TWO SIGNATURES, ONE TRUTH: RECALIBRATING ELECTRONIC EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023 - A PROPORTIONATE "EITHER-OR-PLUS" STANDARD FOR ELECTRONIC RECORDS UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Sneha Narula, LL.B., Jindal Global Law School, O.P. Jindal Global University

ABSTRACT

Most disputes now leave a digital trail - WhatsApp chats, emails, CCTV clips etc. The Bharatiya Sakshya Adhiniyam, 2023 recognises this reality: *Section 61, BSA* places electronic records on the same footing as paper, and *Sections 62–63, BSA* set out how their contents are proved. Trial practice, however, is developing a habit. Alongside the statutory certificate that travels with a "computer output", courts and counsel increasingly expect a second sign-off, either a platform-custodian letter confirming server-side details or a forensic expert's note on hashes, extraction method, and signs of tampering. This paper terms this the "two-signatures" expectation. Two brief definitions keep the discussion grounded. The certificate pathway is used when a party relies on a copy/derivative rather than the original device; admissibility usually rides on a certificate explaining how that output was generated and why it can be trusted. The original-device pathway applies when the actual phone/DVR/server is produced; the court can examine it or have it examined without leaning on the same certificate at the threshold. Unlike the IEA's single-signatory 65B certificate, *Section 63(4) BSA* escalates the threshold by requiring the certificate "at the admission stage" and, critically, two signatures: the person in charge and an expert (including an Examiner of Electronic Evidence under *Section 39(2)).* This shift risks turning a flexible gateway into a rigid, one-size-fits-all bar. A rigid dual-certification gate is normatively overbroad; a proportionate "either-or-plus" standard, admissibility via either a compliant certificate (for secondary outputs) or production of the original device, plus targeted expert/custodian intervention only upon specifically pleaded integrity disputes—better aligns reliability with procedural economy and access to justice.

The paper undertakes a doctrinal reading of *Sections 39–45 (expert evidence)*, *Sections 56–64 (documentary and electronic proof, including*

Section 61 parity and the Section 63 certificate/original-device pathways), *Section 66 and Section 73 (identification and comparison tools—signatures/handwriting/digital signatures)*, and *Sections 94–95 (parol-evidence rule)* under the BSA, together with the IEA–BSA transition; synthesises controlling precedent (*Anvar–Shafhi–Arjun Panditrao*; *Batra–Jai Lal–Ramesh Chandra*); and triangulates those findings with reputable legal-publisher and practitioner analyses on *Section 63(4)'*s dual-signature mechanics, the Schedule's hash fields, and the definition/capacity gaps around "expert". It also draws limited comparative cues and tests the proposed standard through worked examples, yielding proportionate reforms.

Keywords: Bharatiya Sakshya Adhiniyam, Electronic Evidence, Section 63, Digital Evidence, Electronic Records, Admissibility, Procedural Fairness.

A shopkeeper tenders a month of CCTV and a clean certificate after a theft. The DVR is in court; nothing is specifically disputed. Yet, following a "two signatures" habit, the court asks for an expert co-sign, the lab queue delays admission, and a simple case stalls *not because truth is hard to find, but because a second formality is hard to obtain*. This paper asks whether that should be the default, or whether either-or-plus does the same job with less friction.

To what extent is imposing a uniform, one-size-fits-all dual-certification gateway for electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023 (BSA), normatively justified and institutionally efficient? Would a proportionate "either-or-plus" standard—admissibility via either a compliant certificate or production of the original device, supplemented by targeted expert/custodian intervention only upon specifically pleaded integrity disputes—better reconcile evidentiary reliability with procedural economy and access to justice?

