



Sample 65B
Certificate
Inside

How to prove electronic agreements in Court:

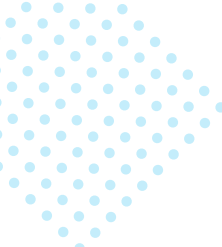
DECODING THE LAW ON SECTION 65B CERTIFICATES

(updated with the latest Supreme Court Judgement)



VINODINI SRINIVASAN

Advocate, Bombay High Court



How to prove electronic agreements in Court:

DECODING THE LAW ON SECTION 65B CERTIFICATES

(updated with the latest Supreme Court Judgement)

Vinodini Srinivasan

Advocate, Bombay High Court

BA LL.B (Hons.), National Law School of India University, Bangalore



Leegality Publications

© 2020

contact@leegality.com

#444, Phase III, Udyog Vihar III, Sector 18, Gurugram, Haryana 122008





ABOUT THE AUTHOR

Vinodini Srinivasan graduated from NLSIU Bangalore in 2014, and is an Advocate at the Bombay High Court. She was, previously, a Senior Associate at Keystone Partners, Mumbai and a Business Analyst at McKinsey & Co.



She can be reached at vinodinisrinivasan@gmail.com

Introduction	5
I. Brief Background on Section 65-B of the Indian Evidence Act	6
II. The position of law on Section 65B before Arjun Panditrao	9
III. The Judgment in Arjun Panditrao	10
IV. The Stage at Which a Section 65-B Certificate Should be Filed	12
V. Implications of Arjun Panditrao for electronic agreements	12
VI. Proving an Aadhaar eSigned/ DSC Signed/ Doc Signer Signed Agreement in Court.	13
VII. Proving agreements that have been authenticated via phone/ email	14
VIII. Other Presumptions that can be accorded to eSigned Documents	16
APPENDIX A: Sample 65B Certificate	17
APPENDIX B: Section 65B FAQs for Leegality Agreements	19



WHAT IS THIS BOOK ABOUT?

The recent judgment of three judges of the Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) has once again brought to the fore questions on how electronic records must be proved in Court. In this primer, we have attempted to provide a brief overview of the law on **Section 65B Certificates and proving your electronic agreements in Court.**



¹In this Primer, we have confined ourselves to the issues you may encounter in civil/ commercial proceedings.

I. Brief Background on Section 65-B of the Indian Evidence Act

The discussion on proving electronic documents has almost become synonymous with *Section 65-B of the Indian Evidence Act 1872* ("**Evidence Act**").

A good starting point to understand this Section is to look at the general law on how paper-based agreements may be proved. As a rule,

paper-based agreements have to be proved by producing the original in Court. It is only in exceptional circumstances, such as when the original has been lost or destroyed, that "secondary evidence" such as a photocopy, may be used.

Evidence Act provisions to prove paper-based agreements

Section 64 of the Evidence Act says that a document must be proved by primary evidence, except in cases hereinafter mentioned. Section 62 of the Act clarifies that primary evidence means the document itself.

Section 65 lays out the cases where secondary evidence (such as photocopies, certified copies etc) may be given. This includes cases where:

- (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, 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 this Act, or by any other law in force;
- (g) when the originals consists 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.

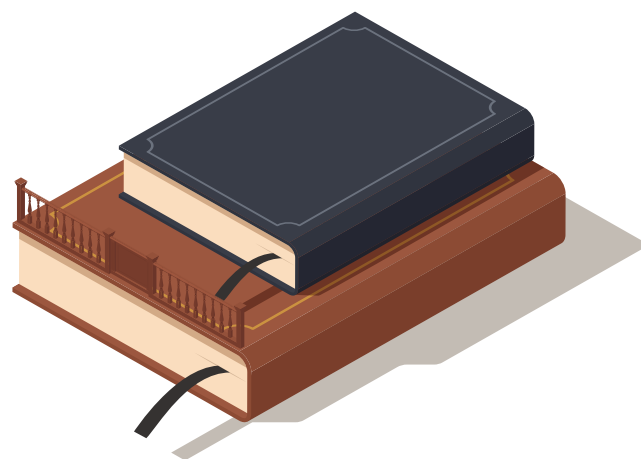
In cases (a), (c) and (d), any secondary evidence of the contents of the document is admissible.

