of a document.

They also fit in nicely with the subject of this book - signing documents “electronically”.

# INTRODUCTION



## **A FRAMEWORK FOR EVALUATING ELECTRONIC SIGNATURES**

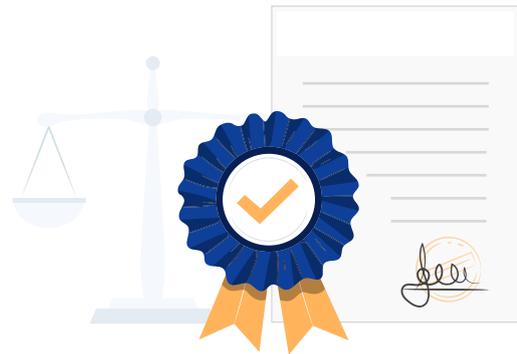
We will be examining electronic signing methods from the prism of 2 primary concepts:

- **Validity** : Whether a particular electronic signing method can, under law, be used for a particular document
- **Enforceability** : How easy or difficult it is to enforce/prove a document that is executed by a particular electronic signing method

## THE QUESTION OF VALIDITY

Validity of a signature for a particular document is a simple “yes or no question”. A signature is either valid or invalid for a particular type of use case. There are no “maybes”.

Validity is **purely** a construct of law - whether by legislation or by regulation.



Under Indian contract law, even an oral contract is valid provided it fulfils the criteria for acceptance under the Indian Contract Act. This means a “handshake” or an “oral yes or no” that fulfils the conditions for acceptance under the Contract Act would be **legally valid**.

In this scenario, an oral acceptance would be equally valid to an electronic signature or a wet-ink signature. There is no question of the oral acceptance being “less valid” than the wet-ink signature or electronic signature.

Let’s take another example. A demat account opening form - common in the investment advisory industry. SEBI, by regulation, **mandates** that such a form be **signed** by investors.

So if a Portfolio Management Service wanted to open a demat account for its customer on the basis of a **handshake** - they would not be able to do so legally as per SEBI guidelines. They would necessarily need to use a **wet-ink** or an **electronic** signature by law.



There is no question of **less valid or more valid**. The handshake here is **invalid** for demat account opening forms as the law requires a signature to be the mode of acceptance. Whereas Both **wet-ink** and **electronic** signatures are **valid** for demat account opening forms.

A matrix of validity for demat account opening forms in the PMS industry would look like this:

Document Type	Wet-Ink Signatures	Electronic Signatures	Oral HandShake
Demat Account Opening Form	✓	✓	✗

In Part I of this book we will be answering the question of validity of electronic signing in a comprehensive way by:

- 1 Examining the legal and technical framework for the 2 tiers of electronic signing in India - electronic signatures and other modes of electronic execution.
- 2 Laying down a Matrix of Validity that maps the validity of electronic signing in India for different documents.

### THE QUESTION OF ENFORCEABILITY

Enforceability is a question of “how easy” it is to “prove” a document in Court or before a regulator.



Enforceability is a creature of **function** rather than purely one of law.

Let’s take a loan agreement. A wet-ink signature would be **valid** to sign this. An electronic signature would also be **valid**.



Technically, as per the Contract Act, even an oral agreement entered into via hand shake would be **equally valid** compared to an electronic signature for executing a loan agreement.

But why don't legal teams in India's big banks use "oral handshakes" to execute loan documentation?

Because validity is NOT the only touchstone to evaluate a signature/execution type.

The journey of a legal document, like a contract, does not simply end at the time of execution.

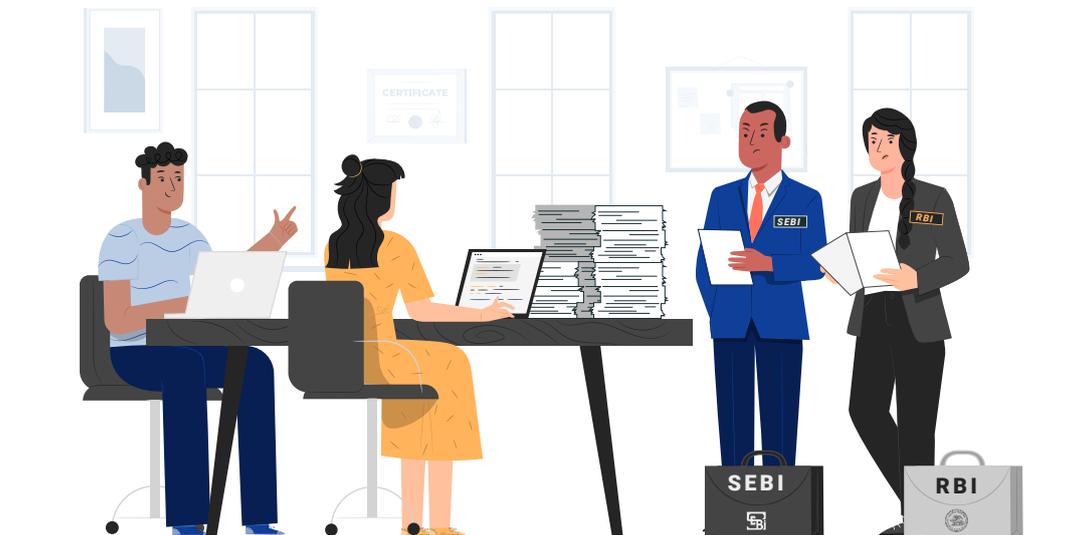
In fact, the whole purpose of executing a legal document is to **use the legal document** in 2 post execution scenarios:

**A)** When a default is committed, the aggrieved party can use the signed legal document as evidence to enforce its claims against the party in breach before a judicial authority



**B)** Regulators like the RBI often conduct audits of the documentation executed by a Bank or NBFC. Signed legal documents are essential to prove compliance before regulators

This stems from the idea that regulators do not encourage or support that borrowers should assume loans without any written document explaining the terms of the loan.



An oral handshake – while being valid in the eyes of the law – won't be of much use in the above scenarios.

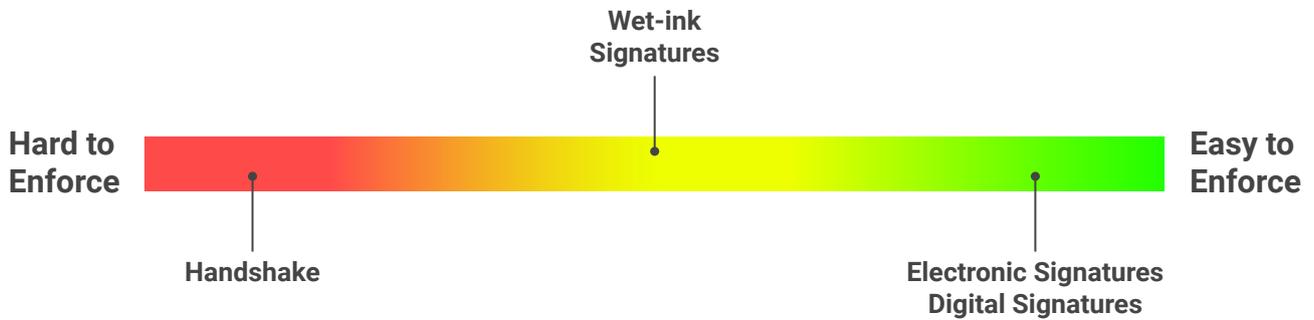
Imagine trying to “prove” that you shook hands with someone in a Court of law. Imagine telling the RBI that the terms and conditions of your loan agreements exist in the hearts and minds of the parties involved.



That's where the concept of **enforceability** comes in. It's not a simple yes or no question. It's more like a spectrum.

A spectrum of enforceability for the loan agreement we mentioned would look something like this:

### THE SPECTRUM OF ENFORCEABILITY



In the second part of this book - we will be deep-diving into the enforceability of various signing types by:

- 1 Mapping the most common types of electronic signing on the spectrum of enforceability
- 2 Examining presumptions of validity under the Evidence Act that exist in favour of certain types of electronic signing that make them even easier to enforce
- 3 Looking at a brief overview on the process that the Evidence Act lays down for producing electronic agreements as evidence in Court



# PART-I

## VALIDITY OF ELECTRONIC SIGNING

The validity of electronic methods of “signing” in India stems from the Information Technology Act, 2000 (**IT Act**)

In this part we will deep-dive into the various valid electronic signing methods in India.

# CHAPTER



# INTRODUCTION TO VALIDITY OF ESIGN

## THE TWO BROAD CATEGORIES OF VALID ELECTRONIC SIGNATURES

Electronic signing methods under the IT Act broadly fit into two categories:



**TIER 1**  
Electronic Signatures



**TIER 2**  
Other Modes of Electronic execution

In this part of the book we'll be unpacking each category of electronic signing by examining:

- How they work (**Technical Framework**)
- How they are allowed (**Legal Framework**)

## ARE THERE ANY DOCUMENTS WHICH CANNOT BE ELECTRONICALLY SIGNED?

The IT Act is an enabling legislation that holds the field when it comes to electronic signatures. This means that if the IT Act says a particular electronic signing type is valid - then you can use that signing type to eSign any type of document (subject to the conditions laid down in the IT Act) WITHOUT the need of any subsequent law or regulation.

The IT Act accords validity to electronically sign virtually ALL types of documents.

However, there are narrow exceptions to this rule.

Schedule I of the IT Act prescribes 5 types of document to which the **IT Act would not apply:**

- (a) Negotiable instruments (other than cheques)
- (b) Powers-of-attorney
- (c) Documents that create trusts
- (d) Wills and other testamentary depositions
- (e) Contracts for the sale of conveyance of immovable property or any interest in such property

It is important to note that Schedule I does not **bar or prohibit** electronic signing types for the 5 documents mentioned above. It merely says that, by default, you **cannot** use electronic signing methods for the above 5 types of documents. You would need a **subsequent enabling law** or regulation in order to be able to electronically sign these documents.

Let's examine this with an illustration.

Let's say you have to get a Power of Attorney signed. You cannot eSign this Power of Attorney today because the IT Act has no **applicability** to Powers of Attorney. However, if tomorrow the Parliament amends the Powers of Attorney Act to allow electronic signing of powers of attorney then you **can** eSign your power of attorney.

However as mentioned above, Schedule I only applies to a very narrow set of documents. For ALL other documents - electronic signing types can be used.

# CHAPTER



## **THE FOUNDATION OF eSIGN IN INDIA - SECTION 5 OF THE IT ACT**

**Section 5 of the Information Technology Act** grants electronic signatures identical validity to wet-ink signatures:

**5. Legal recognition of electronic signatures** - Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

Explanation.- For the purposes of this section, “signed”, with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of this hand written signature or any mark on any document and the expression “signature” shall be construed accordingly.



That is - an “electronic signature” is seen as **legally identical** to a wet-ink physical signature - even if its form and design may be different.

The necessary implication of Section 5 is also that - **where any law** requires that **anything** needs to be authenticated via a “signature” - this can be done digitally via an electronic signature.

In other words, suppose a law or regulation prescribes that a particular type of document must **mandatorily** contain a signature of a party (note: the actual words “signature” or any adjunct version of that word must be used). Under Section 5 of the IT Act, an electronic execution of such a document is only possible with an **electronic signature**.

A few examples of documents which are required to be mandatorily signed under law:

- **Copyright assignment deed** - which are required to be signed under Section 19 of The Copyright Act, 1957
- **e-Insurance Policies** - which are required to bear electronic signatures of the issuer
- **KYC Documentation for various industries** - which also mandatorily require signatures by regulation

**Can electronic signatures be used for other types of documents?**

Electronic signatures can be used for **any document**.

While electronic signatures are **mandatory** for electronic documents where the law/ regulation requires a signature - they can also be used for other types of documents.



**WHAT ARE ELECTRONIC SIGNATURES UNDER THE IT ACT?**

In many global jurisdictions, electronic signature can be any digital representation of a sign e.g a stylus based representation.

Electronic signatures in India on the other hand are very specifically defined under the IT Act.

As per Section 2(ta) of the IT Act, an electronic signature can **only be one of two specific things**:

- An electronic technique specified in the Second Schedule of the IT Act (*elaborated more in Section 3A and Schedule II of the IT Act*)
- A digital signature (*elaborated more in Section 3 of the IT Act*)

**2. Definitions. -**

**(1)(ta)** “electronic signature” means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;



Now let’s deep-dive into the two types of signatures in the next two chapters.

# CHAPTER



## **DIGITAL SIGNATURES UNDER SECTION 3 OF THE IT ACT**

In this chapter we will look at some of the more traditional methods of digitally signing documents (DSC tokens and Doc Signer) and understand the underlying digital signature technology as prescribed under Section 3 of the IT Act.

## THE TECHNO LEGAL FRAMEWORK BEHIND DIGITAL SIGNATURES

Digital signatures are an algorithmic process to authenticate a document.

Fundamentally, digital signatures perform the same functions as wet-ink signatures:

- **Authentication:** The identity of the parties signing the document is clear
- **Integrity:** The document cannot be changed unilaterally after the signatures are affixed
- **Non-repudiation:** The parties cannot later “deny” their acceptance of the terms and conditions of a document at a later stage

However, as we’ll see in this section - digital signatures accomplish the above functions in a *significantly* more secure way than wet-ink signatures.

**Section 2(p)** of the IT Act defines digital signatures as:

(p) “digital signature” means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3



The key takeaway from the above definition is that digital signatures are a *process*. This matches the definition of signature we covered in the prologue to this book.

### THE 5 ELEMENTS THAT MAKE A DIGITAL SIGNATURE

The “digital signature” process - world over - consists of an algorithmic interplay between 5 elements:

- (A) An electronic record
- (B) A hashing function
- (C) An asymmetric cryptographic system
- (D) Hardware Security Module
- (E) Electronic Signature Certificates

While elements A to C are technology standards that are common across the globe, elements D and E are governed by a regulatory process that varies based on local law and regulations.

In this section we'll examine elements A to E - along with the laws/regulations in India that codify this.

## ELEMENT A - ELECTRONIC RECORD

A digital signature, as per *Section 2(p)* is a mode of authenticating an *electronic record*. *Section 3(1)* of the IT Act reinforces this idea.

**3. Authentication of electronic records.** - (1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.



Section 2(1)(t) of the Information Technology Act, 2000 ("**IT Act**") defines electronic record as:

(t) "electronic record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche



For all practical purposes, **ANY** piece of information that is in **electronic form** is an electronic record.

For most eContracts used in a commercial sense - an electronic record would be a PDF document.

Without an **electronic record** - you will have nothing to affix the signature on! It's pretty much the whole point of the digital signing process.



For agreements, electronic records are usually in PDF format

**ELEMENT B - HASHING FUNCTION**

The Explanation to Section 3(2) of the IT Act details what exactly a hash function is:

Explanation.- For the purposes of this sub-section, “hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

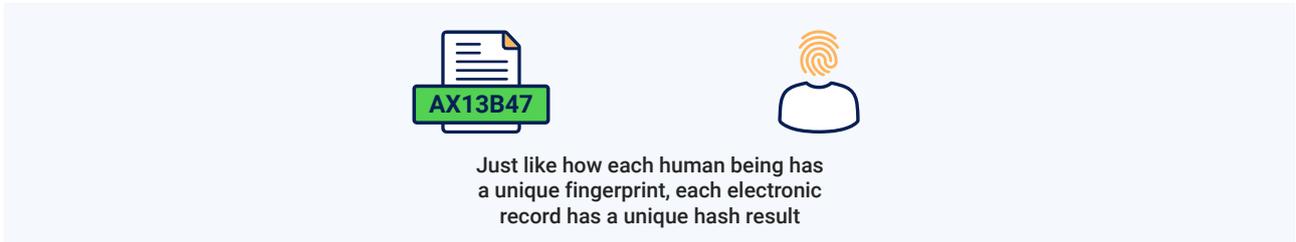
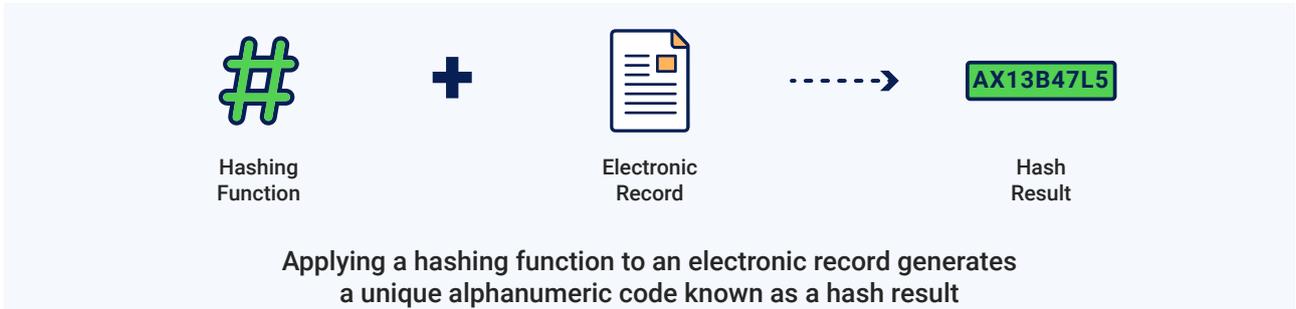
(b) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.



A hash function is, essentially, an algorithm that creates an alphanumeric “representation” of an electronic record - known as a hash result. Every time the hash function is run on a specific document - the same hash result will be generated.

Just like your fingerprint “represents” you in a unique way, a hash result is a unique alphanumeric code that **represents** an electronic record.



There are **2 immutable characteristics** that arise from a hashing function:

**(a) You cannot reconstruct the electronic record from the hash result:**

Your fingerprint is unique to you - but it’s just a representation. If someone gets possession

of your fingerprint - they cannot use that to reconstruct an image of you, right? Similarly, a hash result is just a representation of an electronic record. It cannot be used to recreate the document.

### (b) No two electronic records can produce the same hash result

Just like no two human beings can possess the same fingerprint, no two electronic records can possess the same hash result.

Hashes are a very useful security function - because they can detect ANY change in an electronic record. This is achieved through an elaborate process which we will discuss later in this chapter.

Suppose you apply a hash function to this book and obtain a hash result. Now let's say you make a very small change to the book through your PDF reader - like adding a full stop or a comma. To the naked eye - this document will seem to be the *same document*.

However if you perform a hashing function after you make this change - then you'll get a *completely different* hash result - a clear signal that the document has been changed or tampered with.

## ELEMENT C - THE ASYMMETRIC CRYPTO SYSTEM

An asymmetric crypto system is a system of encryption and decryption that is performed through a secure key pair.



A key doesn't mean a physical key. Instead a key - in crypto parlance - refers to a code that is used to perform an encryption or decryption function



A secure key pair consists of two keys

(A) **PRIVATE KEY** A function which encrypts a piece of information. A private key is **confidential** - being known and controllable **only** to the owner of the secure key pair.

- (B) **PUBLIC KEY** A function which decrypts the piece of information encrypted by the private key. Unlike a private key, the **public** key is public - it is known and controllable by **anyone**.

### The keys in a key pair are inextricably linked:

A private and public key in a secure key pair only work with each other and no other keys. So if, in a key pair, a private key encrypts a piece of information, this information can **ONLY** be decrypted by its corresponding public key. Similarly, a public key **CAN ONLY** be used to decrypt information that is encrypted by its corresponding private key.

#### *Confused? Let's look at an illustration.*

*Imagine that the piece of information you want to encrypt is a combination lock.*

*To lock it - or encrypt it - you have **one unique code** that is available **ONLY** to you. You use that code and lock it. This is akin to what a private key does to a piece of information.*



*Now imagine that the only way to unlock this lock is with **ANOTHER** code. But this other code is affixed as a sticky label on the lock. So anyone who sees the lock can view the code and unlock it. This is what a public key does to a piece of information.*



### Key Pairs are issued by a Certifying Authority

A private key is unique and confidential to its owner (the signer). And the public key is inextricably tied to this exclusive private key. But how exactly is this confidentiality and uniqueness ensured? How does one tie a key pair to its owner?

The answer is Certifying Authorities.

## ELEMENT D - HARDWARE SECURITY MODULE

The asymmetric cryptographic function is ultimately a computer program. It needs some computational power to work.

Where does that computational power come from?

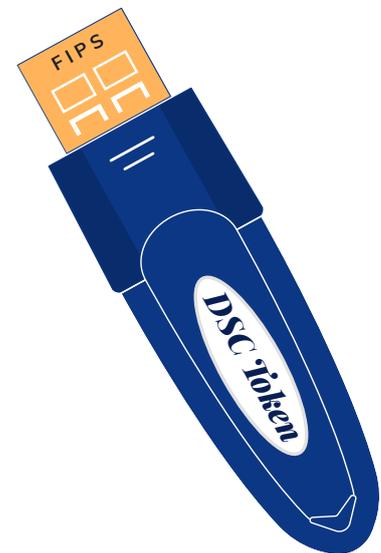
Hardware security modules.

A hardware security module is a physical computing device that stores the secure key pair - and provides the computational power for encryption to happen.

In the case of older forms of digital signature - the Hardware Security Module is in the form of a USB device - also known as a "token" - which every signer must possess.

In the case of newer forms of electronic signature like Aadhaar eSign - the Hardware Security Module is maintained by a neutral entity - enabling device-free electronic signing. We'll cover this in the subsequent chapters.

Hardware Security Modules are activated by a Unique PIN or identifier that is in the exclusive possession of the signer.



## ELEMENT E - DIGITAL SIGNATURE CERTIFICATES

The above elements leave a critical gap - *identity*.

**Think about it:**

- A) How do we ensure that a *secure key pair* is unique to *its owner*?
- B) How do we ensure that the encryption function performed on the *hardware security module* is done by the *signer*?

To solve this gap of identity, countries around the world have set up *neutral, heavily regulated* authorities known as *Certifying Authorities*.

Certifying Authorities are entities tasked with performing an *identity authentication* of prospective signers - and issue signature certificates on that basis.

## Here's how it works:



**A** Anyone who wants a digital signature i.e a subscriber, needs to approach a Certifying Authority. The Certifying Authority will do a KYC authentication process with the subscriber - verifying their identity on the basis of their identity documents. In some cases they also perform a video KYC.



**B** Once authentication is successful, the Certifying Authority will issue a Digital Signature Certificate to the subscriber consisting of a Secure Key Pair AND basic details describing the subscriber (name, gender, date of birth etc.) It is impossible for the subscriber to receive a Digital Signature Certificate in the name of any other person - because the Certifying Authority's KYC process will not allow this.



**C** In case of traditional digital signatures (DSC tokens) - the Certifying Authority also issues a hardware security module to the signer containing the digital signature certificate. This hardware security module can be activated only by a unique PIN in the exclusive possession of the signer.

The successful authentication described above is recorded by way of an electronic certificate known as a *digital signature certificate* or DSC. DSCs are **digitally signed** by Certifying Authorities to safeguard their integrity.

*While DSC tokens have been the most common way of affixing digital signatures, they are not the only way of doing so. Document Signer Certificate, or Doc Signer, is another method of applying digital signatures to an electronic document. Doc Signer certificates can be issued only to organisations, and not persons. It is similar to a digital signature certificate, the only difference being that only organisations can affix such certificates to a document. It does not operate through a USB device like DSC tokens. Rather, it is saved on the organisation's servers. Along with the certificate, configurations are installed on the server to use that certificate for signing. Doc Signer is typically used to automatically sign documents that are required to be executed by the organisation itself.*



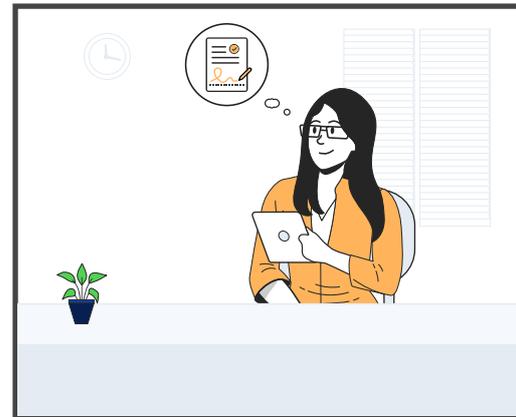
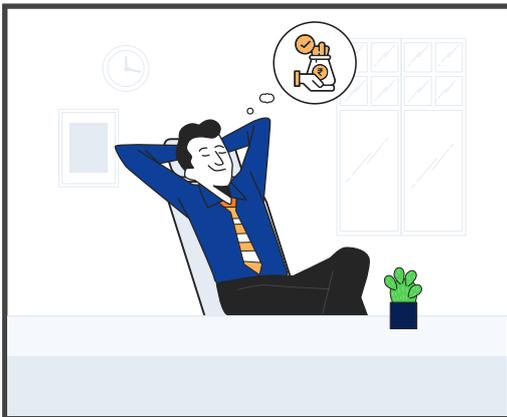
## THE DIGITAL SIGNATURE PROCESS

Ok, now that we've discussed the 5 elements that make up a digital signature - it's time to see how they all combine together to make the digital signature process happen.