The question is not whether electronic records matter — they plainly do —but whether a uniform, one-size-fits-all dual-certification gate is a sensible default under the s 63(4) BSA. The text gives two anchors. First, digital records sit on the same footing as paper (s 61) and their contents are proved via s 63. Second, practice has started to treat two signatures — a responsible custodian and an expert — as the routine ticket for admission whenever a derivative "computer output" is offered[1]. *A "computer output" is any copy or derivative of an electronic record generated by or from a computer system—e.g., a printout, PDF, screenshot, server-log extract, or forensic image—rather than the original device or system itself; under s 63, such*

[1] Anju Gandhi, Rashmi Raveendran & Aniket Rajpurohit, *Electronic Evidence Changes Will Modernise Banking Practices*, INDIA BUS. L.J. (Oct. 22, 2024), https://law.asia/electronic-evidence-indian-law/.

outputs travel the certificate route (s 63(4)) for admissibility. That instinct responds to a real risk: digital artefacts are malleable and copying is lossless. Yet the statute also preserves the original-device route, and our case treats expertise as an aid rather than a universal gate. As *State of H.P. v Jai Lal* put it, "An expert is not a witness of fact. His evidence is really of an advisory character."[2] The task here is to evaluate whether a categorical two-signature rule fits that landscape, or whether a proportionate either-or-plus model better serves truth-seeking, cost, and fairness.

Reputable commentary helps fix what the new text actually does. A doctrinal explainer in Law.asia (India Business Law Journal) reads s 63(4) as requiring a certificate signed not only by the person in charge but also by an expert, and notes that the certificate is expected at the admission stage, while the Act does not define "expert"[3]. Those three features — second signature, timing, and definitional gap — are exactly what have hardened courtroom habits into a two-signature expectation (custodian + expert) . Bar & Bench's transition note makes the mechanics concrete: s 63(4) demands signatures of both signatories in the Schedule format, and the Schedule itself demands a hash value. The same piece flags feasibility pressure by recording that only a small number of Examiners of Electronic Evidence had been notified at the time — thin capacity for India's litigation scale[4]. SCC Times takes the same view, describing the BSA certificate as "also" requiring an expert's sign-off, effectively creating a dual-certificate mechanism.[5] A practitioner note by King Stubb & Kasiva reaches the same destination but warns about practical challenges with intermediaries and hash protocols, urging flexible judicial reading where needed[6]. A LiveLaw explainer usefully sets out the two-part certificate format (Part A by the producing party and Part B "to be filled by the expert") and the hash fields that must be completed[7] explaining why lawyers have begun to default to two signature and hashing early.

Those sources also supply the best case for this habit. A second, independent voice can anchor attribution and integrity in ways a single certificate may not platform letters tether account

[2] *State of Himachal Pradesh v. Jai Lal, AIR 1999 SC 3318, ¶ 17.*
[3] Gandhi et al., *supra* note 1.
[4] Daksh Sachdeva, *Navigating the Transition: Implications of the Bhartiya Sakshya Adhiniyam on Digital Evidence in Ongoing Trials*, BAR & BENCH (Sept. 14, 2024), https://www.barandbench.com/columns/navigating-the-transition-implications-of-the-bhartiya-sakshya-adhiniyam-on-digital-evidence-in-ongoing-trials.
[5] *Bharatiya Sakshya Adhiniyam, 2023—Key Changes*, SCC TIMES (2024), https://www.scconline.com.
[6] *Electronic Evidence under the BSA: Practice Notes*, KING STUBB & KASIVA (2024), https://ksandk.com.
[7] *BSA Certificate—Two-Part Form & Hash Fields Explained*, LIVE LAW (2024), https://www.livelaw.in.

ownership and server logs[8]; forensic notes walk a judge through hash continuity, extraction steps, and anomalies. Getting those answers up front can narrow disputes and increase confidence that what is seen is what was created. The Schedule's hash discipline is good hygiene: if an exhibit's fingerprint stays constant, courts worry less about silent tampering while evidence passes through hands and devices[9]. The trouble is not with using these tools, it is with mandating them uniformly. If "expert" is undefined[10] and notified capacity is thin[11] (as reported by Bar & Bench), a rigid two-signature rule will bottleneck the routine cases, penalising modest litigants who cannot charter forensic labs or obtain overseas custodian attestations on time. If certificates must be in place at admission[12], admissibility begins to swallow weight[13]: records that are probably genuine get parked because a second signatory is slow or out of reach. The law's purpose is to elevate reliable electronic outputs, not to create an obstacle course; proportionality, not ritual, should guide the threshold. At the system level, a rigid two-signature default adds delay. When an expert co-signature or a custodian letter is missing, matters are adjourned while parties send cross-border requests or queue for scarce examiners. For routine, uncontested records, these steps slow admission without improving truth. With dockets already heavy, each pre-admission detour drains court time and raises costs, especially for smaller litigants. A proportionate standard keeps scarce expert capacity for the few cases where integrity is genuinely in dispute.

