UNDERGRADUATE ESSAY:

The role of digital signatures in the digitisation of loan documentation in India

By **Rishabh Sant Tiwari and Deepansh Goyal**

When extending credit (vehicle finance, working capital finance etc.) in India, bulky paperwork is common. However, the use of electronic signatures may change this. Electronic signatures have become an ordinary practice, and the most frequent use of this is by the way of typing a name into an e-mail or the electronic equivalent of the manuscript form of cross – the 'I accept' or 'I agree' icon, used on websites and software to indicate that the signatory intends to enter into a contract or accepts the terms of a licence.[1] Reliance on electronic signature relies on the veracity of the process if it is a product, and the electronic evidence put before a court if it is challenged. This article considers a new electronic signature technique called 'Aadhaar e-KYC services'.

Legal admissibility of digital evidence in India

New sections 65A and 65B were introduced to the Indian Evidence Act, 1872 under the Second Schedule to the IT Act 2000 (see below). Section 65A provides that the contents of electronic records may be proved in accordance with the provisions of section 65B. Section 65B provides that notwithstanding anything contained in the Evidence Act, any information contained in an electronic record, whether it be the contents of a document or communication printed on a paper, or stored, recorded, copied in optical or magnetic media produced by a computer (also referred to as computer output in the Act), it is deemed to be a document and is admissible in evidence without further proof of the production of the original, providing the conditions set out in section 65B(2) – (5) are satisfied.[2] The requirement is the information should be fed in the computer in the ordinary course of business;[3] the computer should be operating properly[4] and is used by a person who is lawfully entitled to the control of such computer.[5]

Electronic signatures

Parliament enacted the Information Technology Act, 2000 ('IT Act 2000') to make electronic records admissible as evidence in legal proceedings in the same way as paper documents, amending it in 2008 to widen the definition of electronic signatures as a mode of authenticating any electronic document. The term 'electronic signature' is defined as 'authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature.'[6] The term 'electronic signature' is very wide and 'digital signature' is only one of the many kinds of electronic signatures one can envisage.[7]

The IT Amendment Act 2008 inserted section 3A as follows:

> (1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic 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

[1] For the full range of electronic signatures, including case law across the world, see Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016).

[2] In the case of *Tomaso Bruno v State of U.P., Criminal,* (2015) 7 SCC 178, Supreme Court of India held that computer generated electronic records in evidence are admissible at a trial if proved in the manner so specified under 65B. Further it was held those electronic documents are to be considered as material evidence.

[3] Section 65B(2)(b), Indian Evidence Act, 1872.

[4] Section 65B(2)(c), Indian Evidence Act, 1872; for a critical analysis of the failure of judges to define what 'operating properly means', see Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), chapter 6.

[5] Section 65B(2)(a), Indian Evidence Act, 1872.

[6] Section 2(ta) of the IT Act, 2000 as amended by IT Amendment Act, 2008.

[7] Section 2(ta) of IT Act, 2000 defines electronic signatures as 'inclusive' of digital signatures; see also *Electronic Signatures in Law*.

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 of 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 information made after its authentication by electronic signature is detectable; and
>
> (e) it fulfils such other conditions which may be prescribed by the Central Government.

Section 3A(2), IT Act 2000 provides as follows:

> 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 of 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 information made after its authentication by electronic signature is detectable; and
> >
> > (e) it fulfils such other conditions which may be prescribed by the Central Government.

Section 3A provides for criteria of any electronic authentication technique to be termed as 'electronic signature' under the IT Act 2000. The criteria include two cumulative conditions – the technique must be considered reliable and specified in the second schedule of the IT Act 2000, although it might be difficult to visualise a situation where the electronic authentication technique is not reliable but specified in the second schedule. The threshold of 'reliability' is set high by prescribing, among other things, that any alteration to the document or signature must be detectable and that the signature is that of the signatory only. The legal recognition of an electronic signature is covered in section 5 of the Information Technology Act, which reads as follows:

> 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.

A new authentication service

The Second schedule of the IT Act 2000 was amended to incorporate a new electronic signature technique called 'e-authentication technique using Aadhaar e-KYC services' ('e-Sign')('e-KYC' means 'electronic Know Your Customer').[8] The 'Digital Certificates' in the case of e-Sign are issued under two classes:

> (a) Aadhaar-eKYC – OTP: This class of certificates shall be issued for individuals use based on OTP authentication of subscriber through Aadhaar e-KYC;[9] and
>
> (b) Aadhaar-eKYC – Biometric (FP/Iris): This class of certificate shall be issued based on

[8] The Ministry of Communications and Information Technology notified the Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 on 27 January 2015, available at http://meity.gov.in/content/notifications .