We'll use a hypothetical to help us explain.

### Meet Waqim.

Waqim wants a loan from his bank - ABFC Bank. The Bank completes all of Waqim's KYC, vets his financial background and approves the loan. Before the Bank can disburse the loan - it needs to complete one critical final step - get a loan agreement signed by Waqim.



The Bank sends a PDF copy of the loan agreement to Waqim. This is the **electronic record** - the first element needed by Waqim to digitally sign it.



Waqim decides that he wants to digitally sign the document. Just 2 weeks back he had applied for a digital signature with a Certifying Authority. After a KYC and purchase process - the CA issued a digital signature certificate to Waqim - along with a physical hardware security module in the form of a USB token.

So now Waqim has the **fourth and fifth elements** as well - the hardware security module and the digital signature certificate.

Waqim opens the PDF document, plugs his DSC token into his laptop, enters his Unique PIN, selects the documents on which he wants the digital signature - and voila! The digital signature is completed.

But in this process - a LOT happens.

**Step 1: Generating the hash result**

When Waqim enters his unique PIN, the first thing his DSC Token does is perform a hashing function on the electronic record (the loan agreement).



The hashing function generates a hash result for the electronic record.

In the case of Waqim’s LOAN AGREEMENT, the following hash result is generated: W47JR73

**Step 2: Encrypting the hash result**

In the second step, Waqim’s private key kicks into action.

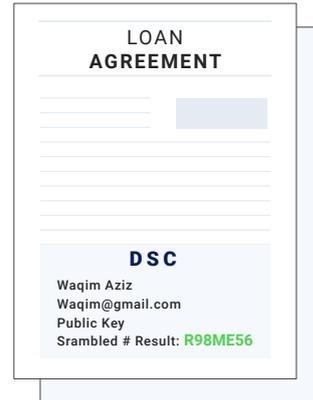
The private key performs its encryption function to scramble the hash result generated in the previous step.

So the original hash result W47JR73 now has a scrambled form which is R98ME56



### Step 3: Affixing the signature

The scrambled hash result is affixed on the electronic record along with the public key. This manifests itself as a digital signature certificate on the document. This certificate also contains several details to identify Waqim (his name, his year of birth etc.)



### Step 4: Sending the document

Waqim sends the digitally signed loan agreement to the Bank

The bank representative opens the agreement on a PDF Reader.

When the PDF reader detects a digital signature - it performs an elegant 3 part verification process - which we will cover in the next 3 steps



### Step 5: Hashing function again

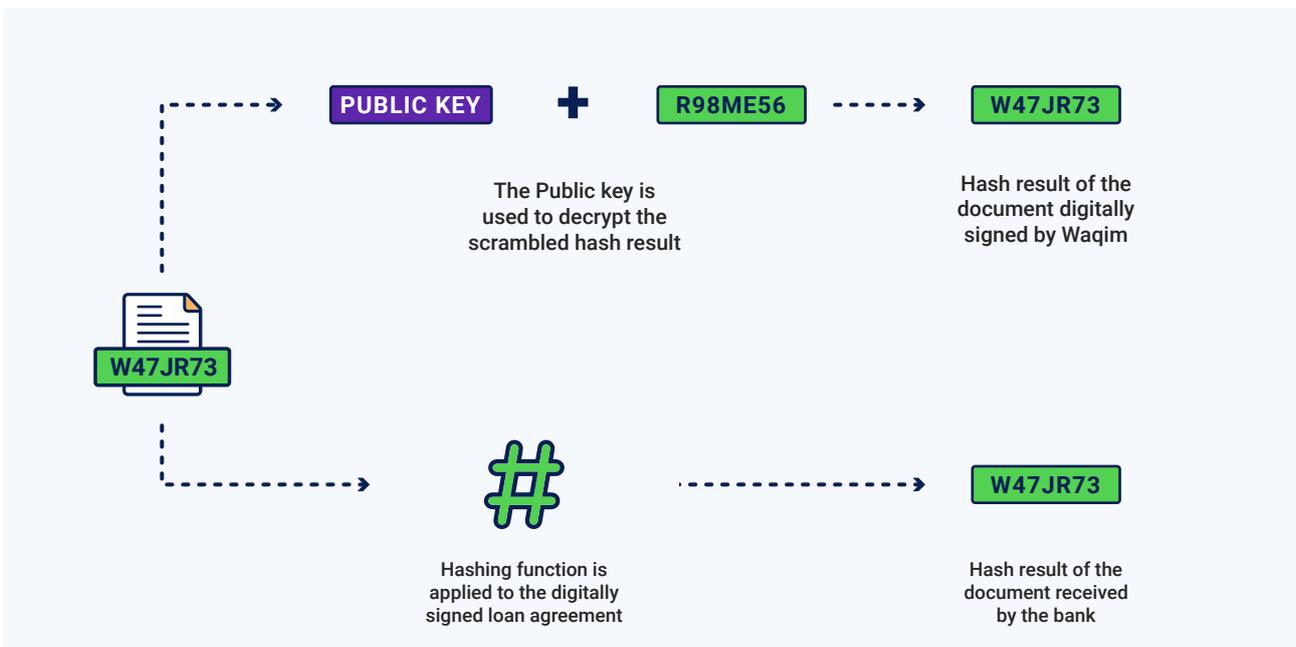
First a hashing function is performed on the digitally signed document. A *hash result* is generated. This hash result represents the document **at the time the Bank’s representative opened the document.**



### Step 6: Decryption

The PDF Reader ‘reads’ Waqim’s public key contained on the digital signature certificate. Using this public key, the PDF reader decrypts the scrambled hash result contained in the digital signature certificate.

The scrambled hash result now gets transformed to its original form - which represents the original hash value of the document **at the time Waqim digitally signed it.**

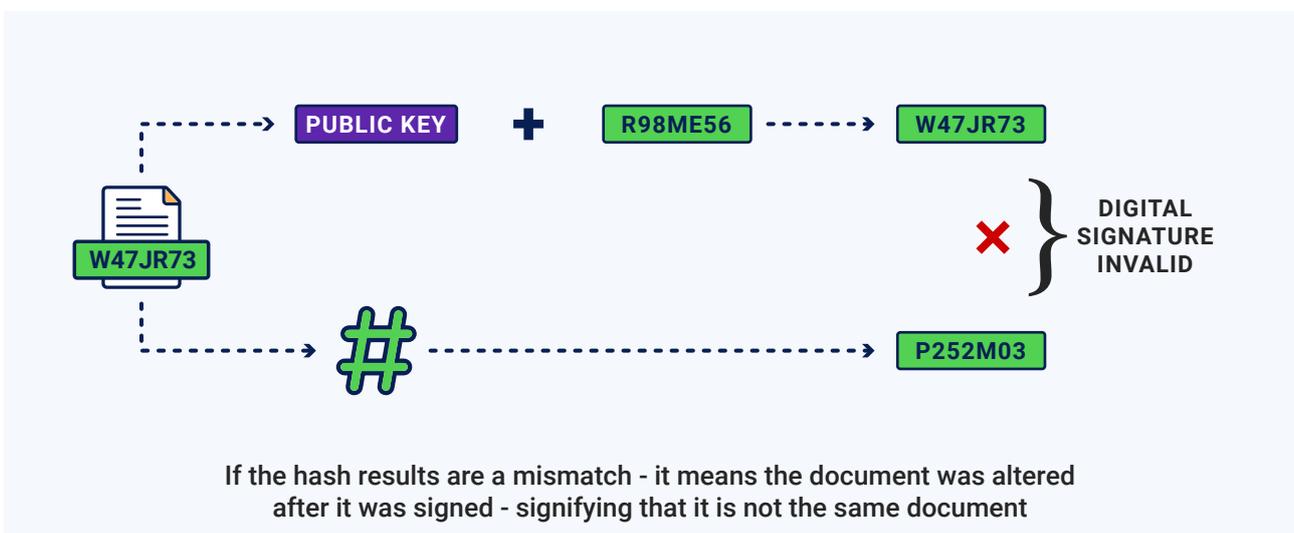
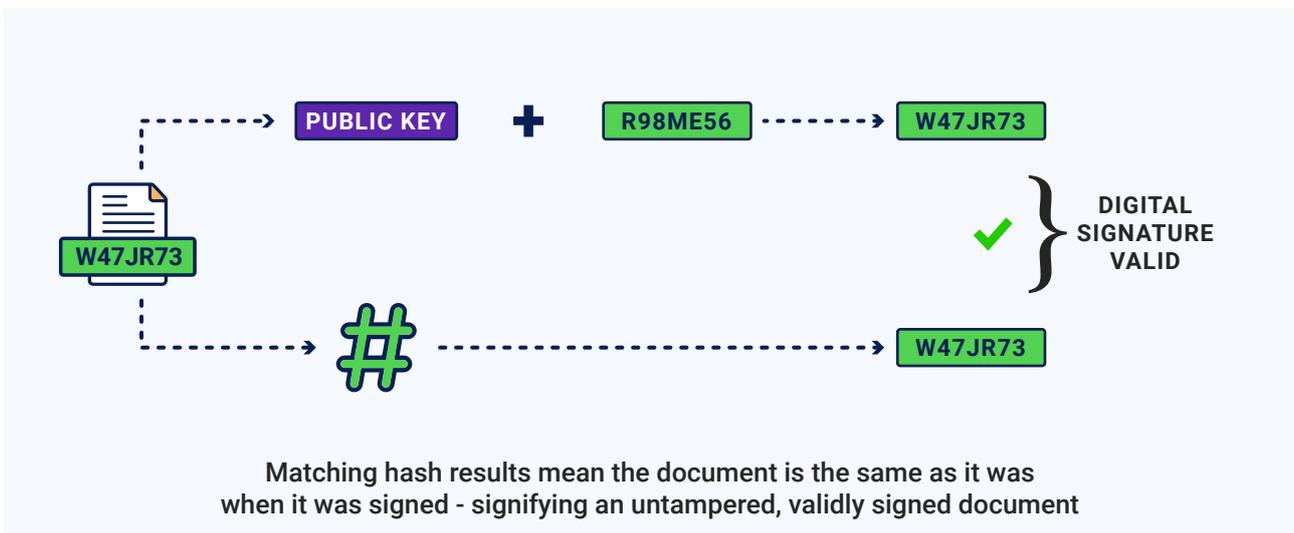


### Step 7: Comparison

The hash result generated in Step 6 (by the hashing function) and the hash result generated in step 7 (by the public key decryption) are **compared**.

If they both **match** then it means that the document opened by the bank representative is the same document that was digitally signed by Waqim. The digital signature is considered **valid**.

If they **don't match** then it means that the document opened by the bank representative was **tampered or changed** after it was sent by Waqim and is not the same document he signed. The digital signature is considered **invalid**.



## HOW WELL DOES THE DIGITAL SIGNATURE PROCESS MEET THE END GOALS OF THE SIGNING PROCESS

We mentioned that the *digital signature* process performs *better* than the wet-ink process in ensuring *Authentication, Integrity and Non Repudiation*. Here's how:

GOAL	DIGITAL SIGNATURES	WET-INK SIGNATURES
<p><b>Authentication:</b> The identity of the parties signing the document is clear</p>	<p style="text-align: center;">✔</p> <p>Waqim's identification details are baked <i>into the digital signature</i> certificate that is digitally signed by the Certifying Authority - and is visible on a digitally signed document.</p> <p>This is essentially the Certifying Authority - a neutral entity - telling the world at large - "<i>Hey this is Waqim's digital signature, take my word for it</i>"</p>	<p style="text-align: center;">?</p> <p>The signature pattern of a person is often said to be unique to a person.</p> <p>However there is no <b>technical</b> barrier or <b>neutral authority</b> that prevents forgery. Because of this, signature experts often have to be called in during Court proceedings - and their opinion is often inconclusive.</p>
<p><b>Integrity:</b> The document cannot be changed unilaterally after the signatures are affixed</p>	<p style="text-align: center;">✔</p> <p>The public key decryption + hash matching process ensures that anyone opening the document on a PDF reader is intimated about whether the document has been <b>altered</b> or not since it was signed.</p> <p>It is computationally impossible to <i>change</i> a hashing function to derive the same hash result for a tampered document. So the hash matching system is virtually foolproof in detecting tampering.</p>	<p style="text-align: center;">✘</p> <p>Anything can be added to a document after it has been physically signed by all parties. Even for printed documents - you can take a pen and make subsequent markings.</p> <p>There is no <b>technical way</b> to track whether a subsequent change was made <b>before</b> or <b>after</b> a wet-ink signature was affixed</p>
<p><b>Non-repudiation:</b> The parties cannot "deny" their acceptance of the terms and conditions of a document at a later stage</p>	<p style="text-align: center;">✔</p> <p>The hashing function and asymmetric crypto system can only be activated by a unique PIN or code that has been handed over <b>ONLY</b> to the signer.</p> <p>For the signer to deny the digital signature - they would need to <b>prove</b> that someone else got access to this PIN or code. This is <b>extremely unlikely</b>.</p>	<p style="text-align: center;">✘</p> <p>Parties can contest their signatures in 2 ways.</p> <p><b>A)</b> By stating that the signature was forged</p> <p><b>B)</b> By stating that the document has been altered/tampered since they signed it. This is very common in retail document journeys - where customers are often made to sign "blank forms"</p>

## WHY TRADITIONAL MODES OF DIGITAL SIGNATURES ARE UNVIABLE AT SCALE

Uptil now we've learnt how *digital signatures* work and why this is **better** than wet-ink signatures in performing the functions of a signature.

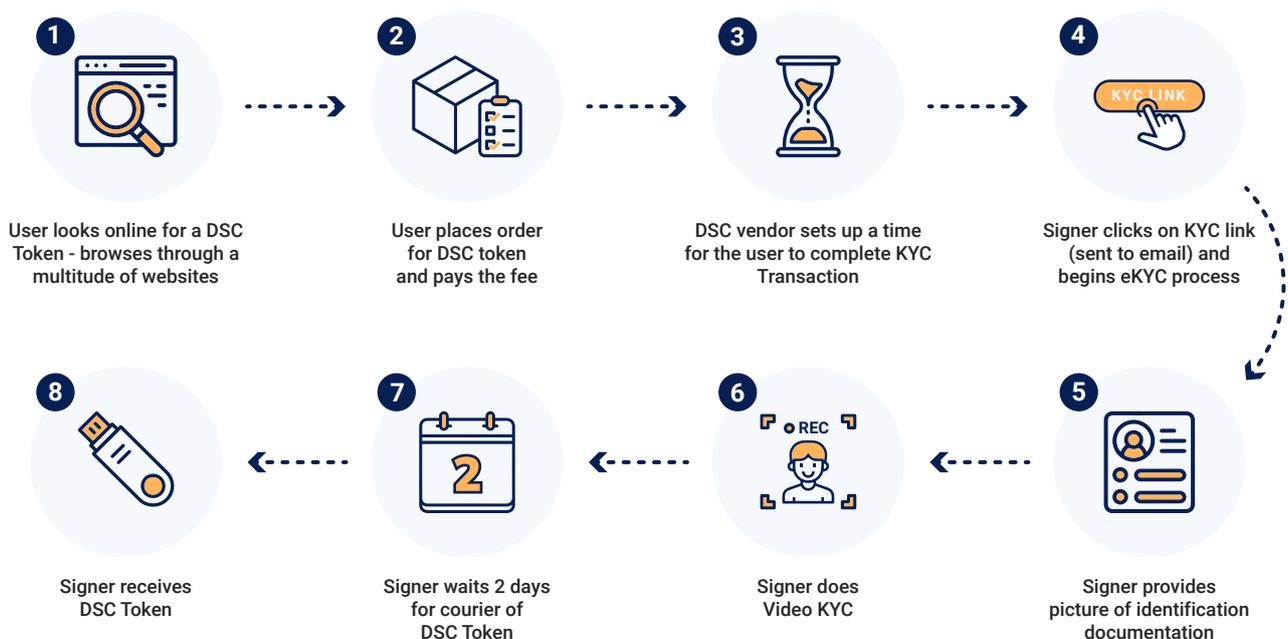
Traditionally, digital signatures in India have only been possible through a USB device known as a "DSC Token".

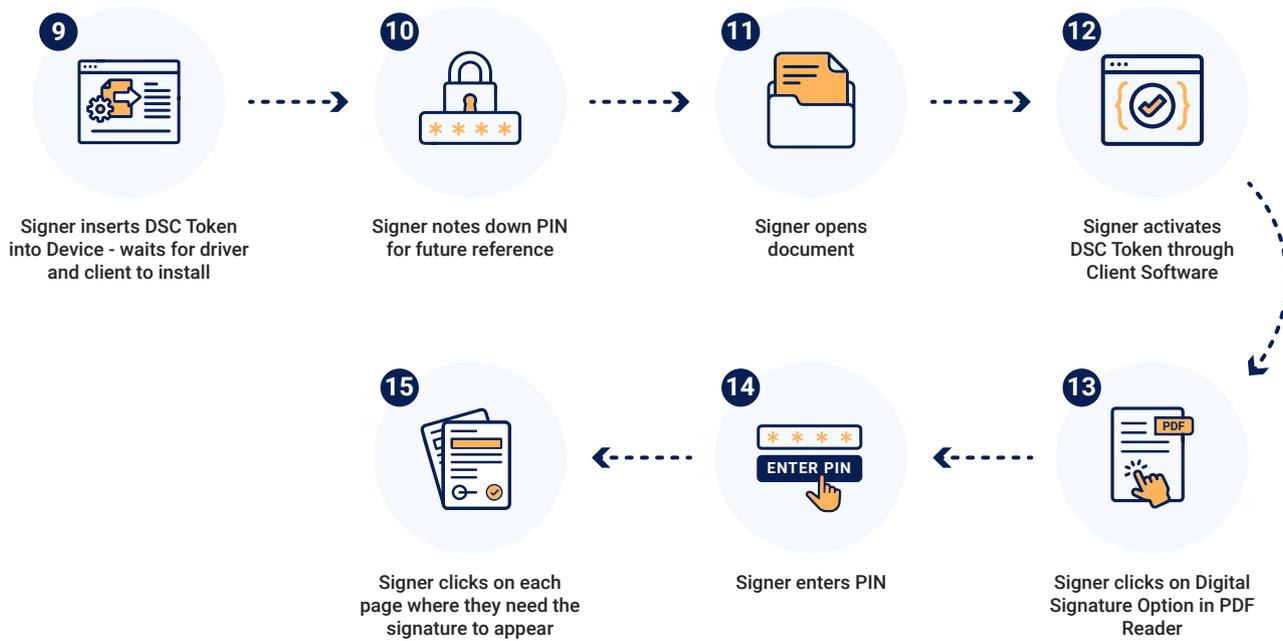
As we mentioned in the previous section, the "DSC Token" acts as a *Hardware Security Module* - i.e provides the computational power to perform the hashing and asymmetric crypto functions. The DSC Token also acts as a **container** for the *digital signature* certificate issued by the Certifying Authority.

In this traditional mode - the signer *has to possess* the *Hardware Security Module*.

But the signer possessing the hardware token is a major problem - they need to *procure it* and they need to *operate it*.

Procuring and Operating is a complex multi-step process that looks like this:





**THIS THROWS UP 4 MAJOR PROBLEMS:**

**(A) Hard to procure:** Procuring a DSC Token involves **payment** of at least INR 1000 PLUS a multi-touchpoint process that takes time. And even after completing this - the signer has to wait a few days to receive the actual hardware. A signer will need to repeat this process **every year**.

**(B) Signing with a DSC Token is hard:** Procurement is only half the battle. Each time a signer needs to sign with a DSC token - they need to undergo a multi-step process involving operation of a “client software” and inputting a PIN that they need to specifically remember for this purpose. This process is prone to be error-ridden - DSC tokens are notorious for malfunctioning without warning.

**(C) Signers need to have the device with them if they want to sign:** If a signer doesn’t have a DSC Token with them **physically** - then they can’t sign digitally. This drastically impacts the actual *mobility* benefits of digital signing.

**(D) Signers can’t sign on mobile devices:** DSC tokens only work on laptop/desktop devices. In India - most people are online via mobile devices.

The above issues make traditional digital signing *impossible to scale* across the Indian population. So while digital signatures may be better than wet-ink signatures - their traditional mode of affixture will never replace wet-ink signatures.

So what's the solution?

That's where electronic signatures under Schedule 2 come in.

***Why should you care?***



*The concepts we are discussing are not in a vacuum. If electronic signing cannot be scaled for use across India - then the whole subject becomes nothing more than a mere academic discussion.*

# CHAPTER



## SCHEDULE 2 ELECTRONIC SIGNATURES

### PART 1

#### Legal and Technical Framework

In the last chapter we concluded that while digital signature *technology* was far superior to wet-ink signing - its *usability* in the traditional form was not.

*Electronic signatures under Schedule 2* are an attempt to leverage digital signature technology and make it *actually usable*.

In this section we'll be discussing the second type of electronic signature in India - *electronic signatures under Schedule 2*.

## SECTION 3A OF THE IT ACT AND THE LEGAL FOUNDATIONS OF ELECTRONIC SIGNATURES IN INDIA

Any analysis of electronic signatures in India must start from the very beginning - the legal amendments that birthed them.

For this we need to turn the clock back to 2008.

### 2008 AMENDMENTS: LEGISLATING FLEXIBILITY

The IT Act was amended in 2008 to introduce a *technology neutral* framework for electronically signing documents.

As noted by the Report of the Expert Committee that drafted the first version of the 2008 Amendments to the IT Act:

The Act is being made technology neutral with minimum change in the existing IT Act 2000. This has been made by amendment of Section 4 of the Act to provide for electronic signature with digital signature as one of the types of electronic signature and by enabling the details of other forms of electronic signature to be provided in the Rules to be issued by the Central Government from time to time. This is an **enabling provision** for the Central Government to exercise as and when the technology other than digital signature matures. Then there will be no need to amend the Act and the issue of rules will be sufficient. Consequently, the term digital is changed to electronic in other sections.



This was an effort designed to empower the Central Government to notify new types of electronic signing if need be - in order to keep up with technological advancement.

Essentially, the Central Government could move beyond the “digital signature” technology prescribed under Section 3, if it saw that other forms of technology could lead to equally reliable modes of electronic authentication of documents.

The enabling provision created by the 2008 Amendments was Section 3-A of the IT Act.



*The recommendations of the Expert Committee mention amendments to Section 4 of the IT Act. However, it is important to note that this was a preliminary committee report. What was mentioned as Section 4 in the Expert Committee Report actually became Section 3-A in the final version of the IT Act.*

**3A. Electronic signature.-** (1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electric record by such electronic signature or electronic authentication technique which-

- (a) is considered reliable; and
- (b) may be specified in the Second Schedule.

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-

- (a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;
- (b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
- (c) any alteration to the electronic signature made after affixing such signature is detectable;
- (d) any alteration to the electronic signature made after affixing such signature is detectable; and
- (e) it fulfils such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule:

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.



Section 3-A of the IT Act mandates a ‘technologically neutral’ threshold of “reliability” that must be met for the Central Government to notify a new type of electronic signature under Schedule II.

“Reliability” in the IT Act consists of 5 conditions mentioned in Clauses (a) to (e) of Sub-section 2.

**SCHEDULE II INSERTIONS ARE INITIATED BY THE CENTRAL GOVERNMENT AND NOT BY PARLIAMENT**

Section 3A(4) and (5) also give more flexibility in notifying new forms of electronic signing.

Any insertion to Schedule II DOES NOT need to be originated by an Act of Parliament. Instead the Central Government needs to simply notify an addition or omission to the Second Schedule and lay this notification before Parliament.

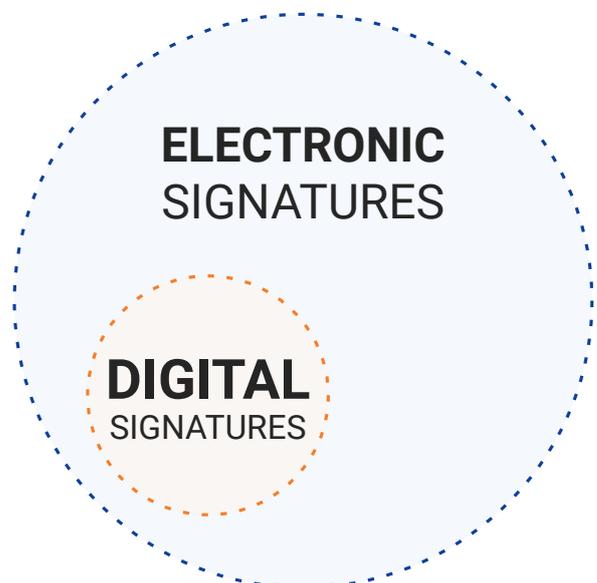
While this seems like a small change - it actually saves a lot of time.