The Supreme Court's arc supports that calibration. *In* Anvar P.V. v P.K. Basheer*[14]*, the Supreme Court reset the law on electronic proof. Where a party relies on a "computer output" rather than the original device, a certificate under s 65B(4) IEA *(*now s 63(4) BSA*)* is a condition precedent to admissibility. The Court treated s 65B as a self-contained code for proving such records (now carried forward in ss 61–63 BSA) and expressly disapproved the lenient approach in State (NCT of Delhi) v Navjot Sandhu*[15]*. In effect, Anvar closed the "any other proof" route for secondary electronic evidence; the alternative original-device gateway was later underscored in Arjun Panditrao Khotkar and is reflected in the BSA's structure (s 63 read with s 61). *Shafhi Mohammad* recognised narrow pragmatic flexibility where the device

[8] *Electronic Evidence under the BSA: Practice Notes*, *supra* note 6.
[9] Bharatiya Sakshya Adhiniyam, 2023, sched. Certificate, No. 47, Acts of Parliament, 2023 (India).
[10] Gandhi et al., *supra* note 1.
[11] Sachdeva, *supra* note 4.
[12] Bharatiya Sakshya Adhiniyam, 2023, § 63(4), sched. Certificate, No. 47, Acts of Parliament, 2023 (India).
[13] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1, ¶¶ 34, 52.
[14] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473, ¶ 24.
[15] *State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru*, (2005) 11 SCC 600.

or system lies beyond a party's control[16]. The Three-Judge Bench in *Arjun Panditrao Khotkar* restored clarity: "The requisite certificate in sub-section (4) is unnecessary if the original document itself is produced,"[17] while reaffirming that the certificate is the usual route for secondary outputs and that courts may permit later filing to prevent injustice.[18] None of these decisions convert expert involvement into a universal pre-admission gate; they set up structured pathways with off-ramps that avoid mechanical exclusion. Read with publisher analyses on hashing and capacity, the doctrinal message is straightforward: secure reliability without letting admissibility swallow questions of weight. Consistent with *State of H.P. v Jai Lal*[19], expert opinion assists rather than binds; its persuasive force turns on disclosed methods and reasons. Hence, the point is not to resist expertise but to deploy it where it actually helps. In Sri Chand Batra[20], the Court warned that expert conclusions carry weight only with disclosed material and reasons. Transposed to digital forensics, a second signature is useful only if it shows the artefacts examined, extraction steps, hash values and limits of the tools—not merely that an 'expert' has signed. This supports an either-or-plus approach: admit via certificate or original device, and order expert/custodian help targeted to a specific integrity issue with methods laid out for scrutiny.

The proportionate answer can be the "either-or-plus" model. Either a compliant certificate (for secondary outputs) or production of the original device satisfies admissibility. Plus, order targeted custodian/expert help only upon (i) a specific integrity dispute, (ii) a chain-of-custody break, or (iii) centrality with doubts that ordinary inspection cannot resolve. Judges can keep momentum by marking exhibits "subject to proof" and setting short timelines so integrity questions are resolved without derailing the trial. This is not leniency; it is calibration - deeper scrutiny where risk is higher, lighter touch where the record is routine and uncontested. The publisher material supports this design: dual signatures exist, hashing is useful, but definition gaps and capacity constraints counsel against making the second signature a universal precondition[21].