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.

The general law places great weight on producing original documents in Court. This can be cumbersome for electronic records, where the original may be on remote servers, or multiple computers, or a phone etc.

Section 65-B of the Evidence Act relieves parties of the obligation to bring the device containing the “original record” to Court and tender it in evidence. Instead, it permits parties to produce a copy of the record in the form of a print-out, USB Drive, CD-ROM, so long as they can demonstrate the integrity and authenticity of the document they are producing.

The most important judgment on Section 65-B of the Evidence Act is *Anwar v. Basheer* (2014). In *Anwar*, the Supreme Court held that an electronic record can be proved in one of two ways (i) by producing the device on which “original” electronic record is stored or, (ii) in accordance with the procedure prescribed under Section 65-B. Thus, unless and until the “original” electronic record itself is brought to Court, the Court held that the procedure under Section 65-B is mandatory.



In *Anwar v. Basheer*, the Court identified the 5 conditions that an electronic record must meet under S. 65B before it can be admitted in evidence. These 5 conditions are reproduced here:



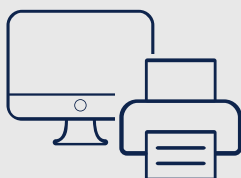
Identify the electronic record

The electronic record must be accompanied by a certificate which **identifies the electronic record** containing the statement;



Manner in which the electronic record was produced

The certificate must **describe the manner in which the electronic record was produced**



Identify the device

The certificate must **furnish the particulars of the device** involved in the production of that record



Show regular use and proper operation of computer

The certificate must demonstrate that the information or electronic record tendered in evidence was produced by a computer/ device, **(i) which was used regularly to store or process such information in the ordinary course and (ii) was, at the relevant time, operating.**



By a responsible official with knowledge

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.**

II. The position of law on Section 65B before Arjun Panditrao

Prior to the decision in *Arjun Panditrao*, there were a series of conflicting judgments on whether a Certificate under Section 65-B was mandatory to prove electronic evidence:

Navjot Sandhu: The first such judgment was the famous parliamentary attack case, *State (NCT of Delhi) v. Navjot Sandhu (2005)*. In this case, Supreme Court held that the procedure under Section 65B is not mandatory, and that the procedure prescribed for giving “secondary evidence” of physical documents may also be followed for electronic records.

Anwar: *Anwar*, specifically over-ruled *Navjot Sandhu* and held that unless the “original electronic record” itself was produced in Court, a certificate under Section 65B was mandatory to prove electronic records.

Tomaso Bruno: However, despite *Anwar* expressly overruling the proposition in *Navjot Sandhu*, the Supreme Court in *Tomaso Bruno v. State of Uttar Pradesh (2015)*, once again cited with approval the judgment in *Navjot Sandhu*, where it was held that electronic evidence can be proved even without following Section 65-B of the Evidence Act.

Shafhi Mohammed: In practice, parties also encountered difficulties in producing a certificate of the nature contemplated in *Anwar*, when they were not in possession of the device generating the relevant electronic record.

For instance, a party who wants to produce call detail records - which are stored on the servers of a telecom service provider and not made independently accessible by third parties. In such cases, if the call records were to be produced in Court - the telecom service provider, and not the party, would have to furnish a certificate under Section 65B. With this scenario in mind, the Supreme Court in *Shafhi Mohammed v. State of Himachal Pradesh (2018)* held that a Section 65B certificate is not mandatory and could be relaxed where the interests of justice so required. A specific relaxation was granted in cases where the relevant device was not in the possession of the party leading electronic evidence at the relevant time.

It was in the backdrop of the cases described above that the Supreme Court delivered its latest verdict in *Arjun Panditrao*. This judgment reiterated that a Section 65-B is **mandatory** in order to prove electronic evidence, and **upheld Anwar**, while over-ruling all other conflicting judgments. The next section analyses the decision in *Arjun Panditrao*.