For starters, identification of new technology can be done by Government ministries focussed on technology like the Ministry of IT rather than via Parliament - which has multiple other things consuming its time.

Second, the actual drafting of the notification and prescription of technology does not need to consume Parliamentary time.

**CHANGING DIGITAL SIGNATURE TO ELECTRONIC SIGNATURE**

Another crucial change made by the 2008 Amendments was to subsume the concept of ‘digital signature’ itself WITHIN a broader concept of “electronic signature.”



The foundation of this change was the insertion of Section 2(ta) in the IT Act.

(ta) “**electronic signature**” means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature



Through this change, anyone using any of the old digital signature methods to authenticate an electronic record, would in fact be “*affixing an electronic signature*” and would be marking the document with an “*electronic signature*”.

The amendments also replaced the word “digital signature” wherever mentioned in the IT Act (*and Evidence Act! We will deal with this in subsequent chapters*) with “electronic signature” - to enable a seamless continuity of the IT Act for the new modes of electronic signing prescribed under Schedule II.

So for instance, “Digital Signature Certificate” was replaced with “Electronic Signature Certificate”:

**35. Certifying authority to issue Electronic Signature Certificate.-** (1) Any person may make an application to the Certifying Authority for the issue of an Electronic Signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority: Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Electronic Signature Certificate or for reasons to be recorded in writing reject the application:

Provided that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.



“Affixing digital signature” was replaced with “Affixing electronic signature”

(d) “**affixing electronic signature**”, with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of electronic signature;



There are several other examples of this. But we won't list them all out here because that will make the chapter too long and pointless.

### **Missed drafting:**

*It would be remiss of us to ignore the misses in making these replacements. In many cases, the legislature simply ‘forgot’ to replace digital signature with electronic signature. The most egregious examples of this are in Sections 36 and 37.*

*So while Section 35 stipulates that a Certifying Authority can issue an Electronic Signature Certificate, Section 36 prescribes conditions for issuance of a Digital Signature Certificate and Section 37 prescribes the procedure for revocation of Digital Signature Certificate.*

*This is clearly missed drafting. If the provisions were to be read in good faith, it would mean that CAs can issue Electronic Signature Certificates but can ONLY revoke Digital Signature Certificates. This is an absurdity clearly not intended by the 2008 amendments.*



*This missed drafting is reflected elsewhere as well. We hope Parliament finds time to rectify this glaring, but avoidable error!*

# CHAPTER



## SCHEDULE 2 ELECTRONIC SIGNATURES

### PART 2

#### Schedule 2 of the IT Act and the Regulatory Framework for Electronic Signatures

In Part 1 of this chapter we looked at the 2008 amendments to the IT Act which introduced the concept of electronic signatures.

In Part 2 we will look at the regulatory framework behind the different types of electronic signatures listed under the Second Schedule of the IT Act.

Similar to the digital signature technology mentioned in Section 3 of the IT Act, the electronic signatures specified under the Second Schedule to the IT Act also rely on a combination of asymmetric crypto system and hash functions.

However, Schedule 2 Electronic Signatures differ from Section 3 Digital Signatures in one critical manner - the way in which signer identity is authenticated.

For digital signatures we looked at how the **identity of the signer is finally tied to the digital signature**. In that process, the signer undergoes a multi-step KYC process with the Certifying Authority. Upon successful KYC – the Certifying Authority issues a digital signature certificate “token” to the signer. A token consists of a secure key pair belonging exclusively to the signer – and can be used by that signer to affix a Certifying Authority validated “digital signature certificate” on a document

Authentication of an electronic record by e-authentication Technique which shall be done by-

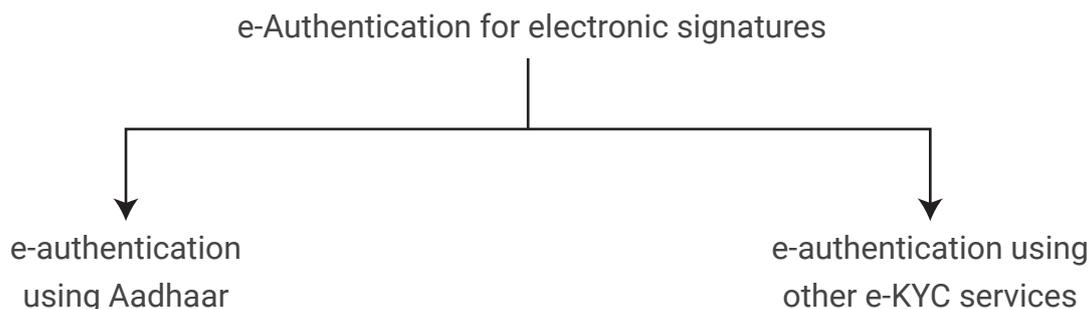
(a) the applicable use of e-authentication, hash, and asymmetric crypto system techniques, leading to issuance of Digital Signature Certificate by Certifying Authority

**Second Schedule of the IT Act**



For electronic signatures under Schedule II of the IT Act, the identity of the signer is established by a process known as “e-authentication”. This e-authentication either happens on the fly (i.e., at the time the signer is affixing the eSign), or on the basis of a one-time online KYC.

Under Schedule II there are **two types** of recognized e-authentication modes for electronic signatures:



Based on this classification, we can divide the electronic signatures recognised under the Second Schedule of the IT Act into two categories:

- 1) Aadhaar based electronic signatures (commonly known as “Aadhaar eSign”)
- 2) Non-Aadhaar based electronic signatures.

e-Authentication makes it **easier to obtain** and **easier to sign** with an electronic signature certificate in comparison to a conventional DSC Token. Let’s examine how.

## AADHAAR BASED ELECTRONIC SIGNATURES (AADHAAR eSIGN)

Aadhaar eSign was given legal sanctity through its inclusion in the second schedule of the IT Act via [Gazette Notification No. 2015 Jan – GSR 61\(E\) \(the Aadhaar eSign Notification\)](#), dated January 27, 2015, entitled “Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015”.

The policy imperative that drove Aadhaar eSign was quite simple – *to enable a mode of electronic signature that could be used scalably by 1 billion + individuals on a regular basis.*



Before Aadhaar eSign, the only acceptable form of “electronic signature” was the DSC Token (which we spoke about in our last chapter). However - as we learnt in the previous chapter - the DSC token system relied upon a laborious purchase, KYC, delivery and usage process. It was impossible to drive mass usage with such a system.

Aadhaar eSign, on the other hand, was super-easy – and far easier to drive mass usage in a 1b+ country like India.

**For Aadhaar eSign, all signers needed was:**

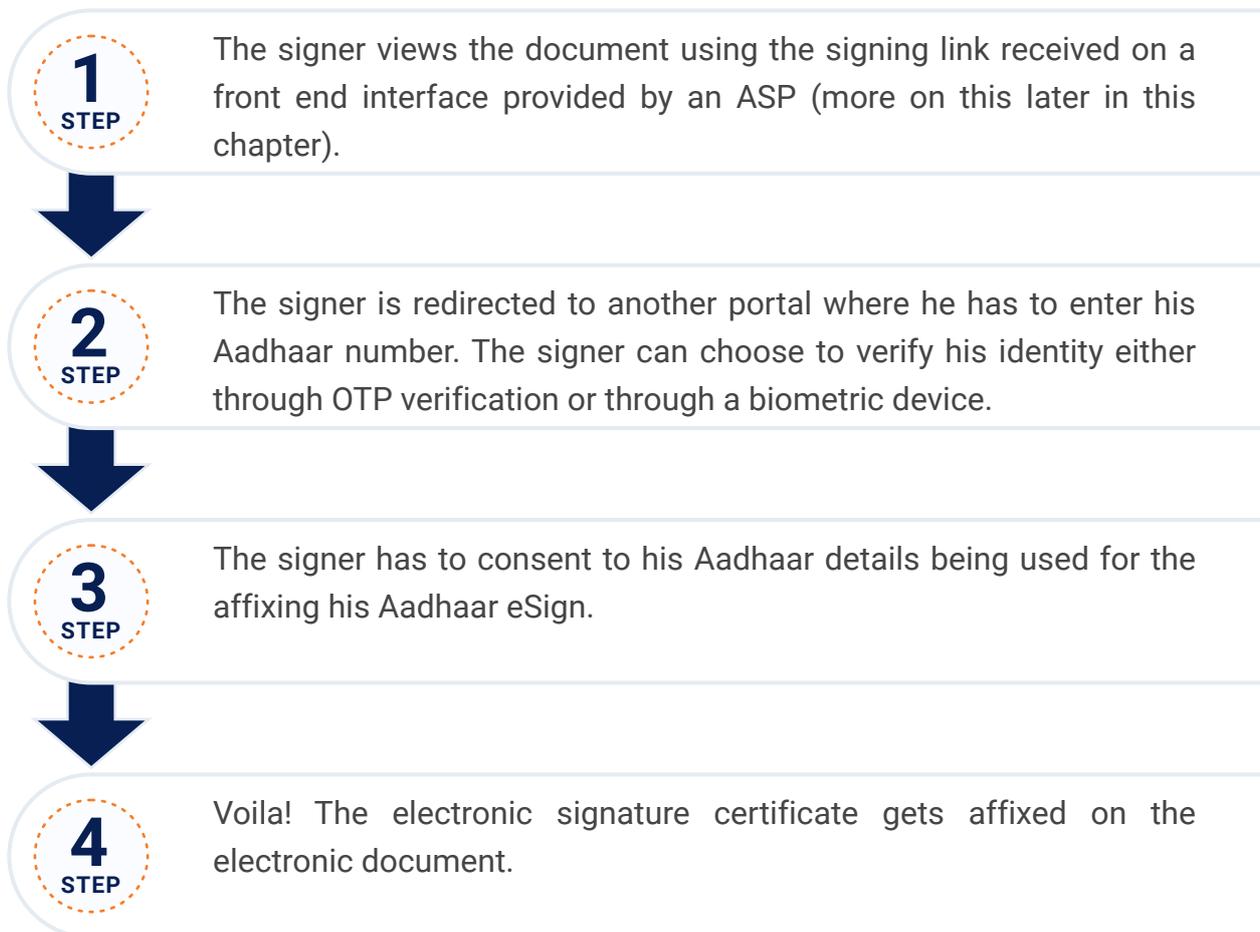
- 1) A valid Aadhaar number
- 2) Linkage between Aadhaar number and phone/email or biometrics
- 3) Access to their registered phone/email ID or to a biometrics device

**And the actual process of signing? Even easier:**

Opening and viewing the document

Giving Consent to Aadhaar eSign

Authenticating Aadhaar with an OTP or Biometrics



For the signer, the entire process is simple and takes about a **minute** (*you can try it out for yourself [here](#)*).

But in the backend - a LOT happens in that **one minute** - eAuthentication, hashing function, asymmetric crypto function - all done through an intricate coordination between multiple parties under a comprehensive regulatory framework.

Let's deep dive into this eventful **one minute**.

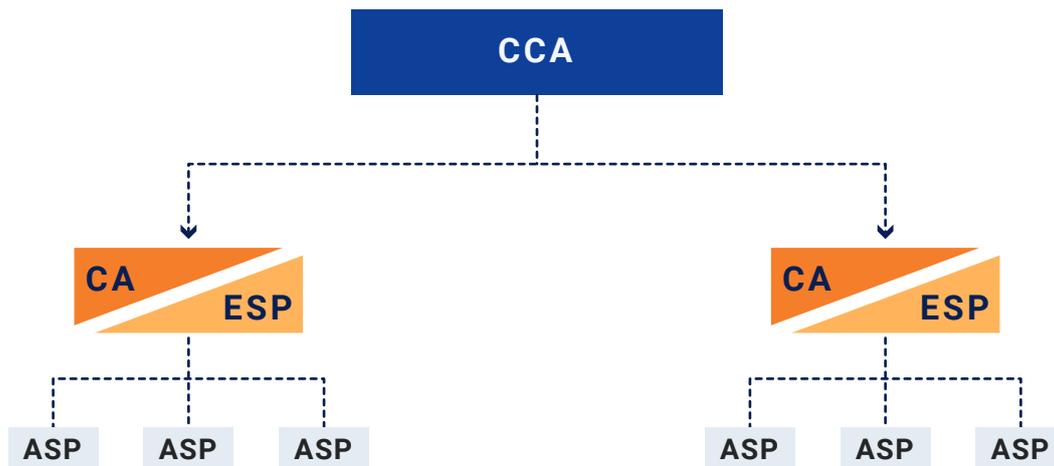
# WHAT HAPPENS IN THE MINUTE IT TAKES TO DO AN AADHAAR eSIGN

## CHARACTERS

First, it's important to understand the characters involved in this **one minute** that it takes for an Aadhaar eSign.

### Regulator

1) **Controller of Certifying Authorities (CCA)** – the CCA is the big boss of the eSign ecosystem in India. It is the apex regulator setup by the Ministry of Information Technology – under S. 17 of the Information Technology Act. The CCA is tasked with regulating and governing the activities of Certifying Authorities. It is also the body that came up with the **e-Authentication Guidelines** first in May 2019.



The CCA regulates all entities in the eSign ecosystem in India - from the CA/ESPs to the ASPs

### Identifier

2) **Unique Identification Authority of India (UIDAI)** – The organization that set up the Aadhaar system. Nothing involving Aadhaar e-Authentication can happen without UIDAI involved.



## Intermediaries

**3) Certifying Authority (CA)** – a regulated entity authorized by the CCA to issue “electronic signature certificates” in India. Aadhaar eSign is a process of generating and affixing an electronic signature certificate. So it can’t happen without involvement of a CA.

For Online Aadhaar eSign, NSDL and CDAC are the 2 most popular CAs that issue certificates.



**4) eSign Service Provider (ESP)** – The entity at the centre of it all. The ESP coordinates with the CA, the UIDAI, the Signer and the ASP (we’ll come to this next) to ensure that a successful electronic authentication is converted into an electronic signature. The ESP essentially performs the same functions as the USB Token device does in a conventional digital signature process. Under India’s regulatory framework – an ESP must be owned and operated by a CA.

So for Online Aadhaar eSign - the 2 most popular ESPs are NSDL and CDAC.

**5) Application Service Provider (ASP)** – The entity responsible for taking Aadhaar eSign to the masses. An ASP provides a front-end layer where a signer can view a document and decide to Aadhaar eSign it. The ASP is also in charge of ensuring fairness and equity in the signing process by making sure the signed copy of the document is accessible by ALL parties involved in the transaction.

## Transacting Parties

**6) End User of the ASP** – The end user is usually a company or individual who uses an ASP to digitally execute its documents with customers, vendors, partners, investors etc. The most common “end users” of Aadhaar eSign so far have been companies in the BFSI sector. But other companies have also begun to use Aadhaar eSign. **Note:** The End User CAN also be an ASP.

**7) eSigner** – The most important party in the transaction – you, dear signer. All the entities above work hard to enable you to sign that contract, form or legal document in **less than a minute** from the convenience of your home. But if you didn’t exist – nor would they.

## THE ACT

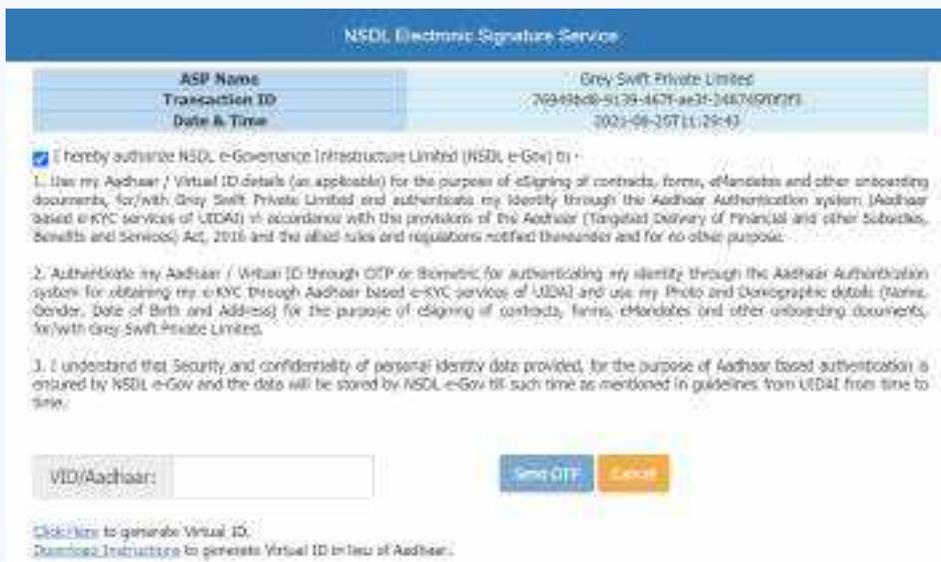
Now for the amazing act of a one-minute electronic signature. How do these characters do it?

### STEP 1

Signers view the document, give consent and click on a signing link – on a front-end interface provided by an ASP. At this stage, the ASP also performs the hashing function on the document to create its hash result (the input document hash).

### STEP 2

After clicking the signing link – signers are redirected to a portal maintained by the ESP.



### STEP 3

The above portal is where the magic of e-authentication happens. The Signer enters their Aadhaar number. The ESP asks UIDAI to conduct an eKYC with the Signer. UIDAI sends an OTP to the Signer’s linked mobile or email. The Signer enters the OTP on the portal. If the OTP is correct – UIDAI verifies the authentication as **successful**. UIDAI relays the success or failure message to the ESP. The e-Authentication process is now complete.

**STEP 4**

Upon successful authentication of the signer’s identity, the ESP creates the Secure Key Pair for the signer. The Private Key of the signer is stored and secured in a Hardware Security Module maintained by the ESP. The private key is destroyed after 30 minutes to prevent misuse.

**STEP 5**

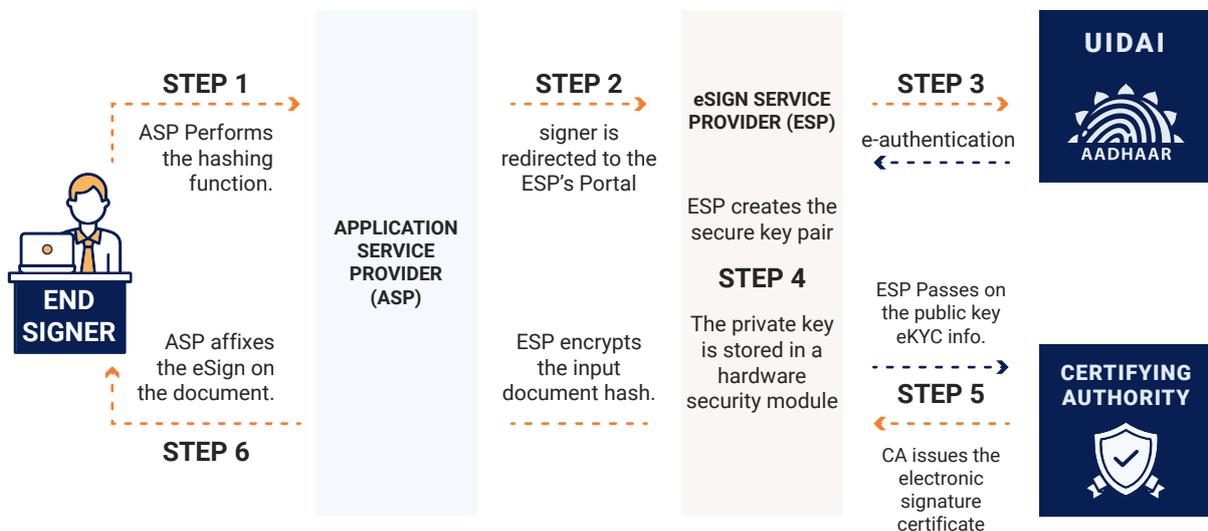
After the key pair generation, the ESP sends the public key and the eKYC information (which it received from UIDAI) to the Certifying Authority in the format prescribed by the CCA under the [eSign API specifications](#). Upon receiving these particulars, the CA issues the Electronic Signature Certificate for the Signer and passes it onto the ESP.

**STEP 6**

The ESP encrypts the input document hash (passed on by the ASP in Step 1) using the private key to create a scrambled hash result. The ESP then passes the Electronic Signature Certificate and the scrambled hash result to the ASP, which then facilitates affixture of the eSign on to the document.

And we’re done. An Aadhaar eSign has now successfully happened. And yes – the process DOES take only a minute (or less).

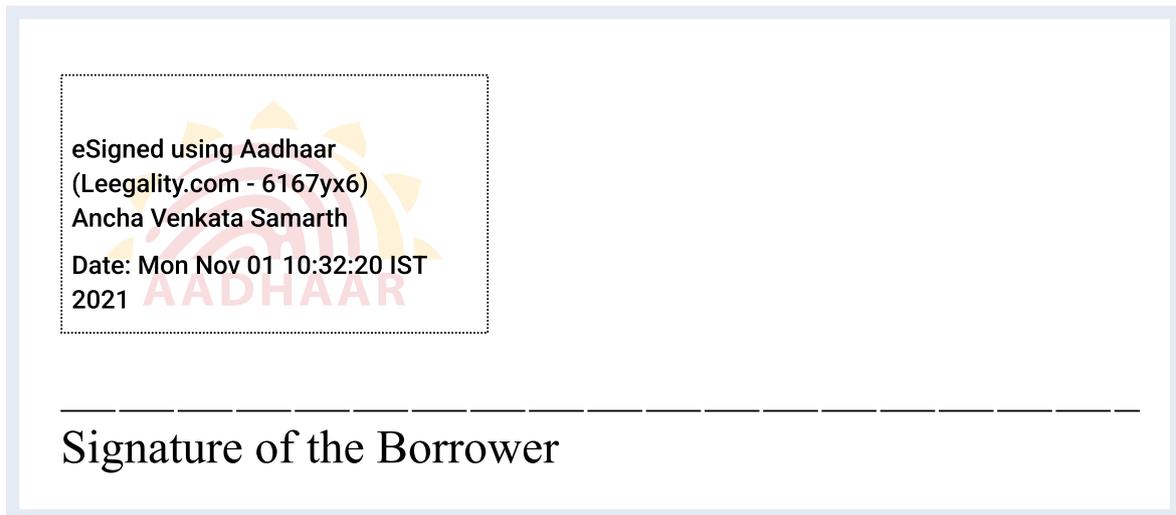
Don't believe that? Try it out for yourself now!