On the ground, the proposed model is intuitive. With WhatsApp chats, if a party files a facially compliant certificate and the opponent merely says, "this looks edited," a blanket rule would

[16] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801, ¶¶ 22–24.
[17] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1, ¶ 34.
[18] *Id*.
[19] *State of Himachal Pradesh v. Jai Lal*, AIR 1999 SC 3318, ¶ 17.
[20] *Sri Chand Batra v. State of U.P.*, AIR 1974 SC 639, ¶ 9.
[21] *Electronic Evidence under the BSA: Practice Notes*, *supra* note 6.

force a full forensic detour. Under either-or-plus, the judge asks for various particulars (which date window? which messages? what header oddities?) and, if the concern is concrete, orders a limited neutral extraction and hash check for that band; otherwise, the chat comes in and is tested on weight through cross-examination. With CCTV, a shopkeeper's certificate and, where feasible, production of the DVR often settles admissibility; if the defence alleges clock drift, the court directs verification of DVR time settings and frame metadata only. For foreign platforms, where custodian letters can take months, device-based proof and screen-capture workflows can carry admissibility[22], with a tightly framed platform request reserved for genuinely central posts that remain contested. These illustrations show how the model harnesses the good parts of the new regime - structured certificates, hashes, expert help - without imposing them everywhere.

The counter-case deserves a fair hearing. One worry is under-deterrence - if parties think they can get in with just "either" some may chance doctored outputs. Another is capacity variance across trial courts. The answer is guidance, not rigidity. High Courts can standardise what a capable certificate must contain[23], specify who a capable custodian is for common sources, and maintain rosters of neutral examiners with short, replicable reporting templates (tools used, versions, logs kept). Courts can also deploy adverse inferences where a party stonewalls a focused integrity order. These steps absorb the best insights from the publisher analyses - hash discipline, expert input, and the reality of scarce capacity - without turning them into universal hurdles.[24]

Two limitations should be acknowledged. First, India lacks robust empirical time-and-cost studies comparing rigid versus proportionate authentication; efficiency claims here are inference-based, aligned with practitioner commentary but not large datasets[25]. Second, the open texture of "expert" will continue to matter[26]. Until clearer guidance emerges, courts should read "expert" functionally - competence shown by validated tools and replicable methods - while recognising that notified Examiners of Electronic Evidence[27] are too few for a universal two-signature rule.

[22] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801, ¶¶ 22–24.
[23] Bharatiya Sakshya Adhiniyam, 2023, sched. Certificate, No. 47, Acts of Parliament, 2023 (India).
[24] Gandhi et al., *supra* note 1.
[25] Sachdeva, *supra* note 4.
[26] Gandhi et al., *supra* note 1.
[27] Information Technology Act, 2000, § 79A.sh

Stepping back, the record is consistent. Read with Supreme Court pathways, the either-or-plus standard best reconciles these pressures: admit via certificate or original device; add expert/custodian help only when a specific integrity risk is shown. Accordingly, the uniform dual-certification gateway is not a fair or efficient default; a proportionate either-or-plus model better reconciles evidentiary reliability with procedural economy and access to justice.

Conclusion

A rigid dual-signature default trades speed for symbolism; proportionality gets us reliability and timeliness. This paper asked whether a uniform dual-certification gateway for electronic evidence under the BSA 2023 is a fair and efficient default. The analysis shows it is usually not. Dual signatures and hash discipline can strengthen integrity, but as a blanket rule they make admissibility swallow questions of weight, slow proceedings, and penalise parties who cannot easily secure an expert or a distant custodian. The statutory architecture and the Supreme Court's arc point instead to structured pathways- a compliant certificate for secondary outputs or production of the original device - while treating expert input as assistance, not as a universal pre-admission gate. Accordingly, a uniform dual-certification gateway is neither normatively justified nor institutionally efficient under the BSA 2023; the either-or-plus standard is preferable: admit via either certificate or original device and add targeted expert steps only upon a specific integrity dispute, a chain-of-custody break, or centrality with doubts unresolved by ordinary inspection. The significance is practical: this calibration reduces over-exclusion, preserves scarce expert capacity for cases that truly need it, and aligns evidentiary reliability with procedural economy and access to justice. Immediate implementation can come through practice directions, a standardised certificate template (with hash fields), a "capable custodian" definition, short timelines for speaking objections, rosters of neutral examiners, and permission to mark exhibits subject to proof—with a functional reading of "expert." Future work should track time-and-cost data and acceptance/exclusion rates across court tiers. Against India's backlog, calibration is a timeliness mandate: it keeps trials moving while reserving heavier procedures for cases that truly need them.

One signature where sufficient; two where sense—not habit—demands it.