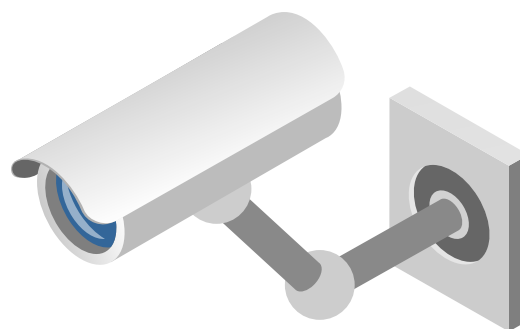
III. The Judgment in *Arjun Panditrao*

In *Arjun Panditrao*, the Appellant's election was challenged on the ground that he had filed his nomination papers after the stipulated time of 3 pm. The Respondents sought to prove this fact through CCTV footage of the office of the Returning Officer. However, despite the Respondent's best efforts to obtain a Section 65-B certificate from the concerned authorities, the concerned authorities refused to furnish the certificate.

In deciding the case, the Supreme Court held that the decision in *Tomaso Bruno* was bad in law and over-ruled *Shafhi Mohammed*. The Court reiterated the law as laid down in *Anwar*, and held that a certificate under Section 65-B, complying with all the pre-requisites laid down by *Anwar*, was mandatory to prove electronic evidence.

The Court clarified that even where the electronic record was generated by a device which was not in the possession of the concerned party, the party could apply to the Court to issue summons to the relevant third party to furnish the Section 65B certificate.

However, in the case before it, the Court recognised that although the Respondents had made all possible efforts, including through the High Court, to procure the Section 65-B certificate, the concerned authorities had deliberately withheld the same. Observing that the Respondents could not be asked to achieve the impossible, and given the exceptional



circumstances, the Court relieved them of the mandatory requirement to produce a certificate under Section 65-B.

Therefore, as per *Arjun Panditrao* - which holds the field today - a Section 65-B is **mandatory** for production of any electronic record in a secondary form. The **only** scenario in which a Section 65-B requirement can be waived is in the event that a party has made all efforts (including judicial) to procure a 65-B but then finds it **impossible** to produce one.

Chronology of Landmark Supreme Court Judgements regarding Section 65B Certificates

State of NCT v Navjot Sandhu

Section 65B is **not mandatory** for proving electronic records. Electronic Records can be proven in accordance with Section 65 of the Evidence Act also

2005

Tomaso Bruno v. State of Uttar Pradesh

Approved Navjot Sandhu, where it was held that electronic evidence can be proved without following the procedure under S. 65-B.

2015

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal

Section 65 B certificate is mandatory even when device is not in possession of party seeking to produce it.

2020

Anwar v. Basheer

Section 65 B is **mandatory** for proof of an electronic record in any form other than the original form.

2014

Shafhi Mohammed v. State of Himachal Pradesh

Section 65 B certificate is **not mandatory** and requirement could be relaxed in the interests of justice

2018

IV. The Stage at Which a Section 65-B Certificate Should be Filed

The Section 65-B Certificate must be filed when the party wants the document to be taken on record, marked as an Exhibit and read in evidence. In *Anwar*, the Supreme Court held as under:

"15. ..Most importantly, such a certificate must accompany the electronic record like computer printout, Compact Disc (CD), Video Compact Disc, pen drive etc, pertaining to which a statement sought to be given in evidence, when the same is produced in evidence"

The Supreme Court in *Arjun Panditrao*, also reiterates this position.

Depending on the Court your case is before, this stage of "evidence" begins when the Court asks parties to file their compilation/statement of documents (for the purpose of marking of documents) or when the Court directs parties to file their Affidavits of Evidence along with their compilation of documents.

V. Implications of *Arjun Panditrao* for electronic agreements

The key takeaway for electronic agreements is that you must ensure that when you tender your agreement and/or Audit Trail (if provided) in evidence, you file a suitable certificate under Section 65B, setting out the 5 Conditions identified by *Anwar*. An indicative draft of a Section 65B certificate is available [here](#).

A common concern is whether you can file a Section 65B Certificate yourself, or whether you need to obtain it from the document execution service/platform through which you have electronically signed the document.

As long as the electronic agreement is independently accessible by you either through (i) your own Platform or (ii) your account with your document execution platform or (iii) in your email inbox, you can provide a Section 65-B

Certificate yourself.

Producing a valid certificate under Section 65-B certificate is only the first step to proving an electronic agreement. In addition, you will be required to prove that the parties have signed/accepted the agreement. This mirrors the requirement in law for physical agreements, where the evidence of a witness has to be led to prove the signature of both parties to the agreement.