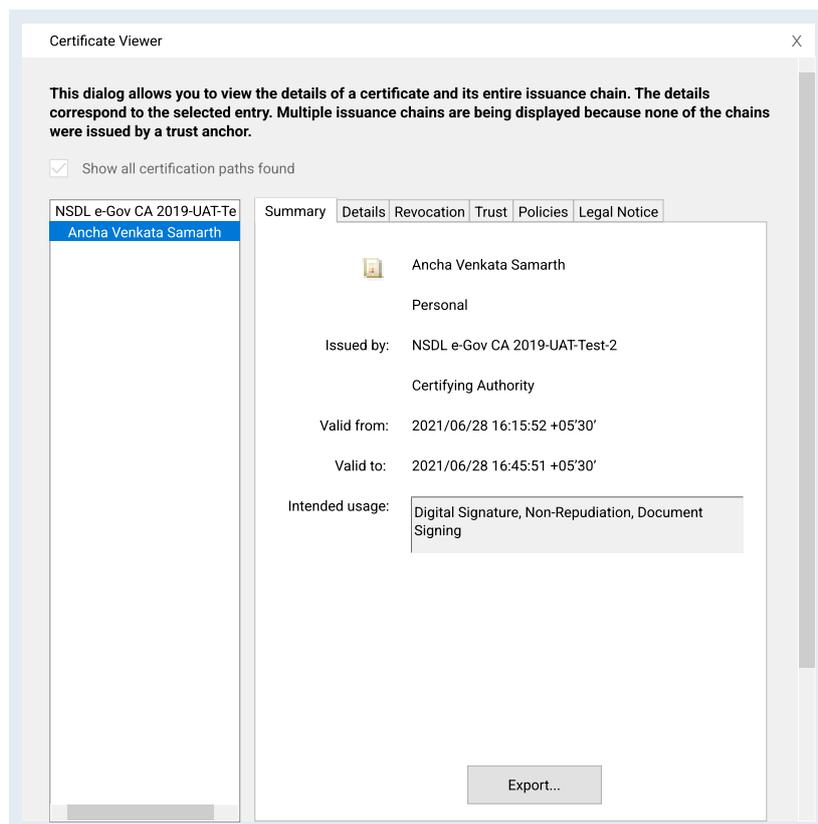
A visual representation of the process described above

## HOW DOES THE AADHAAR eSIGN LOOK ON THE FINAL DOCUMENT?

Visually, Aadhaar eSign appears as a “text with timestamp” on your signed documents – similar to a digital signature using a DSC Token



Since its an electronic signature certificate – you can also access the certificate details from the backend of the PDF:

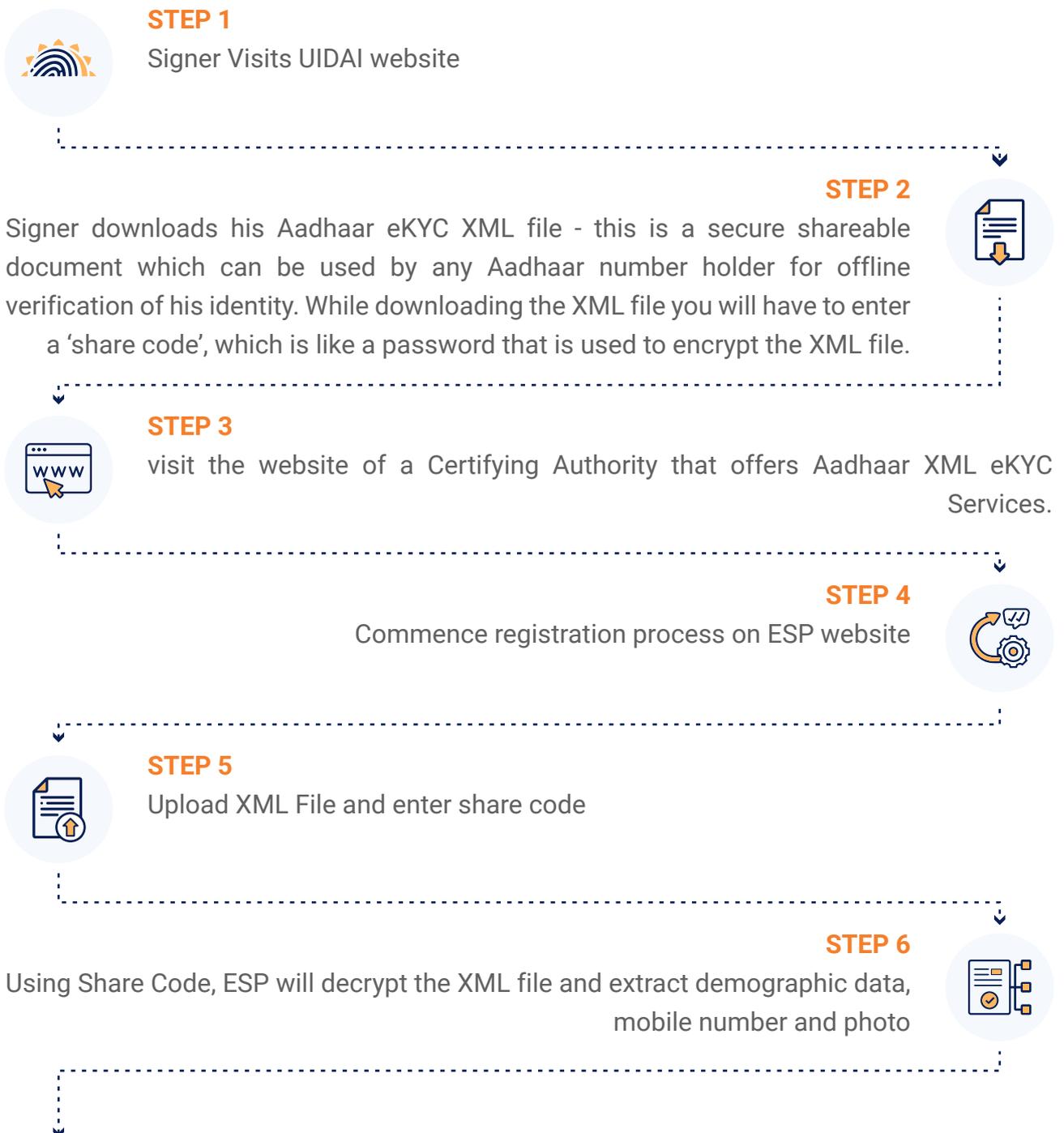


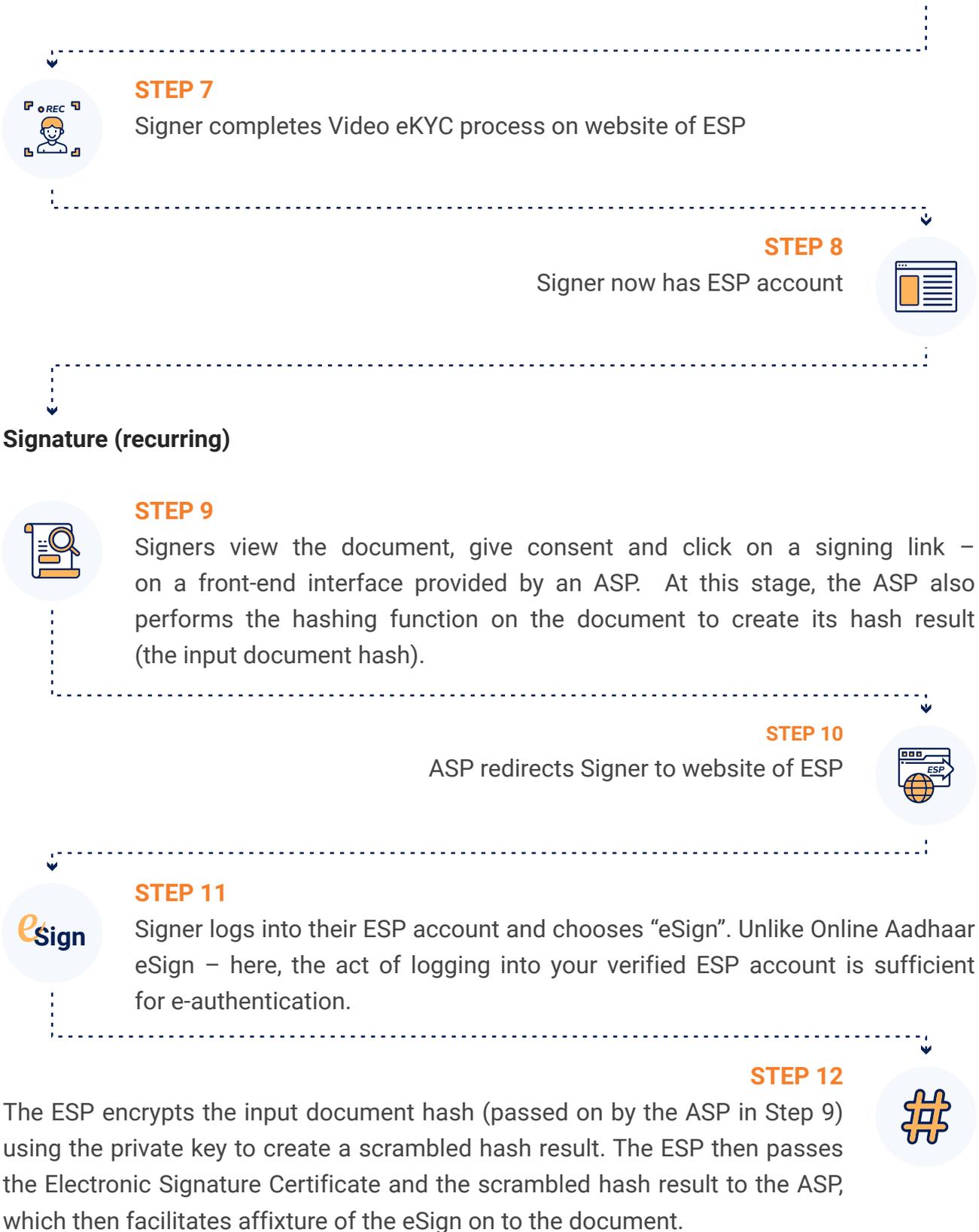
## THE “OTHER” TYPE OF AADHAAR eSIGN

What we have discussed so far is “Online Aadhaar eSign” - the most popular way to eSign a document with Aadhaar.

However there is another, less popular type of Aadhaar eSign – Aadhaar XML eSign. Let’s see how **Aadhaar XML eSign** works.

### Procurement (1 Time process)





The Aadhaar XML eSign process is slightly more complex than the Online Aadhaar eSign process:

- It requires a multi-step procurement process
- Requires remembering an account ID and password

However it is still much easier than a typical DSC Token Process:

- It doesn't require "purchase" of a physical device
- Signing steps are much easier once you have created the ESP account
- It can be used across all devices – mobile or desktop
- It doesn't require a physical device

In that sense, Aadhaar XML eSign is the middle ground between Online Aadhaar eSign and DSC Token eSign.

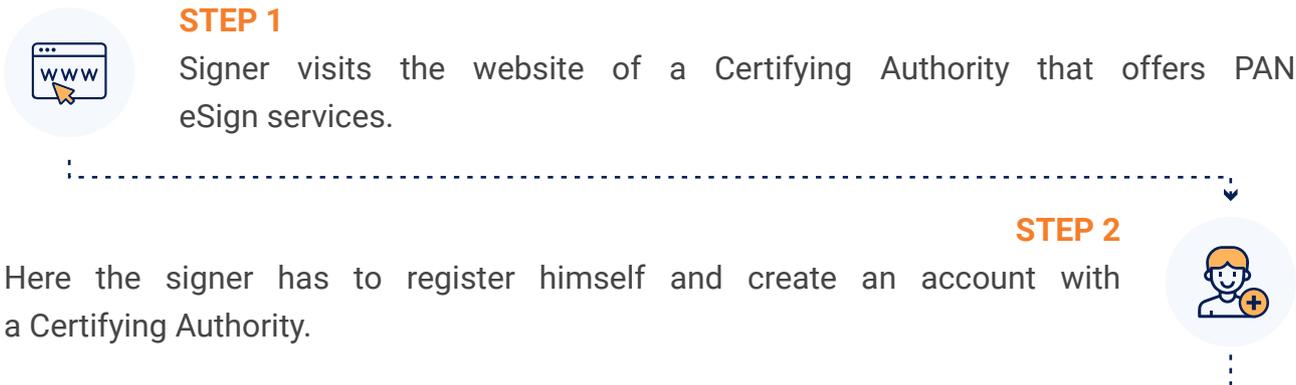
## NON-AADHAAR BASED ELECTRONIC SIGNATURES

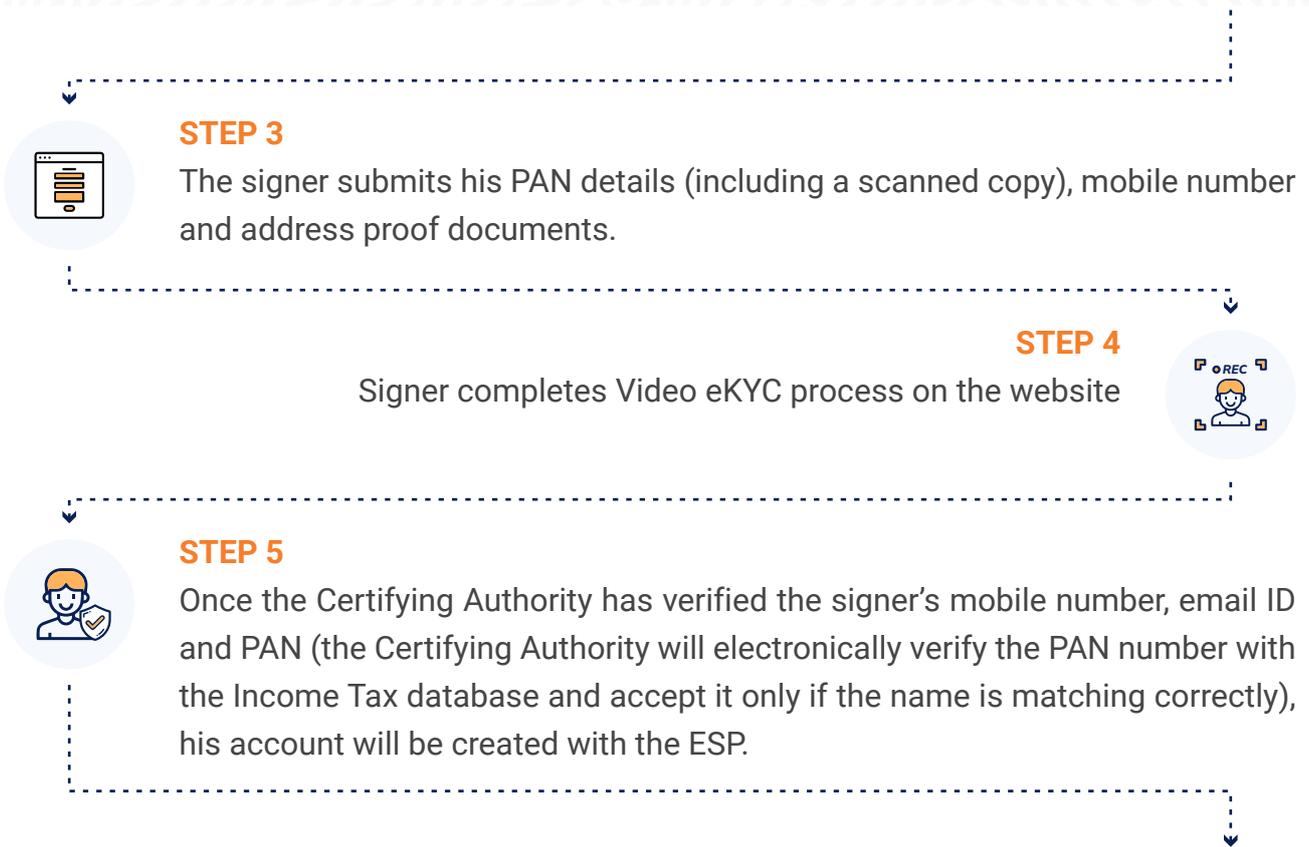
The Second Schedule of the IT Act also recognises e-authentication using "other e-KYC services" (remember?). The scope of the Second Schedule was expanded beyond just Aadhaar based authentication vide Gazette Notification S.O. 1119(E), dated March 1, 2019. The phrase "e-authentication technique using Aadhaar e-KYC services" was substituted with "e-authentication technique using Aadhaar or other e-KYC services".

So what are these other e-KYC services that enable you to eSign a document?

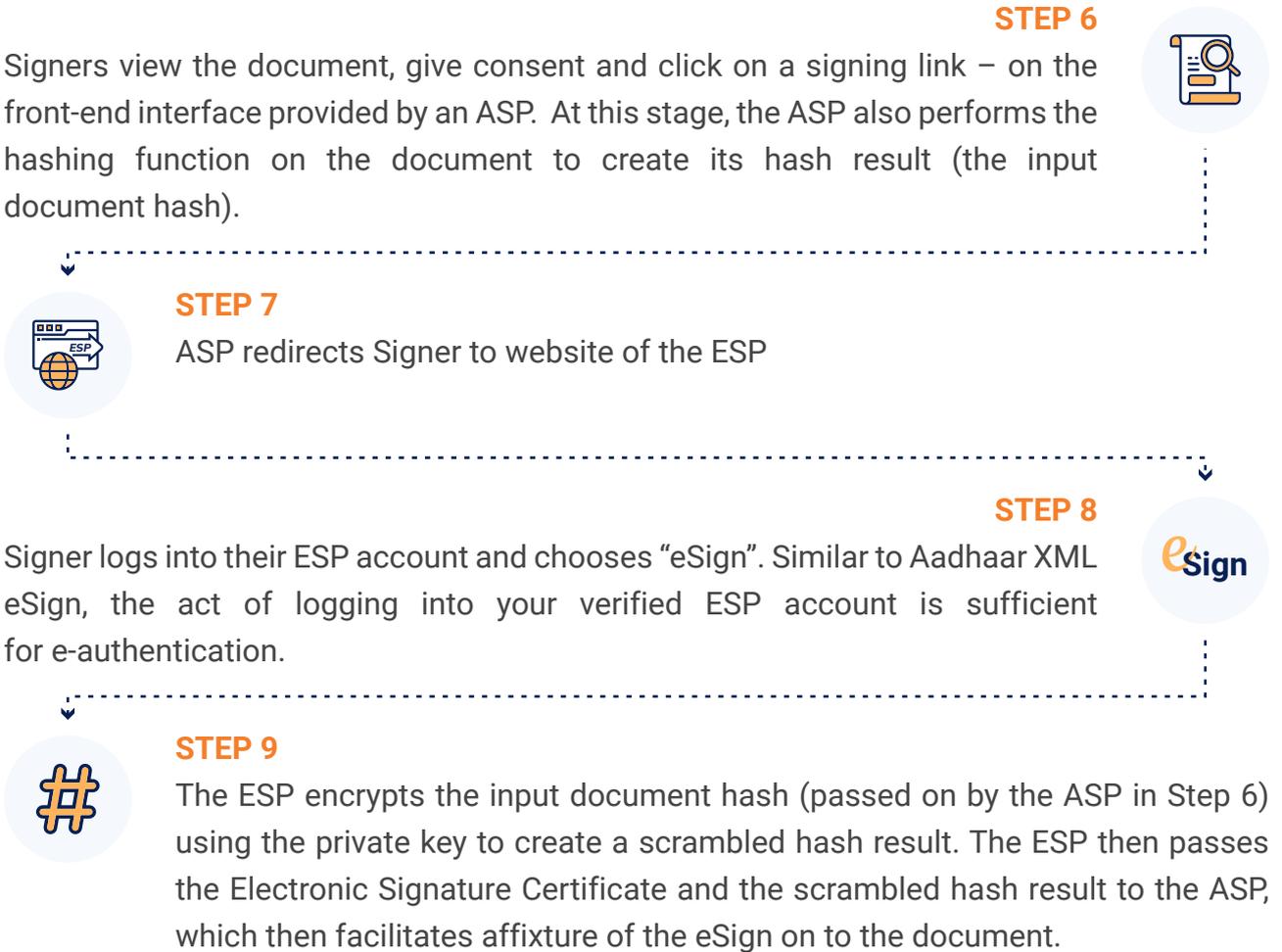
A PAN eSign flow is very similar to an Aadhaar XML eSign flow.

### Procurement (1 Time process)





**Signature (recurring)**



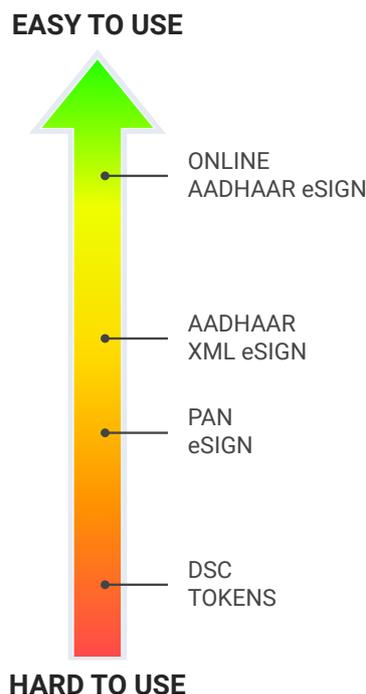
## HOW DO ELECTRONIC SIGNATURES COMPARE AGAINST DIGITAL SIGNATURES?

A document signed using any of these electronic signatures can be easily verified to ensure its integrity, i.e., to make sure the document has not been tampered with after affixture of the eSign.

The underlying technology to ensure this is a combination of asymmetric crypto system and hash functions, similar to the digital technology process we learnt earlier.

Both PAN eSign and Aadhaar XML eSign are easier to operationalize than a DSC Token flow. However, they are still significantly harder to use than a simple Online Aadhaar eSign.

A hierarchy of these various electronic signature options – based on ease of use – would probably look like this:



Currently, Aadhaar Online eSign looks like the best bet for mass usage of electronic signatures on a population level scale.

But are electronic signatures the **ONLY** way to execute documents electronically?

Not quite.

That's what we'll be covering in the next chapter.

# CHAPTER



# OTHER MODES OF ELECTRONIC EXECUTION

“Electronic signatures” – as defined under Section 3 and Section 3A of the Information Technology Act are NOT the only way to execute electronic records.

The IT Act and the Contract Act both allow for another way – or rather ways – to execute documents digitally.

To understand this, we need to first take a brief segue into the Indian Contract Act.

## EXECUTING A CONTRACT DOESN'T REQUIRE A SIGNATURE

One of the biggest myths in modern commercial circles is the idea that contracts require signatures.

This isn't true.

Section 10 of the Indian Contract Act, 1872 (Contract Act) defines a contract:

**10. What agreements are contracts.-** All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void.

Section 10 lists the 5 main ingredients of a lawful contract



Therefore, an agreement becomes a contract if:

- (1) It is made by the free consent of parties;
- (2) The parties are competent to contract under law;
- (3) There is a lawful consideration;
- (4) There is a lawful object; and
- (5) It is not expressly declared to be void.

The word “signature” is not a necessary element of a contract.

But hold on, you say, surely “free consent” i.e condition (1) CAN ONLY be given by way of a signature?

Let's break down condition (1).

Section 14 of the Contract Act lays down the meaning of "free consent":

**14. "Free consent" defined.-** Consent is said to be free when it is not caused by-

- (1) coercion, as defined in section 15, or
- (2) undue influence, as defined in section 16, or
- (3) fraud, as defined in section 17, or
- (4) misrepresentation, as defined in section 18, or
- (5) mistake, subject to the provisions of section 20, 21 and 22.

Consent is said to be so caused when it would not have been given but for the existence of such coercion, undue influence, fraud, misrepresentation or mistake

**"Free consent" under the Contract Act**



Now we know when consent can be said to be "free". But what exactly is "consent" under contract law?

Section 13 of the Contract Act defines what constitutes "consent":

**13. "Consent" defined.-** Two or more persons are said to consent when they agree upon the same thing in the same sense.



Section 13 is the codification of *consensus ad idem* – the legal principle that forms the bedrock of contract law the world over. This principle requires that there should be a "meeting of the minds", i.e., all parties to the contract should agree upon the same thing in the same sense.

So the next question that naturally arises is, if the parties are entering into an agreement by their free consent, and they agree to the terms of the contract in the same sense, **then how can they convey such consent?**



## COMMUNICATING CONSENT

The process for conveying consent to enter into a contract is laid down in Section 3 of the Contract Act:

**3. Communication, acceptance and revocation of proposals.-** The communication of proposals, the acceptance of proposals, and the revocation of proposals and acceptances, respectively, are deemed to be made by an act or omission of the party proposing, accepting or revoking by which he intends to communicate such proposal, acceptance or revocation, or which has the effect of communicating it.



As per Section 3, parties to a contract can agree on **any manner of acceptance** - oral, by letter, by email or even whatsapp.

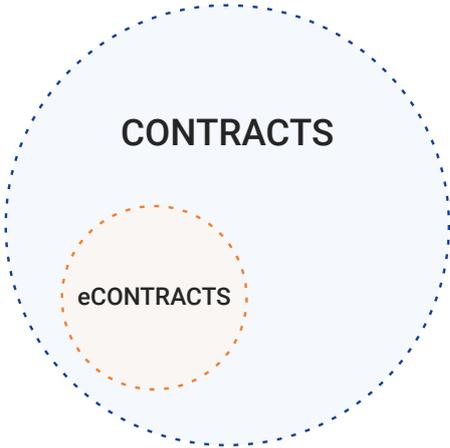
The contract act does not restrict the modes of acceptance for a contract. Here a signature is merely an *option* and not a *mandate*.

That's why agreements entered into orally are perfectly valid under law as long as parties have given consent in a way that meets the 3 conditions laid down in Section 3. With oral contracts this usually happens through a simple handshake.

But since it can be difficult to prove such oral agreements later on in Courts, commercial contracts are mostly (if not always!) entered into by writing down the terms of the contract – either on paper, or in digital form (eContracts).

But what does the Contract Act have to say about eContracts specifically?

Nothing much. Actually, nothing at all. eContracts differ from physical contracts **only in format** and not in legal character - i.e they are found in electronic form. In legal terms, the Contract Act does not make a distinction between physical contracts and eContracts.



## HOW eCONTRACTS CAN BE EXECUTED UNDER INDIAN LAW

The Information Technology Act, 2000, which is the primary legislation in India dealing with electronic commerce, is based on the [UNCITRAL Model Law on Electronic Commerce 1996](#).

Noting the increasing number of transactions in international trade being carried out through eContracts, the UNCITRAL Model Law sought to bring about “progressive harmonization and unification of the law” across countries in matters relating to e-commerce.

Article 11 of the UNCITRAL Model Law, which relates to the conclusion of contracts by electronic means, reads as follows:

*“Formation and validity of contracts –*

*In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.”*

The remarks to Article 11 state that:

*“the provision is needed in view of the remaining uncertainties in a considerable number of countries as to whether contracts can validly be concluded by electronic means.”*

With the growing dependence on electronic means to reach commercial agreements and to give effect to Article 11 of the UNCITRAL Model Law, the Parliament introduced **Section 10A** to the IT Act via an amendment in 2008, **explicitly recognizing eContracts under Indian law.**

**10A. Validity of contracts formed through electronic means.-** Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic records, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

**Section 10A of the IT Act, 2000**



So what does Section 10A do?

If you look closely, Section 10A is more or less the first part of Section 3 of the Contract Act stitched together with the second part of Article 11 of the UNCITRAL Model Law. Section 10A simply **clarifies** that the applicability of Section 3 of the Contract Act applies to electronic execution as well. The **wide latitude to choose the method of conveying consent under Section 3, now specifically includes electronic execution** within its ambit.

Section 10A does this by categorically stating that **a contract cannot be denied enforceability just because it was executed electronically.**

Therefore, any electronic means can be used to execute and enter into a contract as long as the three ingredients of Section 3 are met, i.e., there should be an act or omission, which intends to convey the consent of the party, and has the effect of conveying it.

But what do we mean exactly by “electronic means” here? As per Section 10A you can convey your consent to enter into a contract either in “electronic form” or “by means of an electronic record”.

(r) “electronic form” with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(t) “electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche

**Definition of “electronic form” and “electronic record”  
under Section 2 of the IT Act**



As you can see, the definition of “electronic form” and “electronic record” is very wide. It is wide enough to cover all forms of electronic execution.

## COMMON WAYS OF EXECUTING eCONTRACTS IN INDIA

We have now established that contracts can be executed through a very wide range of electronic means. But what are these electronic means that people use to enter into contracts?

One way of course is through **electronic signatures** - which we discussed in the previous chapter.

However, just like how physical signatures are not the only way of communicating consent to enter into a paper contract - electronic signatures are also not the only way of communicating consent to enter into an eContract.

Let us take a look at some other common modes of electronically executing eContracts in India.

### CLICKWRAP

A clickwrap contract is an online contract in which the user signifies their consent to be bound by the terms of the contract by clicking a button – usually a “Yes / No” or an “I agree / I disagree” button.

Such contracts are most often used in cases where the same boilerplate agreement needs to be signed by multiple users. Common examples of such contracts are privacy policies. You may have seen them as part of the installation process of software packages. They are usually a take-it-or-leave-it sort of contract where the person accepting the terms of the agreement lacks bargaining power and has no power to negotiate the terms of the agreement.

The **act** of clicking the “I Agree” button signifies the **intention** of the user to convey their consent, and since the response gets stored electronically with the maker of the agreement, it also has the **effect of communicating** their consent.



## EMAIL EXCHANGE

Imagine I am looking to sell my iPhone. I find a prospective buyer - who tells me they will pay in installments. To record this understanding, we both decide to exchange emails to confirm the transaction. I send her an email with the purchase agreement as an attachment. She wants to change a certain clause - and replies accordingly. After incorporating the revision, I send the final version - and ask her to accept. She replies saying 'This is fine with me. We can proceed.

Do you think that is a legally valid contract?

Yes, it is. Commercial contracts are often entered into through an exchange of emails. During the Covid-19 pandemic especially, with lockdowns making it extremely difficult to obtain physical signatures, some businesses increasingly relied on emails as a method of negotiation of terms and execution of contracts.

The act of sending an email stating “*This is fine with me. I agree to this agreement. We can proceed*” signifies the person’s **intention** to accept and enter into a contract. And since this reply is immediately sent to the other party, his email also has the **effect of communicating his consent** to be bound by the terms of the contract.

The Supreme Court has also in various judgements accepted and reinforced the freedom that parties have to choose any method of electronic execution for entering into eContracts.

In *Trimex International FZE, Dubai v. Vedanta Aluminum Limited*, (2010) 3 SCC 1, the Supreme Court upheld the validity of a contract entered into via an exchange of emails with the binding observation:

“Once the contract is concluded orally or in writing, the mere fact that a formal contract has to be prepared and initialed by the parties would not affect either the acceptance of the contract so entered into or implementation thereof, even if the formal contract has never been initialed.” (Paragraph 9)

In a similar vein, the Supreme Court in the case of *Ambalal Sarabhai Enterprise Limited v. KS Infraspace LLP Limited*, (2020) SCC OnLine 1 the Supreme Court made the following observation while examining the validity of an eContract which was concluded over an exchange of emails and WhatsApp:

*“The Whatsapp messages which are virtual verbal communications are matters of evidence with regard to their meaning...The emails and WhatsApp messages will have to be read and understood cumulatively to decipher whether there was a concluded contract or not”*

While this observation tells us that contracts can be concluded through electronic means such as email, it also highlights the pitfalls associated with relying on emails as a method of electronic execution. The Supreme Court held the contract to be invalid in this case as the nature and language of the correspondences shared between the parties did not directly equate to affirmation. The Court therefore could not draw the conclusion that the contract had been concluded between the two parties.

### VIRTUAL SIGNATURE

Virtual Signatures are electronic representations of your physical wet-ink signature. Service providers across the world let you affix such signatures to electronic agreements.

Users are usually provided an option to either draw their signature electronically or choose from a computer-generated template of their name, which can be placed anywhere on the electronic agreement as per the user’s choice.



The **act** of affixing this digital representation of one's handwritten signature signifies the person's **intention** to enter into and be bound by the terms of the contract. Since this signature gets affixed on to the document, it has the **effect of communicating** the consent to the other parties to the contract.

Virtual Signatures, by default, do not come with the safeguards of asymmetric cryptographic and hashing algorithms that electronic signatures come with. To mitigate this - a new class of Virtual Signatures, known as "Secure Virtual Signatures" has come up. Unlike normal Virtual Signatures, Secure Virtual Signatures come with ADDITIONAL layers of authentication to eliminate disputability.

## WHEN OTHER MODES OF ELECTRONIC EXECUTION CANNOT BE USED

There are 2 cases where you cannot use these "other means of electronic execution" to enter into a contract:

- (1) If the law mandates that a document **MUST** contain a signature. If you want to execute such a document electronically then you would **HAVE** to use an electronic signature as per S. 5 of the IT Act.
- (2) Section 1(4) of the IT Act states that nothing in the Act applies to documents or transactions mentioned in the First Schedule of the Act. Therefore, such other means of electronic execution cannot be used to execute documents that are expressly excluded from the application of the IT Act under the First Schedule. These excluded documents under the First Schedule are:
  - (i) A negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instrument Act, 1881 (26 of 1881).
  - (ii) A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882 (7 of 1882).
  - (iii) A trust as defined in section 3 of the Indian Trust Act, 1882 (2 of 1882).
  - (iv) A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 (39 of 1925), including any other testamentary disposition by whatever name called.
  - (v) Any contract for the sale or conveyance of immovable property or any interest in such property.

**CHAPTER**



**VALIDITY MATRIX**

Till now, we have examined the technical and legal framework behind the common modes of “electronic signing” in India today:

- A) Section 3 Digital Signatures
- B) Schedule II Electronic Signatures
- C) Other Electronic execution types (Virtual Signature, click-wrap, email exchange)

Besides understanding the underlying technology behind them, we also looked at the legal framework that confers upon them legal recognition - as a **valid** mode of execution.

As we discussed in the Introduction to this book - the question of validity is a **yes or no** question. A particular type of signature is either **valid or invalid** for a particular type of document.

To make your life easier - we’ve prepared a **matrix of validity** for easy identification of the various types of electronic signing you can use for a particular document:

### MATRIX OF VALIDITY OF ELECTRONIC SIGNING

Type of Document	Electronic Signatures	Other Electronic Modes of Execution (Virtual Signature, Emails, Clickwrap)
A document which must mandatorily be <b>signed</b> under any law, rule or regulation	✔	✘
Documents listed in Schedule I of the IT Act (e.g., power of attorney, sale deed for immovable property)	✘	✘
Any document that doesn't <b>need to mandatorily be signed</b> and <b>isn't listed in Schedule I of the IT Act</b>	✔	✔

## HOW TO READ THE ABOVE MATRIX

Let's say you or your organization needs to execute a particular type of document on a regular basis. You're sick of paper agreements and you want a change. Now you want to know the various ways in which you can electronically sign your documents.

The first thing you need to do is look at "Column A" - and identify what type of document it is - and then look at Columns B and C to see if a particular signing type is permitted for that type of document.

## EXPLAINING THE SPECIFIC TERMS OF THE MATRIX

**a) Type of Document:** A document which must mandatorily be signed under any law, rule or regulation

Most documents can be executed by any mode of acceptance. Such a provision will explicitly use the word "sign", "signed" or some other similar form.

A few other examples of such types of contractual documents:

- Copyright assignment agreements - which are required to be signed under Section 19 of the Copyright Act, 1957
- e-Insurance Policies - which are required to bear electronic signatures of the issuer
- KYC Documentation for various industries - which also mandatorily require signatures by regulation

Looking at the above matrix, if you want to **electronically execute** such documents then you will HAVE TO use an electronic signature. That is - either a digital signature under Section 3 of the IT Act or an electronic signature listed in Schedule II of the IT Act.

**b) Type of Document:** A document listed under Schedule I of the IT Act

As we mentioned in an earlier chapter, Schedule I lists out 5 different documents:

- A)** Negotiable instruments (other than cheques)
- B)** Powers-of-attorney
- C)** Documents that create trusts
- D)** Wills and other testamentary depositions

**E)** Contracts for the sale of conveyance of immovable property or any interest in such property

If your document is one of the above types of documents then you **cannot** execute it electronically under the IT Act. The only way in which you can perform an electronic execution is if a **separate law, rule or regulation or a lawful authority** permits you to do so.

**c) Type of Document:** Any document that doesn't need to be signed under any law and isn't listed under Schedule I of the IT Act

As we mentioned earlier, in most cases a document can be executed by way of any form of acceptance. A signature is usually the **preferred execution method** - but isn't the **only execution method**. This principle is also explicitly stated in the Indian Contract Act - and Section 10A of the IT Act.

If your document:

- Doesn't need to be executed via signature under any law, rule or regulation
- Isn't listed under Schedule I of the IT Act

Then you can use **any electronic execution** method.

However in many cases, people prefer **electronic signatures** over other modes of electronic execution - even for documents where they aren't mandatory.

Why is this the case?

Because of the principle of **Enforcement**. This is something we'll look at in the next part of the book.



# PART-II

## ENFORCEMENT OF ELECTRONIC SIGNING

# CHAPTER



# THE ENFORCEMENT OF eSIGNED DOCUMENTS

In the previous section of this book, we covered the validity of the most common ways of electronic signing in India:

- Section 3 Digital Signatures
- Schedule II Electronic Signatures
- Other Modes of Electronic execution like virtual signatures, click-wrap, email exchange etc.

We ended the last section with a “validity matrix” - an easy-to-decipher table charting the applicability of various modes of signing to different types of documents.

What the validity matrix essentially tells us is that the question of validity is a binary question. A particular signing type is either valid or invalid for a particular type of document.

Think of it like a switch.

**Validity of Virtual Signature**

Loan Agreement



**Valid**

Demat Account opening form



**Invalid**

But the question of validity has a very narrow and limited utility when it comes to actually going digital with paperwork. As per the validity matrix, most documents can be validly signed through any type of electronic execution.

The reality of digital paperwork also requires us to ask a far more specific and varied question - the question of enforcement.

## THE ROLE OF ENFORCEMENT IN ELECTRONIC EXECUTION OF DOCUMENTS

The journey of a legal document like a contract does not simply end at the time of execution. If you recall what we said in the prologue - the purpose of executing a legal document is designed to anchor two main forms of trust - commercial and legal.

The practical manifestation of this trust is the use of an executed document in 3 post execution scenarios:

- (1) When a default is committed, the aggrieved party can use the signed legal document as evidence to enforce its claims against the party in breach before a judicial authority.
- (2) In case of any audits by regulators such as RBI or SEBI, signed legal documents are essential to prove to the regulators that your business processes are complying with legal requirements.
- (3) Often, companies have their own internal policies that determine the level of consent/ acceptance - and the manner in which it needs to be obtained for a legal document.

That's where the concept of enforceability of such means comes in. Enforceability is a question of "how easy" it is to "prove" a document in Court or before a regulator.

## EASE OF ENFORCEMENT IS A SPECTRUM

Choosing a signature type based on enforcement considerations depends entirely on the risk appetite of your legal team.

For instance, in the case of a high-ticket secured loan, legal teams would value "enforcement" as a top priority given the stakes involved. In this case, they may ONLY choose electronic signatures for executing the loan agreement because of its ease of enforcement EVEN THOUGH a click-wrap or an exchange of emails would be **equally valid**.

On the other hand, say you have a low-ticket consumer loan agreement. Here, a legal team may not have "enforcement" as a key priority. Instead, cost and accessibility may be given a larger weightage. Here, they may opt for an **equally valid** Virtual Signature instead of an **easier to enforce** electronic signature.

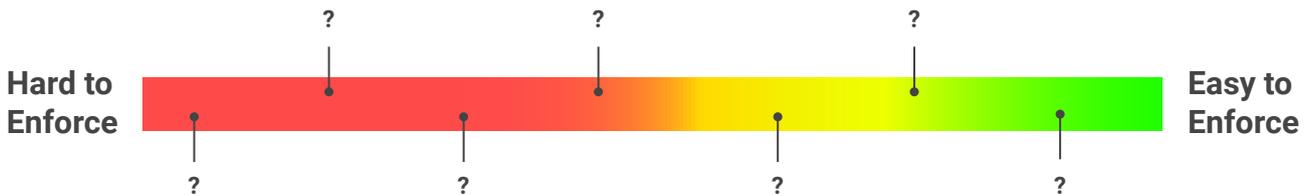
But how did we arrive at the above conclusions? How do we judge ease of enforcement of a particular signing type?

What makes electronic signatures easier to enforce than other signing types? Why is a virtual signature with multi-layered authentication more easily enforceable than just a plain virtual signature?

The answer to all these questions lie in the ability of an electronic mode of execution to **meet the end goals of the signing process**. The better a particular mode of execution is at meeting such end goals, the easier it would be to enforce it in a Court of law or before a regulator.

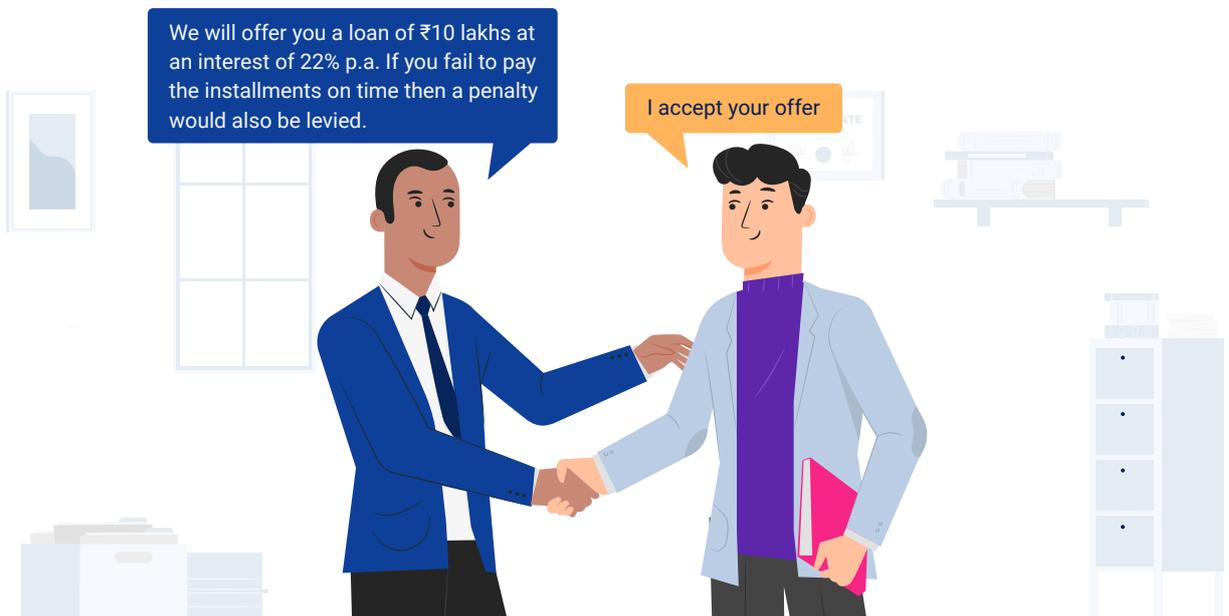
Therefore, unlike validity - which is a simple yes/no matrix - the question of enforcement needs to be visualized as a spectrum - a Spectrum of Enforcement.

**SPECTRUM OF ENFORCEMENT FOR ELECTRONIC SIGNING**



Where do the various “valid” signing types that we have discussed so far fit on this spectrum?

**I. HANDSHAKE AS A MODE OF CONVEYING ACCEPTANCE**

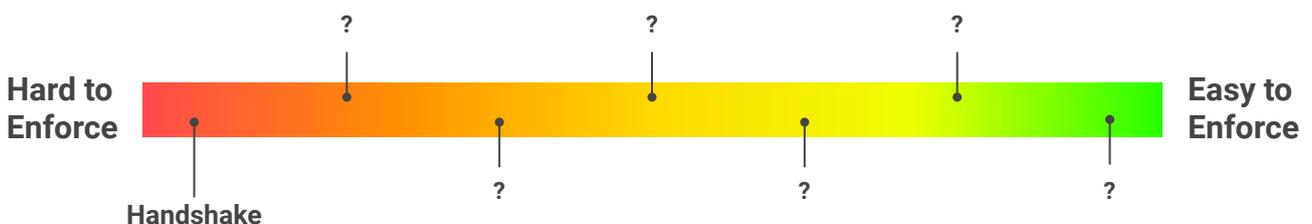


Technically when the borrower has conveyed his consent to enter into a contract through a handshake - it's a valid contract.

How well does this meet the end goals of the signing/execution process?

GOAL	HANDSHAKE
<p><b>Authentication:</b> The identity of the parties entering into the agreement is clear</p>	<p style="text-align: center;"><b>✗</b></p> <p>There is no physical or electronic evidence to show the identity of parties who decided to enter into a contract.</p>
<p><b>Integrity:</b> The terms of the agreement cannot be changed unilaterally after the handshake is done</p>	<p style="text-align: center;"><b>✗</b></p> <p>Handshakes are used to convey acceptance in case of an oral contract. But the terms of an oral contract are not recorded anywhere. This makes it extremely easy for parties to "change" their understanding of the agreed upon terms and conditions, or argue that certain additional conditions were also agreed upon orally.</p>
<p><b>Non-repudiation:</b> The parties cannot "deny" their acceptance of the terms and conditions of a document at a later stage</p>	<p style="text-align: center;"><b>✗</b></p> <p>Parties can contest their acceptance of the terms and conditions as there is no recorded proof of a contract being entered into.</p>

Due to these reasons, handshakes are languishing at the far end of our Spectrum of Enforcement as an extremely difficult-to-enforce method of executing a document.



## II. CLICKWRAP

Clickwrap is often used by mobile application developers to get users to accept their privacy policies. We have all entered into multiple click-wrap contracts in our lives.

But accepting terms of use of a software is one thing - making click-wrap the foundation for a substantial commercial contract with regulatory norms is another thing altogether.

Imagine a bank gives out 5 Lakh loans on the basis of click-wrap agreements.



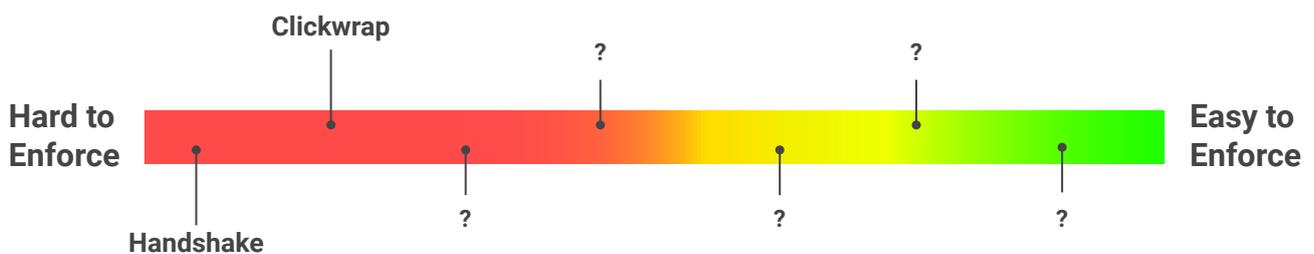
The RBI comes knocking on the bank’s door 6 months later for a routine audit.

When they see the Bank’s agreements - all they see are standard form agreements with proof of an “I agree” execution. There is no *personal, differentiated* mark by specific borrowers on the documents. The RBI has no way of ascertaining or even assuming that the Bank had taken due diligence and informed consent from borrowers on the terms and conditions of the agreement.

So while click-wrap may be *more traceable* than a handshake - it does a very poor job in meeting the goals of the signing process:

GOAL	CLICKWRAP
<p><b>Authentication:</b> The identity of the parties signing the document is clear</p>	<p style="text-align: center;"><b>?</b></p> <p>While you can point to the electronic device from which a response was recorded, the identity of the person who actually clicked the “I agree” or “Yes” button can never be conclusively ascertained.</p>

<p><b>Integrity:</b> The document cannot be changed unilaterally after the signatures are affixed</p>	<p style="text-align: center;"><b>✗</b></p> <p>Anything can be added or deleted to a document that has been click-wrapped. The PDF can be edited later as there are none of the technical safeguards that electronic signatures rely on to assure integrity of the document.</p>
<p><b>Non-repudiation:</b> The parties cannot later “deny” their acceptance of the terms and conditions of a document at a later stage</p>	<p style="text-align: center;"><b>✗</b></p> <p>Given that the identity of the person clicking the “I agree” button cannot be ascertained, it becomes easier for that party to deny their acceptance of the terms and conditions at a later stage.</p>

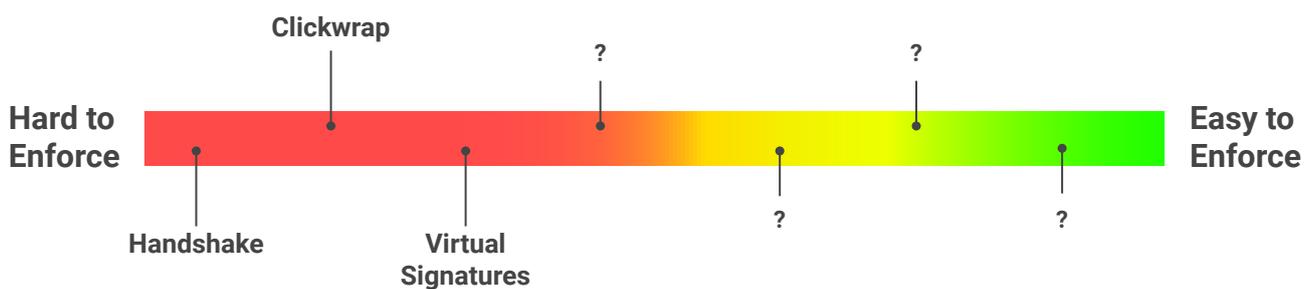


### III. STANDARD VIRTUAL SIGNATURES

Standard virtual signatures are nothing but a visual electronic replication of your wet-ink signature. All you need to affix a virtual sign is the electronic agreement and a service provider which lets you affix virtual signatures on an electronic document. Users can either draw their signature electronically or choose from a computer generated template of their name. You may have signed this way sometimes when you receive a courier.

Standard virtual signatures - while somewhat better than a click-wrap - are still quite shaky.