The mode of proof varies depending on whether you have opted for Aadhar e-sign/ DSC or other modes of electronic authentication (such as verification via phone/ email). In Sections VI and VII, we discuss how the execution of electronic agreements may be proved.

VI. Proving an Aadhaar eSigned/ DSC Signed/ Doc Signer Signed Agreement in Court

Should you opt for an Aadhaar e-sign/DSC Sign/Doc Signer, the process of proving an agreement becomes very simple, and enjoys several presumptions. Both Aadhaar esign and DSC Signs are electronic signatures under Section 2(ta) of Information Technology Act, 2000 ("**IT Act**"). Under 85A of the Indian Evidence Act, the Court "shall presume" that an electronic agreement containing the electronic signature of the parties was so concluded by affixing the electronic signature of the parties.

Aadhaar eSign, DSC Signs and Doc Signer eSigns are also "secure electronic signatures" under Section 15 of the IT Act. This entitles them to a rebuttable presumption under Section 85-B(2) of the Evidence Act, which states that the Court shall presume that secure electronic signatures were affixed by parties with the intention of signing or approving the electronic record. Such presumptions can make it significantly harder for anyone to challenge or deny their Aadhaar e-sign/ DSC/Doc Signer.

Further, an Aadhaar eSign/DSC/Doc Signer is affixed to a document is considered a "security procedure" for the document, it makes the document a secure electronic record under the IT Act. Such a secure document cannot be tampered with as any modifications/ changes become apparent on a mere perusal of the document, and are also tracked. Due to the enhanced security features of such documents, Section 85-B(2) of the Evidence Act presumes that any "secure electronic record" has not been altered/ tampered with after it was signed. This makes it very difficult for anyone to claim that the document being relied upon has been altered or tampered with.



VII. Proving agreements that have been authenticated via phone/ email

Other forms of electronic authentication like click-wrap, or authentication via email/ phone are valid and enforceable in law. However, they do not enjoy the additional presumptions that are accorded to Aadhaar eSign/DSC Sign/Doc Signer, under the Evidence Act. In such cases, you will have to lead evidence to show that the parties have accepted the agreement.

- a. the IP address of the parties
- b. when and how both parties electronically authenticated the document.
- c. whether they authenticated their identity through an OTP shared on their email or their phone
- d. the location and photo of the signing parties (where this feature has been enabled)

In order to simplify the process of proving the execution of the agreement, platforms often issue an “Audit Trail” for agreements. The Audit Trail is an automatically generated document that captures the signing journey of the document. Some illustrative examples of details that can be captured include:

The question is whether the acceptance of the agreement can be proved merely by producing the Audit Trail (along with a valid 65B certificate). Conventional evidence law would, ordinarily, also require a witness who has personal knowledge of the facts set out in the Audit Trail to step into the box and lead evidence of the truth of its contents.



However, in *Kundan Singh v. State*, the Delhi High Court dispensed with such a requirement for documents that are generated automatically, while recognising that no person can be said to really have “personal knowledge” of their contents. The Court held as follows:

“56. Electronically generated record is entirely a product of functioning of a computer system or computer process, like call record details or a report generated on a fax, which shows the number from and to which the fax were sent, time etc. is generated electronically. It does not contain any assertion. Therefore, as noticed above, it is not hearsay. These are not writings made by any person... Normally non-assertive conduct is more reliable, provided that there has been no fraud and interpolation in the preparation of the record. Computer generated telephone records are not similar to a statement made by a human declarant and therefore, cannot be treated as hearsay and the credibility and evidentiary value is determined on the reliability and accuracy of the process involved. Ergo, in these cases when the conditions of Section 65B are satisfied, the probative value or weight can be substantial of course, subject to verification as to the credibility and integrity of the contents.”

Kundan Singh is undoubtedly a step in the right direction, as it permits the truth of the contents of automatically generated documents such as the Audit Trail to be proved by producing the relevant document along with a Section 65-B certificate, without any further oral evidence being led.