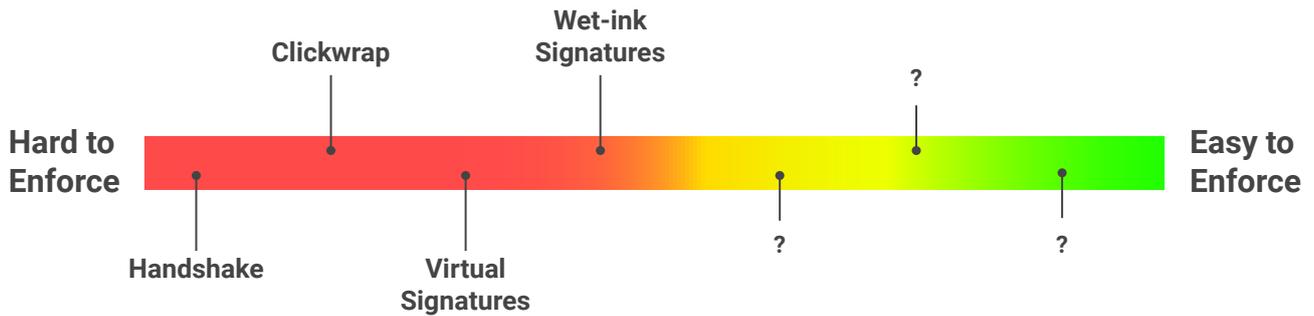
GOAL	VIRTUAL SIGNATURES
<p><b>Authentication:</b> The identity of the parties signing the document is clear</p>	<p style="text-align: center;"><b>?</b></p> <p>While the wet-ink signature pattern of a person is said to be unique to a person, it is tough to draw this unique signature electronically. It is fairly easy for two different people to have the same virtual signature.</p>
<p><b>Integrity:</b> The document cannot be changed unilaterally after the signatures are affixed</p>	<p style="text-align: center;"><b>×</b></p> <p>Anything can be added or deleted once a virtual signature is affixed to an electronic agreement. The PDF can be edited later as there are none of the technical safeguards that electronic signatures rely on to assure integrity of the document.</p>
<p><b>Non-repudiation:</b> The parties cannot later “deny” their acceptance of the terms and conditions of a document at a later stage</p>	<p style="text-align: center;"><b>×</b></p> <p>Similar to wet-ink signatures, parties can contest their virtual signatures also in 2 ways:</p> <ol style="list-style-type: none"> <li>1) By stating that the signature was forged</li> <li>2) By stating that the document has been altered/tampered since they signed it</li> </ol>



#### IV. WET-INK SIGNATURES

For millennia, the wet-ink signature has been the preferred mode of communicating acceptance to enter into a written agreement. Despite this long standing usage and dependence on wet-ink signatures as a source of “evidence” it performs poorly on our Spectrum of Enforcement. Here’s why:

GOAL	WET-INK SIGNATURES
<p><b>Authentication:</b> The identity of the parties signing the document is clear</p>	<p style="text-align: center;"><b>?</b></p> <p><b>Good:</b> The wet-ink signature pattern of a person can, in some cases, show uniqueness</p> <p><b>Bad:</b> However, there is nothing to prevent someone from forging someone else’s “unique” signature. Consequently, signature experts are often called for Court proceedings - and their opinion is often inconclusive.</p>
<p><b>Integrity:</b> The document cannot be changed unilaterally after the signatures are affixed</p>	<p style="text-align: center;"><b>×</b></p> <p>Anything can be added or deleted once a wet-ink signature has been affixed to an agreement. Pages can be removed or inserted later as there is no technical way to track whether a subsequent change was made before or after a wet-ink signature was affixed. Making parties sign “blank pages” is a very common practice in many industries.</p>
<p><b>Non-repudiation:</b> The parties cannot “deny” their acceptance of the terms and conditions of a document at a later stage</p>	<p style="text-align: center;"><b>?</b></p> <p>Parties can contest their signatures in 3 ways:</p> <ol style="list-style-type: none"> <li>1) By stating that the signature was forged</li> <li>2) By stating that the document has been altered/tampered since they signed it</li> <li>3) By stating that they were forced to sign a blank form (which is often the case!)</li> </ol> <p>The only thing that makes wet-ink signatures slightly better than standard virtual signatures is the centuries of legal convention that sees “wet ink signatures” as the “standard” mode of signing</p>

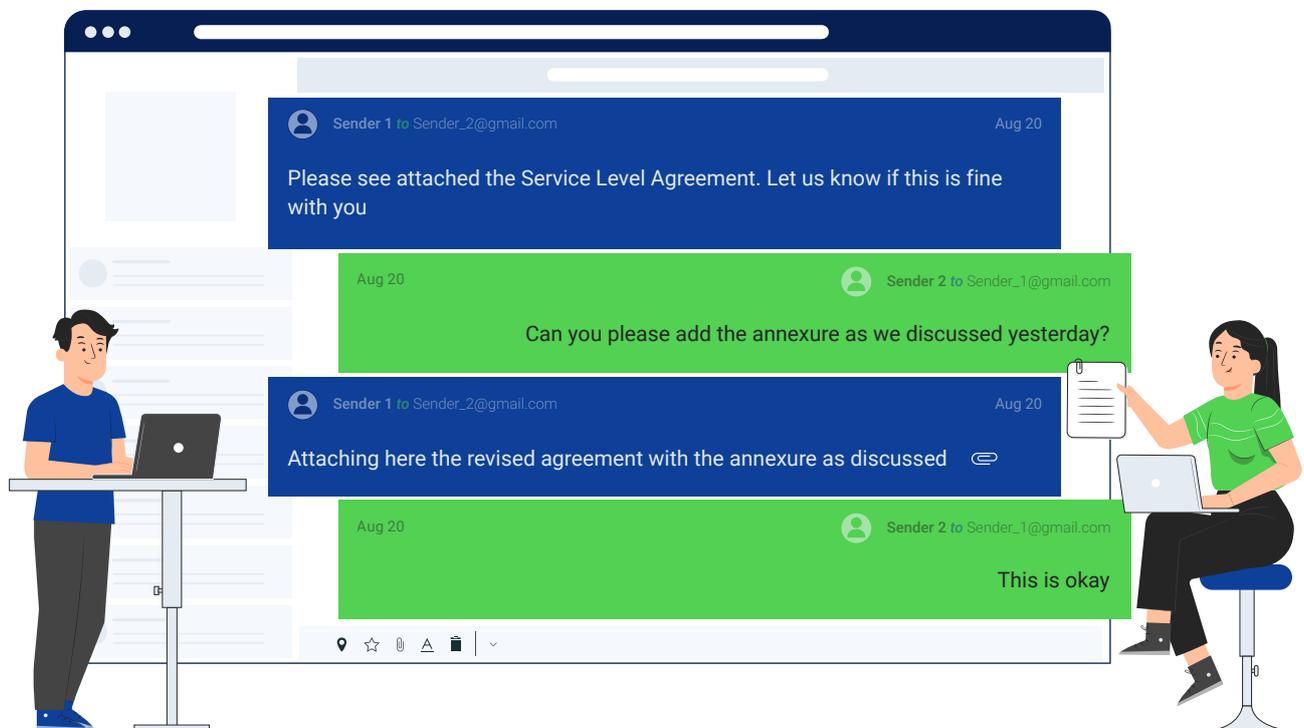


## V. EMAIL EXCHANGE

Commercial contracts are often entered into through an exchange of emails, whenever it is inconvenient for the parties to meet in person. The terms of the contract are negotiated, re-negotiated and finalised over email where parties communicate their consent to enter into a contract through written replies.

Even the Supreme Court, in *Trimex International FZE, Dubai v. Vedanta Aluminum Limited*, (2010) 3 SCC 1, upheld the validity of a contract entered into via an exchange of emails.

But, while email exchanges may be valid, their enforceability is a different matter.



This email chain highlights the problems associated with enforcing contracts concluded over emails:

**Ambiguous acceptance:** What does “this is okay” in the email chain signify? Is she fine with the draft of the annexure? Or is she fine with the agreement as a whole? Even if she was referring to the entire agreement, by saying “this is okay” does she intend to enter into a contract and be bound by the terms and conditions mentioned therein?

This problem of ambiguity while finalising a contract over an email was aptly highlighted in the case of *Ambalal Sarabhai Enterprise Limited v. KS Infraspace LLP Limited*, (2020) SCC OnLine 1. While upholding the validity of emails as a method of concluding contracts, the Court held the contract in this case to be invalid as the nature and language of the correspondences shared between the parties did not directly equate to affirmation. In the Court’s opinion, calling an agreement that was being negotiated between the parties the “final draft”, “cannot be determinative by itself” of a concluded contract.

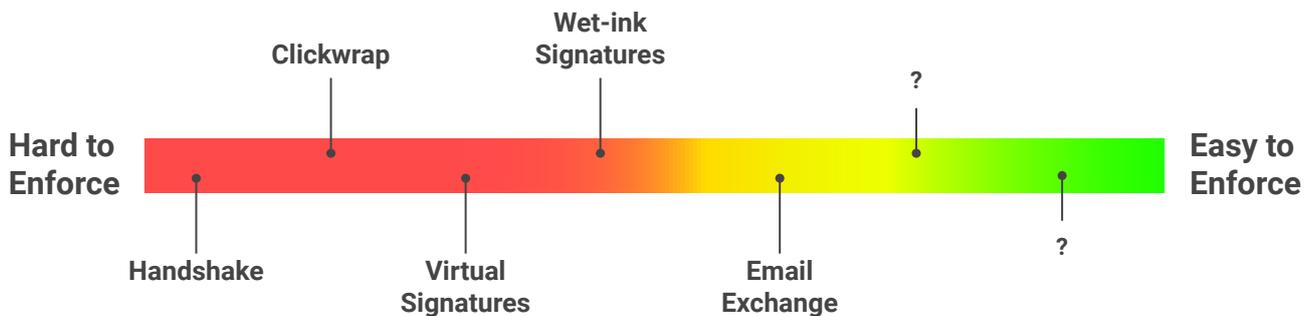
**Identity authentication:** Did the “this is okay” email actually come from the party you intended to enter into a contract with? There is no way of knowing that for sure. Failure to securely establish the identity of the signer can lead to problems later. In case of a legal dispute the other party can always say that the email did not actually come from them.

**Operational inconvenience:** Organisations such as banks, NBFCs and portfolio management services are required by regulators such as the RBI and SEBI to maintain proper records of their dealings with customers. In case these regulators conduct an audit or ask for certain documents, it would be impractical to submit emails in such a scenario.

**Accessibility:** Another drawback of relying on emails as a mode of concluding contracts is that many people, especially in a country like India, do not keep a regular email ID! For many organisations, such as MFIs, who cater to the unbanked and underbanked segments, email is completely out of the question.

With all these problems, it is no surprise that the enforcement of email exchanges is littered with doubts:

GOAL	EMAIL EXCHANGE
<p><b>Authentication:</b> The identity of the parties entering in to the agreement is clear</p>	<p style="text-align: center;"><b>?</b></p> <p><b>Good:</b> Email accounts are a decent signifier of identity in and of themselves.</p> <p><b>Bad:</b> However they do not provide a computationally secure way of ensuring identity. Anyone can create an email ID for another person's name. Email IDs get hacked frequently. Most importantly - most people in India do not have an email ID.</p>
<p><b>Integrity:</b> The document cannot be changed unilaterally after the contract has been concluded</p>	<p style="text-align: center;"><b>✓</b></p> <p>The final draft of the contract to which the parties have conveyed their acceptance on the email chain is electronically recorded on the email service provider's servers. This cannot be changed unilaterally after the contract has been concluded as all parties have the same copy of the contract.</p>
<p><b>Non-repudiation:</b> The parties cannot "deny" their acceptance of the terms and conditions of a document at a later stage</p>	<p style="text-align: center;"><b>?</b></p> <p><b>Good:</b> Courts are generally well-versed with email correspondence as evidence.</p> <p><b>Bad:</b> If there is any ambiguity in the language while conveying acceptance, that party can always repudiate the contract by saying that a final binding contract was not concluded between all the parties. This is enough ambiguity to ensure protracted Court proceedings.</p>



## VI. SECURE VIRTUAL SIGNATURES

We saw how virtual signatures are similar to wet-ink signatures, but applied to an electronic medium. But we also saw how virtual signatures can be hard to enforce. That's where a concept known as "**Secure Virtual Signature**" comes in. It solves for this gap by adding additional layers of authentication

Some examples of added layers of authentication provided by Secure Virtual Signatures:

### 1) OTP authentication system

Signers can be asked to enter an OTP sent to their registered phone number/ email address before they can sign the document. Since the OTP is being sent to a unique parameter exclusive to the signer - an element of identity is added to the process.

### 2) Face Capture

With a Face Capture layer - signers are required to undergo a live face capture before they can sign the document. The face capture feature establishes beyond doubt the identity of the person who has affixed his Secure Virtual Signature to the document.

To prevent cheating by signers, Face Capture can be built with a liveness check - to ensure that it is a live face in front of the camera.

### 3) Geo-location capture

With Geo-location capture, the signer's GPS coordinates are captured at the moment of signing. This is useful in cases where electronic signing is happening at a fixed location like a bank branch or the signer's home.

### 4) Backing each virtual sign with a neutral digital signature

A virtual sign - no matter how secure, does not operate on the asymmetric crypto and hash systems that a digital signature operates on. This opens the virtually signed document to risk of undetected tampering.

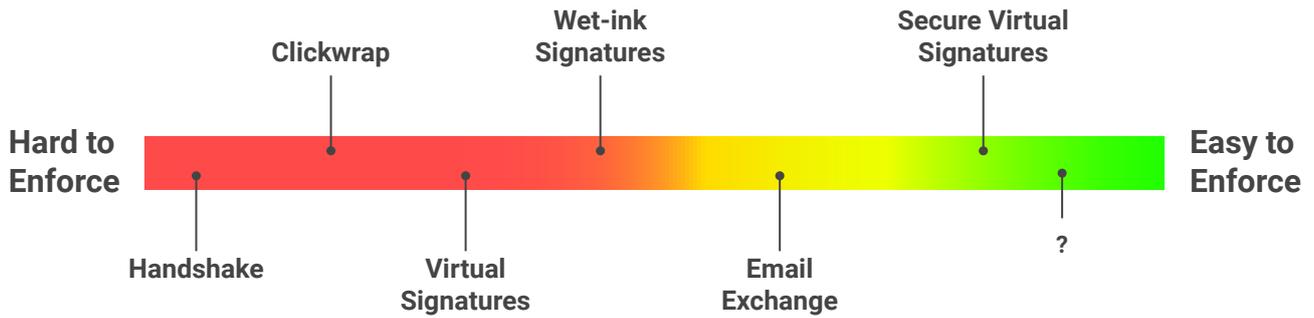
This glaring loophole can be circumvented if the technology platform affixing the virtual sign also affixes a neutral digital signature on the document. This digital signature won't act as a "signature of a party" but as a "security procedure" that safeguards the integrity of the document (more on this in the next chapter).

If all the above layers are in force, it becomes very hard for a signer to repudiate a “Secure Virtual Signature”. To successfully do that they would need to do ALL of the following:

- (i) Prove that the OTP authentication on their phone number was not done by them
- (ii) Prove that they did not perform the act of selecting or inscribing the virtual signature
- (iii) Prove that the geo-location captured does not actually reflect their location at the time of signing the document
- (iv) Prove that it was not their face in the face capture

These additional security features put Secure Virtual Signatures in a very good position when it comes to enforcement:

GOAL	SECURE VIRTUAL SIGNATURES
<p><b>Authentication:</b> The identity of the parties signing the document is clear</p>	<p style="text-align: center;"></p> <p>OTP verification, face capture and geo-capture work together to establish a “virtually irrefutable” trail of identity.</p>
<p><b>Integrity:</b> The document cannot be changed unilaterally after the signatures are affixed</p>	<p style="text-align: center;"><b>?</b></p> <p><b>Bad:</b> Secure virtual signatures do not make use of asymmetric cryptographic systems and hash functions to ensure the integrity of the signed document. So in an ordinary scenario they ensure document integrity in the same way that wet-ink signatures do.</p> <p><b>Good:</b> At times documents signed using secure virtual signatures are secured by a digital signature affixed in the background by the third party platform. This acts as a security procedure under the IT Act to ensure that the document cannot be altered or modified without alerting the parties.</p>
<p><b>Non-repudiation:</b> The parties cannot “deny” their acceptance of the terms and conditions of a document at a later stage</p>	<p style="text-align: center;"></p> <p>Added security layers make it extremely hard for signers to repudiate secure virtually signed documents in Court.</p>



### VII. ELECTRONIC SIGNATURES (INCLUDING DIGITAL SIGNATURES)

Aadhaar eSign (online and offline), PAN eSign and DSC tokens form the crème de la crème of electronic signing methods - not only because they are legally valid for the most number of use cases, but also because they are the easiest to enforce.

We have already seen how the underlying combination of asymmetric cryptographic systems and hash functions behind [digital signatures](#) and [electronic signatures](#) helps in:

- Linking the identity of the signer irrefutably to the document
- Making it computationally impossible to tamper the digitally signed document without parties being alerted

There is no other signature type that meets the end goals of the signing process better than electronic signatures.

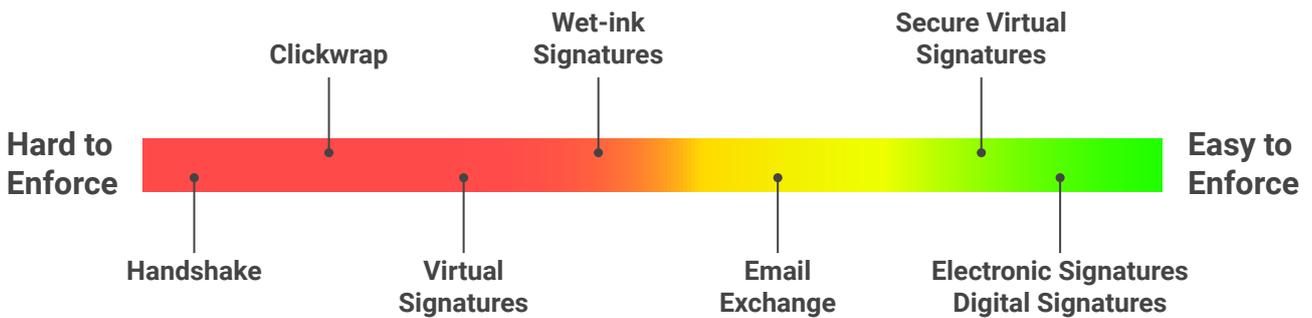
GOAL	ELECTRONIC SIGNATURES	DIGITAL SIGNATURES
<p><b>Authentication:</b> The identity of the parties signing the document is clear</p>		<p>The secure key pair encryption/decryption process helps to clearly establish the signer's identity, details of which are contained in the electronic signature certificate that is digitally signed by the Certifying Authority, a neutral entity.</p>
<p><b>Integrity:</b> The document cannot be changed unilaterally after the signatures are affixed</p>		<p>The public key decryption + hash matching process ensures that anyone opening the document on a PDF reader is alerted if the document has been <b>altered</b> after the signatures were affixed.</p> <p>The hash matching process is virtually foolproof in detecting tampering since it is computationally infeasible for two different documents to have the same hash result.</p>

<p><b>Non-repudiation:</b> The parties cannot “deny” their acceptance of the terms and conditions of a document at a later stage</p>	<p style="text-align: center;">✔</p> <p>The secure key pair is only issued by the ESP once the Aadhaar based eKYC of the signer has been successfully carried out by UIDAI.</p> <p>For the signer to deny their Aadhaar eSign, they would need to prove that someone else had their Aadhaar number and their mobile phone which they used to carry out the e-authentication process. This is <b>extremely unlikely</b>.</p>	<p style="text-align: center;">✔</p> <p>The asymmetric crypto system can only be activated by a unique PIN or code that has been handed over <b>ONLY</b> to the signer.</p> <p>For the signer to deny the digital signature - they would need to prove that someone else got access to this PIN or code. This is <b>extremely unlikely</b>.</p>
--	---	---

Authentication, check. Integrity, check. Non-repudiation, check.

## THE FINAL SPECTRUM OF ENFORCEMENT

So, based on the above analysis, the final spectrum of enforceability of common electronic signing types looks like this:



The above spectrum is a handy tool to assess enforceability of a particular electronic execution type you are evaluating as you make the transition to digital documentation.

You can assess the location of each signing type on the spectrum against other key factors like:

- Likelihood of the need of enforcement arising
- Regulatory/Audit requirements
- Internal compliance

Using this evaluation methodology - instead of **just validity** - will make it easier for you to transition to digital documentation in a safe, enforceable way that gives you peace of mind.

## CHAPTER



# **LEGAL PRESUMPTIONS IN FAVOUR OF eSIGNS UNDER THE EVIDENCE ACT**

We saw how electronic signatures, or eSigns, best meet the end goals of the signing process, hence making them the most easily enforceable form of executing a document. But do our laws also recognise this inherent superiority of electronic signatures over other methods of execution? The short (and sweet) answer is YES.

The Evidence Act creates several presumptions in favour of the validity of eSigns. These presumptions - when combined with the solid technical architecture of eSigns - make enforceability even easier. In this chapter we will look at what these legal presumptions in favour of eSigns are.

## PRESUMPTIONS OF VALIDITY UNDER THE IT ACT

The Indian Evidence Act, 1872 lays down the rules governing admissibility of evidence in India. The Indian Evidence Act carves out several presumptions that make eSign much easier to enforce compared to other electronic execution methods. Let us take a look at what these presumptions are.

### I. SECTION 47A

**47A. Opinion as to electronic signature, when relevant.-** When the Court has to form an opinion as to the electronic signature of any person, the opinion of the Certifying Authority which has issued the Electronic Signature Certificate is a relevant fact.



As per Section 47A of the Indian Evidence Act 1872, the opinion of the issuing Certifying Authority is a relevant fact for the Court to make an opinion as to the electronic signature of any person. Certifying Authorities maintain full transactional logs to assist and certify any transactions carried out through them for adjudication purposes. Therefore, in the unlikely event that an electronic signature is ever questioned in Court, there is a standing help in the form of a regulated neutral entity that can vouch for it.

Additionally, the signature certificate, its properties and details such as the name of the signer etc. can be viewed by anyone in the PDF reader itself.

## II. SECTION 67A

**67A. Proof as to electronic signature.**—Except in the case of a secure electronic signature, if the electronic signature of any subscriber is alleged to have been affixed to an electronic record the fact that such electronic signature is the electronic signature of the subscriber must be proved.



Before we delve into this Section, let us look at what secure electronic signatures are.

### Secure electronic signatures

As per Section 3 of the Evidence Act, a “secure electronic signature” shall have the same meaning as assigned under the IT Act.

Section 15 of the IT Act defines what secure electronic signatures are.

**15. Secure electronic signature.** - An electronic signature shall be deemed to be a secure electronic signature if-

- (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
- (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation.- In case of digital signature, the “signature creation data” means the private key of the subscriber.



From Section 15 we understand that for an electronic signature to be a secure electronic signature, the **signature creation data or the private key needs to be under the exclusive control of the signatory and no other person.**

So do DSC tokens, Doc Signer, Online Aadhaar eSign, Aadhaar XML eSign and PAN eSign qualify as secure electronic signatures?

For DSC tokens, after the KYC authentication process is complete, the Certifying Authority issues the hardware token to the signer which contains the private key of the signer. This hardware token remains exclusively in the custody of the signer. Additionally, a unique PIN known only to the signer is required to activate the token. Similarly, for Doc Signer, the private key is saved safely on the organisation's servers. Therefore, the signature creation data or the private key remains under the exclusive control of the signer in the case of DSC tokens and Doc Signer.

In Online Aadhaar eSign, the signer clicks on the signing link provided by the ASP to initiate the signing journey. This redirects the signer to the portal maintained by either NSDL or CDAC. Here the signer authenticates her identity through either OTP or biometric verification. Only upon the signer finishing these steps is the private key generated by the ESP and stored in her hardware security module. The generation of the private key can only be triggered via the signer performing her identity e-authentication using information solely in her control. For Online Aadhaar eSign this is the Aadhaar number and subsequent OTP. For Aadhaar XML and PAN eSign it's the assigned ID and password. All of these parameters are under the exclusive control of the signer at all times. This means that the private key is under the exclusive control of the signer at the time of affixing the signature.

Therefore, DSC tokens, Doc Signer, Online Aadhaar eSign, Aadhaar XML eSign and PAN eSign qualify as secure electronic signatures under the IT Act where such signatures are affixed in accordance with the specifications prescribed.

Now let's come back to **Section 67A**. It states that if a signer uses a secure electronic signature to execute a document then it will be presumed that such eSign belonged to the signer herself and not to any other person. This means that for non secure eSigns, the affixture of the electronic signature must be proven to have been done by the signer. But for secure electronic signatures - this burden of proof is not required. Therefore, someone who has signed using a secure electronic signature later cannot refute his signature. This Section is the legal recognition of the ability of eSigns to meet the "authentication" goal of the signing process.

### III. SECTION 85A

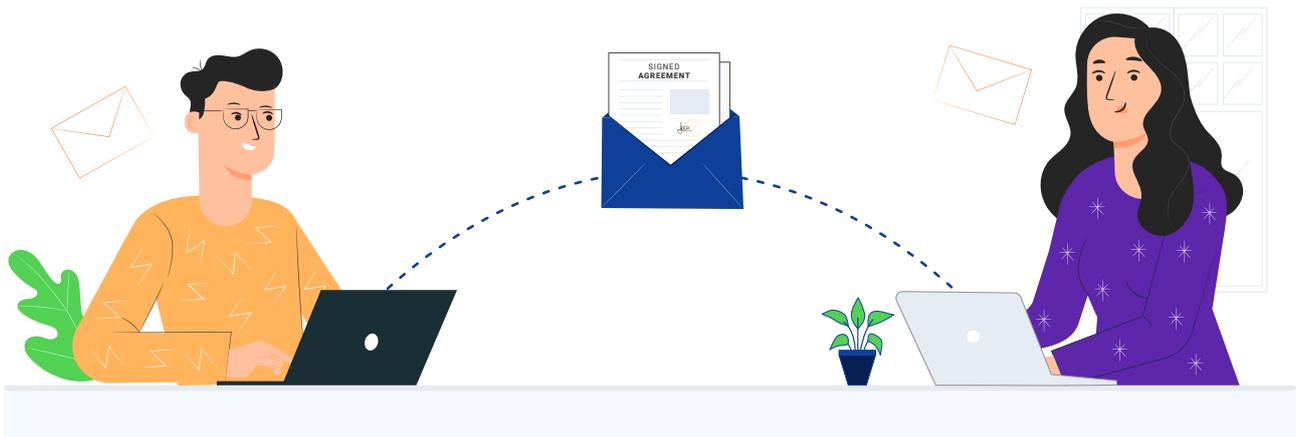
**85A. Presumption as to electronic agreements.**- The Court shall presume that every electronic record purporting to be an agreement containing the electronic signature of the parties was so concluded by affixing the electronic signature of the parties.



Section 85A says that an agreement which has been executed using electronic signatures will be presumed to have been concluded between the parties.

So what does this mean exactly?

Let's take the help of a Supreme Court case to understand this better.



In *Ambalal Sarabhai Enterprise Limited v. KS Infraspace LLP Limited*, (2020) SCC OnLine 1, the main point of contention was whether there was a concluded contract between the parties. While the plaintiff argued that there was a concluded contract between him and the defendant regarding sale of certain immovable property, the defendant denied that the contract “*did not attain finality but remained at the stage of discussions only.*” The Court looked at the negotiations that had happened between the parties over email and Whatsapp, and concluded that no contract had been concluded between the two. The Court stated that “*the use of the words “final draft” in the e-mail dated 30-3-2018 cannot be determinative by itself*” of a concluded contract.

Now, had the parties actually affixed their electronic signature to this “final draft” of the contract, then the plaintiff’s life would have been much easier. By virtue of Section 85A, the Court would have had to presume that the contract was concluded when the parties affixed their electronic signature. The defendant would then have had to adduce additional evidence to show that the contract had in fact not been concluded. But given the superior technological framework employed



by electronic signatures which make altering the contract post-signing virtually impossible, it would have been very difficult for the defendant to rebut such a presumption. Section 85A thus lends certainty as to the finality of the terms and conditions agreed between parties to the agreement.

**IV. SECTION 85B**

**85B. Presumption as to electronic records and electronic signatures.-** (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure electronic signature, the Court shall presume unless the contrary is proved that—

- (a) the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record;
- (b) except in the case of a secure electronic record or a secure electronic signature, nothing in this section shall create any presumption, relating to authenticity and integrity of the electronic record or any electronic signature.



Before we break down Section 85B into its constituent parts, we first need to learn one more concept - secure electronic records.

*Introducing **secure electronic records***

As per Section 3 of the Evidence Act, a “secure electronic record” shall have the same meaning as assigned under the IT Act.

Section 14 of the IT Act defines secure electronic records as:

**14. Secure electronic record.-** Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.



So what are these ‘security procedures’ that when applied to an electronic record make it a secure electronic record?

Section 16 of the IT Act answers this question:

**16. Security procedures and practices.-** The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices:

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.



The Central Government, exercising the powers conferred by Section 16, enacted the Information Technology (Security Procedure) Rules, 2004 vide Notification G.S.R. 735(E) dated October 29, 2004.

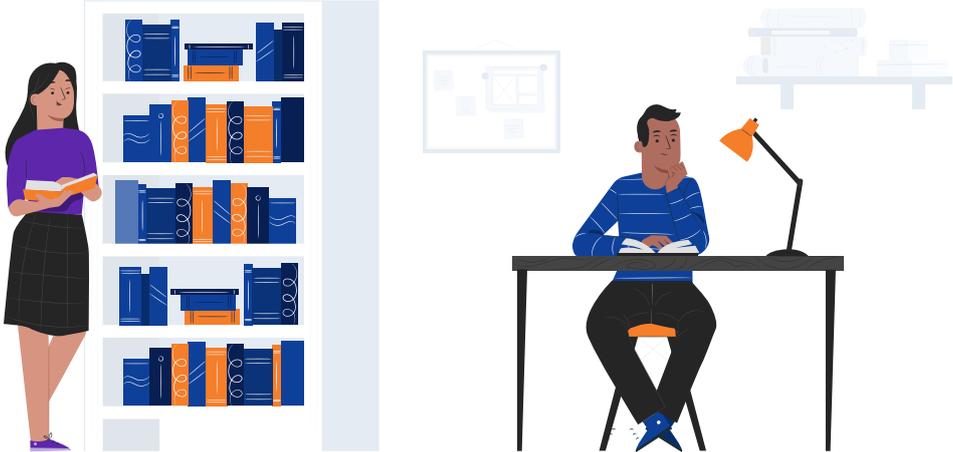
Rule 3 of the Security Procedure Rules state that:

**3. Secure electronic record.-** An electronic record shall be deemed to be a secure electronic record for the purposes of the Act if it has been authenticated by means of a secure digital signature.



This means that if one uses a secure digital signature to authenticate an electronic document, then that document will be a secure electronic record under law. But what is a 'secure digital signature'?

Rule 4 of the Security Procedure Rules as amended by Information Technology (Security Procedure) Amendment Rules, 2015 defines secure digital signature:



**4. Secure digital signature.-** A digital signature shall be deemed to be a secure digital signature for the purposes of the Act if the following procedure has been applied to it, namely:-

- (a) that the smart card or hardware token, as the case may be, with cryptographic module in it, is used to create the key pair;
- (b) that the private key used to create the digital signature always remains in the smart card or hardware token as the case may be;
- (c) that the hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system;
- (d) that the information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature;
- (e) that the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person;
- (f) that the standards referred to in rule 7 or rule 12 of the Digital Signature (End Entity) Rules, 2015 have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and
- (g) that the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated.



So a digital signature, which complies with the points (a) to (g) of Rule 4 shall be a secure digital signature, which can be used to create secure electronic records.

But does this mean that only digital signatures can be used to create secure electronic records, and not electronic signatures?

No. Even electronic signatures, such as Online Aadhaar eSign, Aadhaar XML eSign and PAN eSign rely on the same algorithmic interplay between an electronic record, hashing functions, an asymmetric crypto system, a hardware security module and electronic signature certificates, just like digital signatures. The Security Procedure Rules were drafted in 2004 and haven't been suitably updated to reflect the 2008 amendments to the IT Act which brought in the concept of electronic signatures.

All types of electronic signature commonly used in India today seem to fulfil the requirements of Rule 4 and thus should be considered as secure digital signatures capable of creating secure electronic records.

<p><b>RULE 4 REQUIREMENTS</b></p>	<p><b>eSIGNS</b> (DSC TOKENS, DOC SIGNER, ONLINE AADHAAR eSIGN, AADHAAR XML eSIGN AND PAN eSIGN)</p>
<p>(a) the hardware token is used to create the key pair</p>	<p style="text-align: center;"></p> <p>The DSC Token consists of a hardware security module that stores the secure key pair. For Doc Signer, the organisation's servers act as the hardware security module which is used to create the key pair.</p> <p>For Online Aadhaar eSign, Aadhaar XML eSign and PAN eSign, the ESP creates the key pair which is stored and secured on a hardware security module maintained by the ESP itself.</p>
<p>(b) The private key used to create the digital signature always remains in the hardware token</p>	<p style="text-align: center;"></p> <p>The private key used by all these 5 types of eSign to create the digital signature is stored solely in the hardware security module</p>
<p>(c) The hash of the content to be signed is taken from the host system to the hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system</p>	<p style="text-align: center;"></p> <p>Upon entering the unique PIN, the DSC token performs a hashing function on the electronic document, which generates a hash result for the electronic record. This hash result is then encrypted by the private key housed in the hardware token.</p> <p>In Online Aadhaar eSign, Aadhaar XML eSign and PAN eSign, the ASP performs the hashing function on the electronic document to create its hash result. This hash result is passed on to the ESP where the Hardware Security Module is stored. The ESP encrypts the input document hash (passed on by the ASP) using the private key to create a scrambled hash result. The ESP then passes the Electronic Signature Certificate and the scrambled hash result to the ASP, which then facilitates affixture of the eSign on to the document.</p>

<p>(d) The information contained in the hardware token is solely under the control of the person who is purported to have created the digital signature</p>	<p style="text-align: center;">✔</p> <p>In our explanation to Secure Electronic Signatures we saw that for DSC tokens, Doc Signer, Online Aadhar eSign, Aadhaar XML eSign and PAN eSign the private key is under the exclusive control of the signer at the time of affixing the signature.</p>
<p>(e) the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person</p>	<p style="text-align: center;">✔</p> <p>The fact that a public key is able to decrypt the scrambled hash proves that the signature was affixed by the signer's private key.</p>
<p>(f) the standards referred to in rule 7 or rule 12 of the Digital Signature (End Entity) Rules, 2015 are complied with, in so far as they relate to the creation, storage and transmission of the digital signature</p>	<p style="text-align: center;">✔</p> <p>The standards laid down in Rule 7 and 12 are complied with</p>
<p>(g) the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated</p>	<p style="text-align: center;">✔</p> <p>PDF readers use the public key of the signer stored in the electronic signature certificate to unscramble the hash result and verify the integrity of the signed document.</p>

To avoid any ambiguity and to give flexibility in the future for different eSign types that do not rely on digital signature technology but can still be used to create secure electronic records, Rule 3 and 4 should be amended and made technology neutral, so as to include electronic signature technology also within its ambit. We had earlier highlighted that the IT Act [suffers from sloppy drafting](#) in parts. While the Parliament should rectify those errors in the Act itself, the Central Government must also undertake a clean-up of the IT Rules to bring them at par with changes in the IT Act.

**Breaking down Section 85B**

Now let's get back to what Section 85B of the Evidence Act says.

## Document integrity

**Clause (1)** states that in proceedings involving a secure electronic record, it will be presumed that the **secure electronic record has not been altered** since the time it was executed by a secure digital signature.

With physical signatures the problem that often arises is that a signer may later repudiate the contract entered into by saying that it has been tampered with and certain terms and conditions have been added or deleted. But by virtue of Section 85B(1), such an argument is rendered untenable. The ability of Section 3 Digital Signatures and Schedule II eSigns to ensure integrity of the signed document is not just technologically assured, but now it is also legally recognised.

## Signer approval

**Clause (2)** of Section 85B states that wherever there is a **secure electronic signature**, the Court will presume that it was **affixed by the signer with the intention of signing or approving** the electronic record.

The effect of Section 85B(2) is that no party to an agreement, in case they use a secure electronic signature to execute the document, can later claim that they did not know what they were signing. Intention of the signer to approve the contents of the signed document is legally presumed, by virtue of this section.

Signers who have signed a document physically often contend that they were made to sign blank forms, or that their signature was unlawfully obtained. Such contentions can elongate and frustrate judicial proceedings. However, with Section 85B(2) since the intention of the signer to approve the contents of the document is also presumed, such frivolous claims are taken care of. This makes the electronic signature - and the document which it signs - much easier to enforce.

This section reinforces the ability of secure electronic signatures to meet the end goals of the signing process, especially “integrity” and “non-repudiation”.

## V. SECTION 85C

**85C. Presumption as to Electronic Signature Certificates.-** The Court shall presume, unless contrary is proved, that the information listed in a Electronic Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.



Section 85C states that the details mentioned in the Electronic Signature Certificate, such as name of the signer, email ID and time of signing will be presumed to be true. This helps in establishing the identity of the person who signed the document.

## VI. SECTION 90A

**90A. Presumption as to electronic records five years old.-** Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the electronic signature which purports to be the electronic signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explanation. – Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.



Section 90A applies to electronic records that are five or more years old. If such electronic records contain an electronic signature, then the Court will **presume** that it was **affixed by the person whose electronic signature** it purports, or appears, to be. Section 90A is similar to Section 67A of the Evidence Act, to the extent that the identity of the signer is presumed and need not be proven.

# CHAPTER



# **PRODUCING ELECTRONIC AGREEMENTS AS EVIDENCE IN COURT**

Based on the underlying technical architecture behind each form of execution we learnt why certain execution methods are easier to enforce than others. We saw that this ease of enforceability of electronic signatures is legally recognised as well under the Indian Evidence Act, 1872. So if a dispute were to arise between parties to an agreement, how does one exactly go about proving these electronic agreements in Court? In this chapter we will answer this question by providing an overview of the law on Section 65B of the Indian Evidence Act, 1872.

## PROVING PHYSICAL AGREEMENTS

Before we get into how electronic agreements are proved in Court, let us take a quick look at how traditional paper-based agreements may be proved.

As a general rule, one must produce the original copy of the paper-based agreement in Court. Only in certain exceptional circumstances (for example, if the original has been lost or destroyed) can one use “secondary evidence” (such as a photocopy) of the original agreement.

**Section 64** of the Evidence Act states that a document must be proved by primary evidence, except in cases provided for under the Act. Primary evidence here means the document itself, as per **Section 62**.

The **exceptions to the rule** of providing original copies have been enumerated under **Section 65** of the Act. As per this Section, secondary evidence may be given of the existence, condition or contents of a document in the following cases:-

- (a) When the original is shown or appears to be in the possession or power (i) of the person against whom the document is sought to be proved, or (ii) of any person out of reach of, or not subject to, the process of the Court, or (iii) of any person legally bound to produce it, and when, after the notice mentioned in section 66, such person does not produce it;
- (b) When the existence, condition or contents of the original have been proved to be admitted in writing by the person against whom it is proved;
- (c) When the original has been destroyed or lost, or when the party offering evidence of its contents cannot, for any other reason not arising from his own default or neglect, produce it in reasonable time;

- (d) When the original is of such a nature as not to be easily movable;
- (e) When the original is a public document within the meaning of section 74;
- (f) When the original is a document of which a certified copy is permitted by the Evidence Act, or by any other law in force in India to be given in evidence;
- (g) When the originals consist of numerous accounts or other documents which cannot conveniently be examined in Court, and the fact to be proved is the general result of the whole collection.

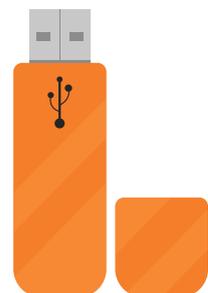
In each of the aforementioned cases, only the following types of secondary evidence are permitted:

In cases (a), (c) and (d), any secondary evidence of the contents of the document is admissible. In case (b), written admission is admissible. In cases (e) or (f), a certified copy of the document, but no other kind of secondary evidence, is admissible. In case (g), evidence may be given as to the general result of the documents by any person who has examined them, and who is skilled in the examination of such documents.

While this general rule of providing original copies might be feasible for physical documents, it becomes **extremely cumbersome in the case of electronic documents**. The “original” electronic record might be stored on remote servers, multiple computers, phone etc.

### Enter Section 65B

Section 65B of the Evidence Act helps solve this problem. It lays down the process by which the contents of electronic records can be admitted into evidence. You do not need to bring the device containing the original electronic record to be able to tender it in evidence in Court. Instead, you can just produce a copy of the record in the form of a printout, USB drive or CD-ROM, as long as you can demonstrate the integrity and authenticity of the document being produced.

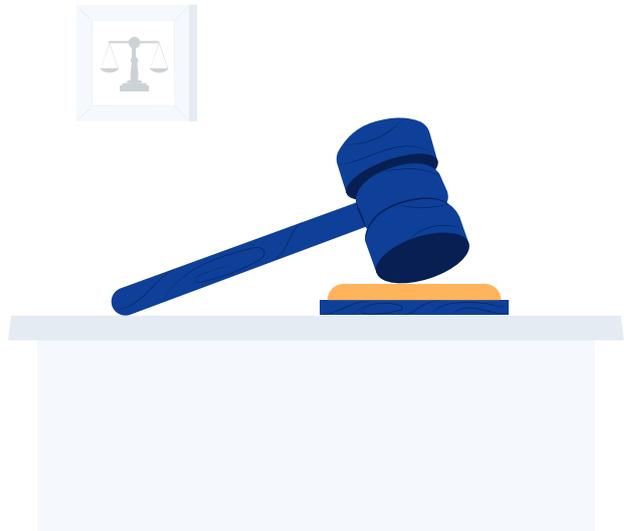


Is Section 65B mandatory for producing electronic agreements in Court? While there has been some confusion on this point in legal circles - the Supreme Court's position is quite clear and unambiguous.

### Judicial pronouncements

The most important judgment on Section 65B, which has been discussed in a number of other cases since, is *Anvar P.V. v. P.K. Basheer*, 2014 10 SCC 473. In this case, the Supreme Court held that an electronic record can be proved by either:

- (a) Producing the device on which the "original" electronic record is stored; or
- (b) In accordance with the procedure prescribed under Section 65B.



The Court held that if a party is not able to produce the "original" electronic record, the procedure under Section 65B is mandatory.

In this case the Court identified 5 conditions under Section 65B that an electronic record which is sought to be proved in evidence must necessarily fulfil before it can be admitted in evidence. The Court held that the electronic record must be accompanied by a certificate (commonly known as the 65B certificate), which must:

- (i) **Identify the electronic record** containing the statement;
- (ii) **Describe the manner in which the electronic record was produced;**
- (iii) **Furnish the particulars of the device** involved in the production of that record;
- (iv) Demonstrate that the information or electronic record tendered in evidence was produced by a computer/device, (a) which was **used regularly to store or process such information** in the ordinary course and (b) was, **at the relevant time, operating.**
- (v) The certificate must be signed by a person occupying a **responsible official position** in relation to the operation of the device, who must state that all the above conditions have been met, **to the best of her knowledge or belief.**

Per Section 65B, this certificate will be treated as evidence of any matter stated in the certificate.

Post *Anvar v. Basheer*, there were a number of conflicting decisions on whether a certificate under Section 65B is mandatory or not.

This confusion was however laid to rest by the Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1. In this case, the Supreme Court, while upholding *Anvar* and over-ruling all other conflicting judgments, reiterated that a **Section 65B certificate is mandatory** to prove electronic evidence.

In *Arjun Panditrao*, the appellant's election was challenged on the ground that the nomination papers were filed after the stipulated deadline. The respondents sought to prove this with the help of the CCTV footage from the office of the returning officer. Despite their best efforts to obtain a Section 65B certificate, the concerned authorities refused to furnish the same.

The Court held that a certificate under Section 65B, complying with all the pre-requisites as laid down in *Anvar*, was mandatory to prove electronic evidence. It even clarified that when the device in which the electronic record is stored **is not in the possession** of the concerned party, then the party could **apply to the Court to issue summons** to the relevant third party to furnish a Section 65B certificate.

However, in this case, the Court recognised that despite the respondents making all possible efforts, including through the High Court, to procure the Section 65B certificate, the concerned authorities had deliberately withheld the same. Given these exceptional circumstances, the Court observed that the respondents could not be asked to achieve the impossible, and relieved them of the mandatory requirement to produce a Section 65B certificate.

Therefore, **as per the law today a Section 65B certificate is mandatory for production of any electronic record in secondary form**. The only **exception** to this would be a scenario where a party has made all efforts (including approaching the judiciary) to procure a Section 65B certificate, but still finds it impossible to find one. However, such good and valid reason for failure must be presented before the court to its satisfaction.

Therefore, if you want to prove an electronically signed agreement in Court, you must ensure that when you tender your agreement in evidence (a printout or in a CD-ROM/USB device), it must be accompanied with a Section 65B certificate which fulfils the conditions as laid down in *Anvar*.

But where does one get this Section 65B certificate from?

### Who can issue a Section 65B certificate for you

Can you file a Section 65B certificate yourself? Or do you need to obtain it from the tech platform through which you are eSigning documents?

As long as the electronically signed agreement is independently accessible by you either through (i) your own platform or (ii) your account with your ASP or (iii) in your email inbox, you can provide a Section 65-B Certificate yourself!

A **sample 65B certificate** that you can use for tendering electronic agreements as evidence in Court has been annexed to this ebook.

## PROVING ELECTRONIC AGREEMENTS

Once you have filed the certificate, you **need to prove that the parties signed the agreement**. The way in which you can go about proving this depends on the mode of electronic execution you used. This requirement to prove that the signer indeed electronically signed the agreement mirrors the legal requirement applicable for physical agreements - where a witness may give evidence to prove that both parties indeed signed the agreement.

### (I) DOCUMENTS EXECUTED USING DSC OR SCHEDULE II eSIGNS

The process of proving electronic documents executed through Section 3 Digital Signatures or Schedule II eSigns is very simple. Can you guess why?

It is because of the number of presumptions carved out in their favour that we discussed in the previous chapter. Hence, documents executed using DSC or the three Schedule II eSigns:

- (i) The signature will be presumed to belong to the signer herself and not of any other person (Section 67A).
- (ii) Will be **presumed to have been concluded** between the parties (Section 85A);
- (iii) Will be **presumed to have not been altered** since affixture of the electronic signatures (Section 85B);

- (iv) The signatures will be presumed to have been affixed by the signers with the **intention of signing** or approving the document (Section 85B); and
- (v) The identification details of the signer mentioned in the **Electronic Signature Certificate will be presumed to be correct** (Section 85C).

By virtue of Section 4 of the Evidence Act, 'presumption' here means that the Court will presume such fact to be proved, unless and until it is disproved by the other party by adducing additional evidence. But given the complex technological framework of electronic signatures, it is very difficult to disprove any of these presumptions.

## **(II) DOCUMENTS AUTHENTICATED USING OTHER MODES OF ELECTRONIC EXECUTION**

Other modes of electronic execution such as email, clickwrap etc do not enjoy any presumptions under the Evidence Act. Therefore, to prove electronic documents executed using such means you will have to lead evidence to show that the parties have accepted the agreement. For example, you may lead additional evidence to prove that (i) you sent an email attaching the agreement to the other party, who either accepted it or did not deny it, or (ii) that the conduct of the other party shows that he has acted pursuant to the agreement (for example, disbursement of the loan amount pursuant to a loan agreement is sufficient to show conduct in pursuance of the agreement).

Even for virtual signatures you may have to tender such additional evidence to prove that the parties approved the agreement. However, if your technology platform provides a Secure Virtual Signature and issues an 'Audit Trail' then your job becomes a whole lot easier. An Audit Trail is an automatically generated document that captures all the details of the signing journey, such as:

- Public IP of the signing parties
- Timestamp of the signatures
- The form of authentication used by the parties
- Location and photo of the signing parties (in case this feature is provided by your technology platform)

If this Audit Trail is signed by the ASP using a secure digital signature, then it becomes a secure electronic record, and enjoys the favourable presumptions under the Evidence Act as discussed earlier.

In addition to the Audit Trail, some Secure Virtual Signatures are digitally signed by the technology platform with a secure digital signature. This act would make the document a secure electronic record. Thus, the document - from the point in time at which the secure digital signature was affixed - would enjoy the presumption of integrity laid down in Section 85B(1) of the Evidence Act.



# ANNEXURES

**ANNEXURE: IS RELIABILITY ALONE NOT A SUFFICIENT CRITERIA?**

A common misconception is that electronic signatures need not be specified in Schedule II as long as they meet the standards of **reliability** under Section 3-A.

This misconception stems from the following wording:

**3A. Electronic signature.-** (1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electric record by such electronic signature or electronic authentication technique which-

- (a) is considered reliable; and
- (b) may be specified in the Second Schedule.



The words “may be specified” are used to show that listing in the Second Schedule is optional and not mandatory.

But this is simply not true.

***May can connote optional or mandatory***

It is well established in common law that the word “may” - in law - does not by itself connote that something is optional.

In fact, the Supreme Court has, on multiple occasions ([Govindlal Chhaganlal Patel v. The Agricultural Produce Market Committee, AIR 1976 SC 273](#); [Siddheshwar Sahakari Sakhar Karkhana Ltd. and Ors. v. Commissioner of Income Tax, Kolhapur and Ors., 2004 12 SCC 1](#)) held that the word “may” can be read to be either a “directory”/optional command OR a “mandatory” command.

The broader circumstances of the statute and provision in which the word “may” is used need to be considered and scrutinized to determine whether “may” is an optional directive or a mandatory one.

The wording and circumstances of both Section 3A and the IT Act indicate that “may” is actually **mandatory** and not optional. Let’s examine how.

### Circumstance #1: Section 2(ta)

The first key circumstance is the “definition” provision for electronic signature. If you remember, Section 2(ta) says:

(ta) “**electronic signature**” means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature



Section 2(ta) is **explicitly clear** that an electronic signature is **ONLY** one of two things:

- A) An electronic technique **specified in the Second Schedule**
- B) Digital Signature

As per the definition provision, listing in the Second Schedule is mandatory. There are no words which hint at any other possibility.

Therefore if the word “may” in Section 3A were held to connote “optional” - then it would come into **direct conflict** with Section 2(ta). 3A would be directly undercutting 2(ta) - with no scope of reconciliation. An absurd situation - where one provision essentially **negates** another.

The only way we can reconcile the two provisions is if the word “may” in Section 3A were to connote “mandatory”. In this scenario, listing under Schedule II is mandatory under both 2(ta) and 3A - and there is no conflict between the two provisions.

In fact, there is also perfect positive harmony. Section 2(ta) defining what electronic signatures are **AND** Section 3A laying down **the criteria and process** for when an electronic signature can be notified by the Government.