However, the jurisprudence in this area is still nascent. No occasion has arisen as yet for a Courts to consider *Kundan Singh* in the context of Audit Trails and how they may be proved. It is, thus, advisable to also lead oral evidence in addition to the Audit Trail to prove the execution of the agreement. For instance, you may step into the box to prove that (i) you sent an email attaching the executed agreement to the other party, who either accepted it/ did not deny it or that (ii) the conduct of the other party clearly demonstrates that he has acted pursuant to the agreement. In everyday commercial transactions, it is highly likely you will have several examples of such conduct that shows that the other party has accepted the agreement, making it extremely difficult for the other party to deny the Agreement. For instance, if you are a Bank, disbursement of the loan pursuant to an agreement would itself be conduct in pursuance of the agreement.

VIII. Other Presumptions that can be accorded to eSigned Documents

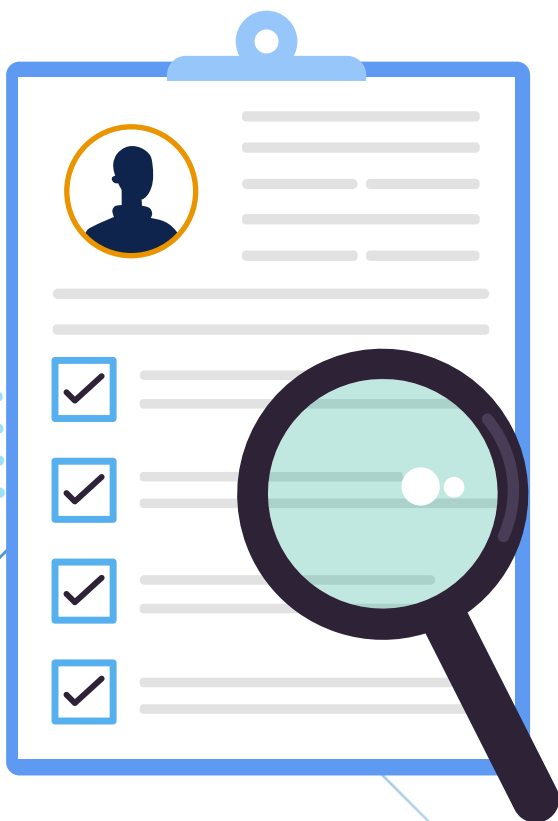
To reiterate, Aadhaar eSigned/DSC/ Doc Signer signed documents are “**secure electronic records**” under the IT Act. Every alteration/change made to such a document is tracked, and thus, such documents cannot be tampered with. As a result, such documents are entitled to a presumption under Section 85B of the Evidence Act that they have not been altered since the specific point of time to which their secure status relates.

Ordinarily, documents signed by other electronic means are not secure electronic records. Similarly, several audit/transactional trails are also not secure electronic records. This may make them susceptible to challenges and lead to enforcement hassles.

However, this problem can be overcome easily if the document authenticated by other electronic means is **also** signed by the document execution platform through a **secure digital signature**. This would make the document a **secure electronic record**. Similarly, if the Audit Trail is signed by the document execution platform through a **secure digital signature** - the Audit Trail would also become a **secure electronic record**. Thus, it would become readily evident if the electronically authenticated document/Audit Trail has been altered or tampered with.

It is important to note that digital signing of the document/Audit Trail by the document execution platform does not make that platform a party to the agreement or document. It is only a “security procedure” as provided for by the IT Act to secure the electronic record

Therefore, in cases where an Audit Trail is generated or where documents are signed in ways other than Aadhaar eSign/DSC Sign/Doc Signer - a Digital Signature on the document and Audit Trail by the document execution platform would greatly strengthen enforceability.



APPENDIX A

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

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

5. I have compared the contents of the aforesaid Agreement stored on the computer as well as the print outs of the Agreement annexed to my Affidavit of Evidence with the original stored on Leegality and confirm that its contents are identical to the original. The original Agreement is retained in its original form on Leegality, and may be accessed through the login ID **[Insert login ID]**

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,

APPENDIX B

SECTION 65B FAQs FOR LEEGALITY SIGNED AGREEMENTS

1. As a business seeking to enforce electronic agreements in Court, what do I need to know about how electronic agreements are proved?

There are two steps to proving an electronic agreement (1) you have to furnish a valid certificate under Section 65-B of the Evidence Act (2) you have to prove that the parties have signed/accepted the agreement.