Not convinced? There’s more

### Circumstance #2: Section 3A itself

Let’s look at the wording of the **rest** of Section 3A.

Section 3A(4) and 3A(5) lay down a clear cut procedure for listing of an electronic signature technique under the Second Schedule. We discussed this above - the Central Government can specify a technique in the Second Schedule **if it is reliable** by way of notification. This notification must then be laid before Parliament for approval.

This two-step process for listing clearly indicates that the Act envisions a level of scrutiny for Second Schedule electronic signatures:

- At one level, by the Central Government - to notify modes based on the reliability standard.
- And at another level by Parliament - to verify if the Central Government has adhered to the reliability standard prescribed under 3A.

In this scenario, if the word “may” were to be optional - it would be notionally possible for ‘electronic signatures’ to be created that would **completely bypass** the two-step scrutiny of the Government and Parliament - resulting in an ambiguous mess:

- A)** Any class not specified in Schedule II which can be deemed to be reliable by the **signer** would be as valid as a signature listed in Schedule II.
- B)** A class that is specified in Schedule II - after double scrutiny by the Central Government and Parliament. This type would be beyond ambiguity.

This would effectively render Sections 3A(4) and (5) and Schedule II COMPLETELY POINTLESS.

Here, the reliability standard would, in effect, be determined by Courts on a case-by-case basis when a document is taken for enforcement. This would lead to multiplicity of case law and Court mandated definitions of valid electronic signature types. Lots of confusion!

This absurdity does not exist if the word “may” were read to be **mandatory**. This would lead to a much simpler explanation of:

- 1) Second Schedule listing being mandatory for electronic signatures (other than digital signatures under Section 3)
- 2) Reliability being a governing criteria that is binding on the Central Government for listing signatures/techniques under Schedule II
- 3) Parliament scrutinizing whether the Government has followed the criteria

Still not convinced? Well, there’s another critical circumstance.

### Circumstance #3: Legislative Intent

In the face of absurdity resulting from a particular interpretation, legislative intent can also be relied on.

Have a look at the Summary of the Proposed Amendments laid down by the Expert Committee constituted by the Ministry of IT. Remember, it was this Committee's recommendations which were largely accepted by Parliament when drafting the Amendments.

We covered it above, but we'll repeat it here:

The Act is being made technology neutral with minimum change in the existing IT Act 2000. This has been made by amendment of Section 4 of the Act to provide for electronic signature with digital signature as one of the types of electronic signature and by enabling the details of other forms of electronic signature to be provided in the Rules to be issued by the Central Government from time to time. This is an **enabling provision** for the Central Government to exercise as and when the technology other than digital signature matures. Then there will be no need to amend the Act and the issue of rules will be sufficient. Consequently, the term digital is changed to electronic in other sections.



The above reasoning **clearly** indicates that the word “may” **needs to be read as “mandatory”**.

### Circumstance #4: Existence

There is just NO EVIDENCE of any other mode or type of electronic signing being recognized that isn't either specified in the Second Schedule OR specified under Section 3.

On the flipside, Second Schedule signatures have comprehensive regulatory codes that they are governed by.

Given this absence of any proof of existence of a Non-Second Schedule, Non-Section 3 electronic signature - one cannot help but conclude that the word “may” indeed needs to be read as mandatory.

### ***“May” is therefore mandatory***

Given the catena of circumstances above - it is clear, beyond any reasonable doubt, that the word “may” in Section 3A is a **mandatory directive**.



# **COMPENDIUM OF LEGAL PROVISIONS AND CASE LAWS**



## TABLE OF CONTENTS

### A. LEGAL PROVISIONS

#### 1. eSign

##### 1.1. Definitions

1.1.1. Affixing electronic signature

1.1.2. Digital signature

1.1.3. Electronic form

1.1.4. Electronic record

1.1.5. Electronic Signature

##### 1.2. Documents that cannot be eSigned

##### 1.3. Digital signature

##### 1.4. Electronic signature

##### 1.5. Legal recognition of electronic signatures

##### 1.6. Certifying Authority

##### 1.7. Controller of Certifying Authorities

#### 2. Other modes of electronic execution

#### 3. Secure electronic record

#### 4. Presumptions under the Evidence Act

#### 5. Proving electronic agreements in Court

### B. CASE LAWS

## PART A: LEGAL PROVISIONS

### 1. ESIGN

#### 1.1. DEFINITIONS

##### 1.1.1. Affixing electronic signature

Section 2(1)(d) of the Information Technology Act, 2000

(d) “affixing electronic signature”, with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of electronic signature;

##### 1.1.2. Digital signature

Section 2(1)(p) of the Information Technology Act, 2000

(p) “digital signature” means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

##### 1.1.3. Electronic form

Section 2(1)(r) of the Information Technology Act, 2000

(r) “electronic form” with reference to information, means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

##### 1.1.4. Electronic record

Section 2(1)(t) of the Information Technology Act, 2000

(t) “electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

**1.1.5. Electronic signature**

Section 2(1)(ta) of the Information Technology Act, 2000

**(ta)** “electronic signature” means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;

**1.2. DOCUMENTS THAT CANNOT BE ESIGNED**

First Schedule of the Information Technology Act, 2000

**DOCUMENTS OR TRANSACTIONS TO WHICH THE ACT SHALL NOT APPLY**

Sl. No.	SECURE VIRTUAL SIGNATURES
1.	A negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881 (26 of 1881)
2.	A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882 (7 of 1882)
3.	A trust as defined in section 3 of the Indian Trusts Act, 1882 (2 of 1882)
4.	A Will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 (39 of 1925) including any other testamentary disposition by whatever name called.
5.	Any contract of the sale of conveyance of immovable property or any interest in such property

**1.3. DIGITAL SIGNATURE**

Section 3 of the Information Technology Act, 2000

**3. Authentication of electronic records.** - (1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

*Explanation.-* For the purposes of this sub-section, “hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

- (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
- (b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

#### **1.4. ELECTRONIC SIGNATURE**

##### Section 3A of the Information Technology Act, 2000

**3A. Electronic signature.-** (1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electric record by such electronic signature or electronic authentication technique which-

- (a) is considered reliable; and
- (b) may be specified in the Second Schedule.

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if-

- (a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;
- (b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
- (c) any alteration to the electronic signature made after affixing such signature is detectable;

- (d) any alteration to the electronic signature made after affixing such signature is detectable; and
- (e) it fulfils such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule:

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.

Second Schedule of the Information Technology Act, 2000

**ELECTRONIC SIGNATURE OR ELECTRONIC AUTHENTICATION TECHNIQUE AND PROCEDURE**

SL. NO.	DESCRIPTION	PROCEDURE
1.	E-authentication technique using Aadhaar or other e-KYC services	<p>Authentication of an electronic record by e-authentication Technique which shall be done by-</p> <p>(a) the applicable use of e-authentication, hash, and asymmetric crypto system techniques, leading to issuance of Digital Signature Certificate by Certifying Authority</p> <p>(b) a trusted third party service by subscriber's key pair-generation, storing of key pairs and creation of digital signature provided that the trusted third party shall be offered by the certifying authority. The trusted third party shall send application form and certificate signing request to the Certifying Authority for issuing a Digital Signature Certificate to the subscriber.</p>

		<p>(c) Issuance of Digital Signature Certificate by Certifying Authority shall be based on e-authentication, particulars specified in Form C of Schedule IV of the Information Technology (Certifying Authorities) Rules, 2000, digitally signed verified information from Aadhaar or other e-KYC services and electronic consent of Digital Signature Certificate applicant.</p> <p>(d) The manner and requirements for e-authentication shall be as issued by the Controller from time to time.</p> <p>(e) The security procedure for creating the subscriber's key pair and other e-KYC services shall be in accordance with the e-authentication guidelines issued by the Controller.</p> <p>(f) The standards referred to in rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 shall be complied with, in so far as they relate to the certification function of public key of Digital Signature Certificate applicant.</p> <p>(g) The manner in which the information is authenticated by means of digital signature shall comply with the manner and standards specified in rules 3 to 12 of the Digital Signature (End Entity) Rules, 2015 in so far as they relate to the creation, storage, and verification of Digital Signature.</p>
<p>2.</p>	<p>E-authentication technique and procedure for creating and accessing subscriber's signature key facilitated by trusted third party</p>	<p>Authentication of an electronic record by e-authentication technique which shall be done by-</p> <p>(a) the applicable use of e-authentication, hash, and asymmetric crypto system techniques, leading to issuance of Digital Signature Certificate by Certifying Authority, provided that Certifying Authority shall ensure the subscriber identity verification, secure storage of the keys by trusted third party and subscriber's sole authentication control to the signature key.</p>

(b) Identity verification of Digital Signature Certificate applicant shall be in accordance with the Identity Verification Guidelines issued by Controller from time-to-time.

(c) The requirement to operate as trusted third party shall be specified under e-authentication guidelines issued by the Controller.

(d) a trusted third party shall

(i) facilitate Identity verification of Digital Signature Certificate Applicant;

(ii) establish secure storage for subscriber to have sole control for creation and subsequent usage of subscriber's signature key by sole authentication of subscriber;

(iii) facilitate key pair-generation, secure storage of subscriber's signature key and facilitate signature creation functions;

(iv) facilitate the submission of DSC application form and certificate signing request to the Certifying Authority for issuing a Digital Signature Certificate to the DSC applicant, and

(v) facilitate revocation of Digital Signature Certificate and destruction of subscriber's signature key.

(e) Issuance of Digital Signature Certificate shall be based on verification of credentials of Digital Signature Certificate applicant by Certifying Authority as per the provisions of the Information Technology Act and Rules made thereunder.

(f) The manner and requirements for authentication and storage of keys shall be as issued by the Controller from time to time under *e-authentication guidelines*

(g) The security procedure for creating the subscriber's key pair shall be in accordance with the e-authentication guidelines issued by the Controller.

		<p>(h) The standards referred to in rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 shall be complied with, in so far as they relate to the creation function of public key of Digital Signature Certificate applicant.</p> <p>(i) The manner in which information is authenticated by means of digital signature shall comply with the manner and standards specified in rule 3 to 12 of Digital Signature (End Entity) Rules, 2015 in so far as they relate of the creation, storage and verification of Digital Signature.</p>
--	--	---

### 1.5. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES

Section 5 of the Information Technology Act, 2000

**5. Legal recognition of electronic signatures** - Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.

Explanation.- For the purposes of this section, “signed”, with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of this hand written signature or any mark on any document and the expression “signature” shall be construed accordingly.

### 1.6. CERTIFYING AUTHORITY

Section 35 of the Information Technology Act, 2000

**35. Certifying authority to issue Electronic Signature Certificate.**- (1) Any person may make an application to the Certifying Authority for the issue of an Electronic Signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:

Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Electronic Signature Certificate or for reasons to be recorded in writing reject the application:

Provided that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

## 1.7. CONTROLLER OF CERTIFYING AUTHORITIES

### Section 17 of the Information Technology Act, 2000

**17. Appointment of Controller and other officers.**—(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification, appoint such number of Deputy Controllers, Assistant Controllers, other officers and employees as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers, Assistant Controllers, other officers and employees shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

## 2. OTHER MODES OF ELECTRONIC EXECUTION

### Section 10 of the Indian Contract Act, 1872

**10. What agreements are contracts.-** All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void.

### Section 14 of the Indian Contract Act, 1872

**14. "Free consent" defined.-** Consent is said to be free when it is not caused by-

- (1) coercion, as defined in section 15, or
- (2) undue influence, as defined in section 16, or
- (3) fraud, as defined in section 17, or
- (4) misrepresentation, as defined in section 18, or
- (5) mistake, subject to the provisions of section 20, 21 and 22.

Consent is said to be so caused when it would not have been given but for the existence of such coercion, undue influence, fraud, misrepresentation or mistake

### Section 13 of the Indian Contract Act, 1872

**13. "Consent" defined.-** Two or more persons are said to consent when they agree upon the same thing in the same sense.

### Section 3 of the Indian Contract Act, 1872

**3. Communication, acceptance and revocation of proposals.-** The communication of proposals, the acceptance of proposals, and the revocation of proposals and acceptances, respectively, are deemed to be made by an act or omission of the party proposing, accepting or revoking by which he intends to communicate such proposal, acceptance or revocation, or which has the effect of communicating it.

Section 10A of the Indian Contract Act, 1872

**10A. Validity of contracts formed through electronic means.-** Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic records, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

### 3. SECURE ELECTRONIC RECORD

Section 14 of the Information Technology Act, 2000

**14. Secure electronic record.-** Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Section 16 of the Information Technology IT Act, 2000

**16. Security procedures and practices.-** The Central Government may, for the purposes of sections 14 and 15, prescribe the security procedures and practices:

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

Rule 3 of the Information Technology (Security Procedure) Rules, 2004

**3. Secure electronic record.-** An electronic record shall be deemed to be a secure electronic record for the purposes of the Act if it has been authenticated by means of a secure digital signature.

Rule 4 of the Information Technology (Security Procedure) Rules, 2004

**4. Secure digital signature.-** A digital signature shall be deemed to be a secure digital signature for the purposes of the Act if the following procedure has been applied to it, namely:-

- (a) that the smart card or hardware token, as the case may be, with cryptographic module in it, is used to create the key pair;

- (b) that the private key used to create the digital signature always remains in the smart card or hardware token as the case may be;
- (c) that the hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system;
- (d) that the information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature;
- (e) that the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person;
- (f) that the standards referred to in rule 7 or rule 12 of the Digital Signature (End Entity) Rules, 2015 have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and
- (g) that the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated.

#### Section 15 of the Information Technology Act, 2000

**15. Secure electronic signature.** - An electronic signature shall be deemed to be a secure electronic signature if-

- (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
- (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation.- In case of digital signature, the "signature creation data" means the private key of the subscriber.

## **4. PRESUMPTIONS UNDER THE EVIDENCE ACT**

#### Section 85A of the Indian Evidence Act, 1872

**85A. Presumption as to electronic agreements.-** The Court shall presume that every electronic record purporting to be an agreement containing the electronic signature of the parties was so concluded by affixing the electronic signature of the parties.

Section 85B of the Indian Evidence Act, 1872

**85B. Presumption as to electronic records and electronic signatures.-** (1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure electronic signature, the Court shall presume unless the contrary is proved that—

- (a) the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record;
- (b) except in the case of a secure electronic record or a secure electronic signature, nothing in this section shall create any presumption, relating to authenticity and integrity of the electronic record or any electronic signature.

Section 85C, Indian Evidence Act, 1872

Section 85C of the Indian Evidence Act, 1872

**85C. Presumption as to Electronic Signature Certificates.-** The Court shall presume, unless contrary is proved, that the information listed in a Electronic Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

Section 90A of the Indian Evidence Act, 1872

**90A. Presumption as to electronic records five years old.-** Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the electronic signature which purports to be the electronic signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explanation. – Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.

## 5. PROVING ELECTRONIC AGREEMENTS IN COURT

### Section 62 of the Indian Evidence Act, 1872

**62. Primary evidence.** -- Primary evidence means the document itself produced for the inspection of the Court.

Explanation 1. --Where a document is executed in several parts, each part is primary evidence of the document. Where a document is executed in counterpart, each counterpart being executed by one or some of the parties only, each counterpart is primary evidence as against the parties executing it.

Explanation 2. -- Where a number of documents are all made by one uniform process, as in the case of printing, lithography or photography, each is primary evidence of the contents of the rest; but, where they are all copies of a common original, they are not primary evidence of the contents of the original.

#### *Illustration*

A person is shown to have been in possession of a number of placards, all printed at one time from one original. Any one of the placards is primary evidence of the contents of any other, but no one of them is primary evidence of the contents of the original.

### Section 64 of the Indian Evidence Act, 1872

**64. Proof of documents by primary evidence.** -- Documents must be proved by primary evidence except in the cases hereinafter mentioned

### Section 64 of the Indian Evidence Act, 1872

**65. Cases in which secondary evidence relating to documents may be given.** -- Secondary evidence may be given of the existence, condition or contents of a document in the following cases: --

- (a) when the original is shown or appears to be in the possession or power -- of the person against whom the document is sought to be proved, of any person out of reach of, or not subject to, the process of the Court, or of any person legally bound to produce it, and when, after the notice mentioned in section 66, such person does not produce it;
- (b) when the existence, condition or contents of the original have been proved to be admitted in writing by the person against whom it is proved or by his representative in interest;

- (c) when the original has been destroyed or lost, or when the party offering evidence of its contents cannot, for any other reason not arising from his own default or neglect, produce it in reasonable time;
- (d) when the original is of such a nature as not to be easily movable;
- (e) when the original is a public document within the meaning of section 74;
- (f) when the original is a document of which a certified copy is permitted by this Act, or by any other law in force in India to be given in evidence;
- (g) when the originals consist of numerous accounts or other documents which cannot conveniently be examined in Court and the fact to be proved is the general result of the whole collection.

In cases (a), (c) and (d), any secondary evidence of the contents of the document is admissible. In case (b), the written admission is admissible.

In case (e) or (f), a certified copy of the document, but no other kind of secondary evidence, is admissible.

In case (g), evidence may be given as to the general result of the documents by any person who has examined them, and who is skilled in the examination of such documents.

#### Section 65B of the Indian Evidence Act, 1872

**65B. Admissibility of electronic records.** -- (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely: --

- (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
- (b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
- (c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly

or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether--

(a) by a combination of computers operating over that period; or

(b) by different computers operating in succession over that period; or

(c) by different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, --

(a) identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section, --

(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation. --For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived therefrom by calculation, comparison or any other process.

## PART B: CASE LAWS

### 1. *Trimex International FZE, Dubai v. Vedanta Aluminium Limited*, (2010) 3 SCC 1

In this case, the Supreme Court upheld the validity of a contract entered into via an exchange of emails with the binding observation:

*“Once the contract is concluded orally or in writing, the mere fact that a formal contract has to be prepared and initialed by the parties would not affect either the acceptance of the contract so entered into or implementation thereof, even if the formal contract has never been initialed.”* (Paragraph 9)

### 2. *Ambalal Sarabhai Enterprise Limited v. KS Infraspace LLP Limited*, (2020) SCC OnLine 1

In this case, the main point of contention was whether there was a concluded contract between the parties. While the plaintiff argued that there was a concluded contract between him and the defendant regarding sale of certain immovable property, the defendant denied that the contract *“did not attain finality but remained at the stage of discussions only.”*

The Supreme Court made the following observation while examining the validity of an eContract which was concluded over an exchange of emails and WhatsApp:

*“The Whatsapp messages which are virtual verbal communications are matters of evidence with regard to their meaning...The emails and WhatsApp messages will have to be read and understood cumulatively to decipher whether there was a concluded contract or not”*

While this observation tells us that contracts can be concluded through electronic means such as email, it also highlights the pitfalls associated with relying on emails as a method of electronic execution. The Supreme Court held the contract to be invalid in this case as the nature and language of the correspondences shared between the parties did not directly equate to affirmation. In the Court’s opinion, calling an agreement that was being negotiated between the parties the *“final draft”*, *“cannot be determinative by itself of a concluded contract.”*

### **3. *Anvar P.V. v. P.K. Basheer*, 2014 10 SCC 473**

In this case, the Supreme Court held that an electronic record can be proved by either:

- (a) Producing the device on which the “original” electronic record is stored; or
- (b) In accordance with the procedure prescribed under Section 65B.

The Court held that if a party is not able to produce the “original” electronic record, the procedure under Section 65B is mandatory.

In this case the Court identified 5 conditions under Section 65B that an electronic record which is sought to be proved in evidence must necessarily fulfil before it can be admitted in evidence. The Court held that the electronic record must be accompanied by a certificate (commonly known as the 65B certificate), which must:

- (i) Identify the electronic record containing the statement;
- (ii) Describe the manner in which the electronic record was produced;
- (iii) Furnish the particulars of the device involved in the production of that record;
- (iv) Demonstrate that the information or electronic record tendered in evidence was produced by a computer/device, (a) which was used regularly to store or process such information in the ordinary course and (b) was, at the relevant time, operating.
- (v) The certificate must be signed by a person occupying a responsible official position in relation to the operation of the device, who must state that all the above conditions have been met, to the best of her knowledge or belief.

### **4. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1**

In this case, the Supreme Court, while upholding *Anvar* and over-ruling all other conflicting judgments, reiterated that a Section 65B certificate is mandatory to prove electronic evidence.

In *Arjun Panditrao*, the appellant’s election was challenged on the ground that the nomination papers were filed after the stipulated deadline. The respondents sought to prove this with the help of the CCTV footage from the office of the returning officer. Despite their best efforts to obtain a Section 65B certificate, the concerned authorities refused to furnish the same.

The Court held that a certificate under Section 65B, complying with all the pre-requisites as laid down in *Anvar P.V. v. P.K. Basheer*, 2014 10 SCC 473, was mandatory to prove electronic evidence. It even clarified that when the device in which the electronic record is stored is not in the possession of the concerned party, then the party could apply to the Court to issue summons to the relevant third party to furnish a Section 65B certificate.

However, in this case, the Court recognised that despite the respondents making all possible efforts, including through the High Court, to procure the Section 65B certificate, the concerned authorities had deliberately withheld the same. Given these exceptional circumstances, the Court observed that the respondents could not be asked to achieve the impossible, and relieved them of the mandatory requirement to produce a Section 65B certificate.



# **SAMPLE 65B CERTIFICATE**

**INDICATIVE SAMPLE CERTIFICATE BY WAY OF AFFIDAVIT UNDER  
SECTION 65-B OF THE INDIAN EVIDENCE ACT, 1872**

I, **[Insert Name]**, **[Insert Position]** of the **[Insert Name of the Party abovenamed]** having my office at \_\_\_\_\_, do hereby solemnly affirm and state as under:

Responsible Official  
With Knowledge

1. I state that I have annexed a printout of the Agreement dated **[Insert Date]** between **[Party 1]** and **[Party 2]**, as Annexure '\_\_\_' to my Affidavit of Evidence.

Identifying the  
Electronic Record

2. The Agreement is stored in account of **[Insert name of the Party]** on the domain *www.leegality.com* (hereinafter "**Leegality**"). The said account is accessible through the login ID **[Insert login ID]**, and is duly secured by a password.

3. I say that Leegality is a service provider that permits parties to execute agreements in the electronic form. The agreements so executed are stored on Leegality and are accessible through the "account" of such the concerned party on Leegality.

Manner in which  
Electronic Record  
was produced

4. A copy of the Agreement was downloaded by me from the aforesaid Leegality account of **[Insert name of the Party]** by using a computer, manufactured by **[Insert name of manufacturer]** and bearing Serial No. **[Insert Sr. No]**, which is used by **[Insert name of the Party]** in the ordinary course of business. The said computer was used by me to procure a print-out of the said Agreement through a printer, manufactured by **[Insert name of manufacturer]** and bearing Serial No. **[Insert Sr. No]** used by **[Insert name of the Party]** in the ordinary course of business.

Furnish Particulars  
of Device & Show  
Regular Use and  
Proper Operation of  
Computer

6. The aforesaid account has been used regularly by **[Insert name of the Party]** in order to execute agreements in the electronic form. To the best of my knowledge and belief, the aforesaid account, the aforesaid computer and printer have been operating properly since the date of creation and have not suffered from any defects that may affect the electronic record or the accuracy of its contents.

Show regular use  
and proper operation  
of computer

7. I have also tendered a print-out of the Audit Trail , available on Leegality as Annexure \_\_\_ to my Affidavit of Evidence. This Audit Trail is automatically generated by Leegality for every agreement executed through the said website.

8. I have accessed the said Audit Trail using my aforementioned computer and printed the same using my aforementioned printer.

9. I confirm that the contents of the print outs of the Audit Trail are identical to the original stored on Leegality. I hereby certify that these are true copies of the electronic records that were viewed on my computer.

10. The aforesaid computer has been used regularly by **[Name of the Party]** to access Leegality to execute agreements in the electronic form, as also to regularly access websites. The aforesaid computer has been operating properly since the date of its purchase and has not suffered from any defects that may affect the electronic record or the accuracy of its contents.

Show regular use  
and proper operation  
of computer

11. The aforesaid printer was operating properly on the date when the print outs were taken and does not suffer from any defects that may affect the print outs of the electronic record or the accuracy of its contents.

Show regular use  
and proper operation  
of computer

12. The present certificate may be taken to be in compliance with the requirements under the Indian Evidence Act, 1872.

Solemnly affirmed at \_\_\_\_\_ )

This \_\_\_ day of \_\_\_\_\_ )

Before me,



**LAWS OF eSIGN (1<sup>ST</sup> EDITION, MARCH 2022)**

© Leegality Publications

## **Connect With Us**

**Call:** +91 011 4117 0704

**mail:** [enquiry@leegality.com](mailto:enquiry@leegality.com)

**Web:** [www.leegality.com](http://www.leegality.com)

**Social:** @leegality  