The Supreme Court in the landmark judgment of *Anwar v. Basheer* identified the following 5 conditions that an electronic record must meet under Section 65-B, before it can be admitted in evidence:

- (a) It must be accompanied by a certificate which **identifies the electronic record** containing the statement;
- (b) The certificate must **describe the manner in which the electronic record was produced**
- (c) The certificate must **furnish the particulars of the device** involved in the production of that record
- (d) The certificate must demonstrate that the information or electronic record tendered in evidence was produced by a computer/ device, **(i) which was used regularly to store or process such information in the ordinary course and (ii) was, at the relevant time, operating properly.**
- (e) 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.**

2. **What does the latest judgment, Arjun Panditrao, say on Section 65B of the Evidence Act?**

In *Arjun Panditrao*, the Supreme Court held that a certificate under Section 65-B is **mandatory** for production of any electronic record in a secondary form. The **only** scenario in which a Section 65-B requirement can be waived is in the event that a party has made all efforts (including judicial) to procure a 65-B but then finds it **impossible** to produce one.

3. **What are the implications of Arjun Panditrao for my Leegality agreements?**

The key takeaway for electronic agreements is that you must ensure that when you tender your agreement and Audit Trail in evidence, you file a suitable certificate under Section 65B, setting out the 5 Conditions identified by Anwar. An indicative draft of a Section 65B certificate is available [here](#).

4. **Will Leegality provide me with a Section 65-B Certificate?**

There is no need to obtain a Section 65-B Certificate from Leegality. You can provide the relevant 65-B certificate yourself. Your Leegality agreement is always accessible to you either through (i) your own Platform or (ii) your account with your document execution platform or (iii) in your email inbox. Thus, you are best placed to furnish a Section 65-B certificate.

Leegality Comment: However, should you at any point, encounter any difficulties in proving your Leegality agreement, we are here to help.

5. **At what stage do I have to file the Section 65-B certificate in Court?**

You have to file the certificate at the stage of evidence. Depending on the Court where your case is before, this stage of “evidence” begins when the Court asks parties to file their compilation of documents (for the purpose of marking of documents) or when the Court directs parties to file their Affidavits of Evidence along with their compilation of documents.

6. How do I prove my Aadhaar eSigned/ DSC Signed Leegality Agreement in Court?

Should you opt for an Aadhaar e-sign/DSC Sign/Doc Signer, the process of proving an agreement becomes very simple, and enjoys several presumptions:

- First, that the electronic agreement containing the Aadhaar e-sign/DSC Sign/Doc Signer was so concluded by affixing the electronic signature of the parties. (*Section 85A of the Evidence Act*)
- That the Aadhaar e-sign/DSC Sign/Doc Signer was affixed by parties with the intention of signing or approving the electronic record. (*Section 85B of the Evidence Act*)
- That the agreement has not been altered or tampered with after it was signed (*Section 85B of the Evidence Act*)

7. What if I have opted for another mode of Virtual Sign instead? How would I prove it before Court?

Your Leegality Virtual Sign agreements are digitally signed by Leegality, and thus enjoy a presumption that they have not been altered or tampered with after signing (*Section 85B of the Evidence Act*). However, you will have to lead additional evidence to show that the parties have accepted the agreement.

Ordinarily, you should be able to do this by producing the Audit Trail in Court along with a suitable certificate under Section 65-B of the Evidence Act. Your Leegality Audit Trail is also digitally signed by Leegality, and thus, it enjoys a presumption that it has not been tampered with.

Further Leegality offers several additional layers of authentication, such as Face Capture (with Liveliness Check) and Geolocation Capture. Adding these layers of authentication can reduce the deniability of the signature and make it easier for you to prove the same in Court.

It is also advisable to also lead oral evidence in addition to the Audit Trail to prove the execution of the agreement. For instance, you may step into the box to prove that (i) you sent an email attaching the executed agreement to the other party, who either accepted it/ did not deny it or that (ii) the conduct of the other party clearly demonstrates that he has acted pursuant to the agreement.

THANKS FOR READING

We hope you found this informative. Stay tuned for more eBooks and Articles demystifying the legal aspects of electronic contracts and execution.

Do you have any questions or feedback for us?
Feel free to drop us a line at enquiry@leegality.com



Leegality Publications

© 2020