[9] Accounts opened using OTP based e-KYC are subject to seven conditions, for which see the amended Directions (8 December 2016), RBI/2016-17/176DBR.AML.BC. No. 18/14.01.001/2016-17 to the Reserve Bank of India (Know Your Customer (KYC)) Directions, 2016, available at https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=10770&Mode=0 .

biometric authentication of subscriber through Aadhaar e-KYC service.[10]

This permits a new technique to be used by anyone for authenticating any electronic document.[11]

How e-Sign works

The regulatory authority of e-Sign is the Controller of Certifying Authorities, who has been appointed by the Central Government under the IT Act 2000.[12] The Office of Controller of Certifying Authorities aims at promoting the growth of E-Commerce and E-Governance through wide use of digital signatures.[13] Digital signatures are approved via designated Certifying Authorities, who issue Digital Signature Certificates (DSC) for authentication of users who sign documents electronically. Prior to issuing a DSC, a Certifying Authority (CA) is required to verify the credentials of the applicant as stated in the Application Form and supporting documents. The IT Act 2000 provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities.

There are various organizations and individuals in the e-Sign process. They include the Application Service Provider ('ASP') which is the 'consumer institution' of e-Sign services (any financial service providing institution can be one of the examples of ASP); the e-Sign Service Provider ('ESP') which is one of the Certifying Authorities licensed by Controller of Certifying Authorities for providing e-Sign services throughout India;[14] the Unique Identification Authority of India ('UIDAI') which is a statutory authority established under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; and the end user.

The following is the step by step process of affixing an e-Signature on a document:[15]

At the Application Service Provider:

ASP generates the Application Form in .pdf form.

ASP takes the mobile number or the biometrics of the applicant ('other details').

ASP generates the hash of the document.

ASP sends the 'xml' (hash + other details) to e-Sign service provider ('ESP').

At the ESP

ESP sends the Aadhar card details (e-KYC input) for verification to UIDAI.

If verified, based on the e-KYC information, a key pair is generated. The public key is sent to the Certifying Authority for the creation of a certificate called a 'Digital Signature Certificate'. The private key is kept by the ESP.

The Certifying Authority creates the Digital Signature Certificate using the public key and e-KYC information.

The Digital Signature Certificate is sent to the ESP.

Based on the Digital Signature Certificate, the ESP signs the document hash using a private key.

At the ASP

The ASP receives the signed hash from the ESP.

Attaches the signature to the document.

The procedure of affixing an e-Sign on a document is fairly simple from the point of view of the end user. The end user just has to give his 'Aadhar' details and receive the e-Sign(ed) document within few minutes. Moreover, the process is quite cost effective as the cost of a 'transaction'[16] is minimal.[17]

[10] *ASP On-Boarding Guide (Draft for discussion only)*, Controller of Certifying Authorities Department of Electronics and Information Technology Ministry of Communications and Information Technology, Version 1.0, April 2015, available at http://www.cca.gov.in/cca/sites/default/files/files/ASPOn-BoardingGuidebook_v3.0-RC_20.4.15_DRAFT.pdf .

[11] The Reserve Bank of India also ordered the Aadhaar based verification for Card Present Transactions via circular DPSS.CO.PD.No.892/02.14.003/2016-17 dated 29 September 2016 and again through RBI/2016-17/170 DPSS.CO.PD No.1421/02.14.003/2016-17 dated 2 December 2016.

[12] Section 17, IT Act, 2000.

[13] About CCA, available at http://www.cca.gov.in/cca/?q=about.html.

[14] There are four Certifying Authorities authorized to provide e-Sign Services in India at present: eMudhra Ltd; C-DAC; (n)Code Solutions and NSDL e-Governance Infrastructure Ltd, http://www.cca.gov.in/cca/?q=service-providers.html.

[15] *ASP On-Boarding Guide*.

[16] A 'transaction' is the completion of the process starting with ASP generating the document that is to be signed and ending with affixation of e-Signature on the document.

[17] The transactional cost depends on the negotiations between API and ESP. Generally, it can be around Rs. 3 to Rs. 5 per transaction. In one transaction, the number of pages contained in a document may be irrelevant and the whole document may be signed by incurring the cost of one transaction. This is by the virtue of the fact that if there is any tampering with the document, the digital signature

Practical problems with the implementation of e-signatures in a financial institution

Payment of stamp duty

One of the major obstructions to the implementation of the digitization process is the payment of stamp duty on the loan agreement. Generally, when the document is in physical form, the stamp duty is paid by a legal instrument attached to the physical document. Hence, there arises a difficult situation when the document is in electronic form. This difficulty has been removed by the ability to make a payment of stamp duty on-line. The payment receipt can then be attached to the document in electronic form. The problem is that the facility of making a payment of stamp duty on-line is not provided by every state in India. In fact, Maharashtra is the only state that has a system to collect stamp duty on-line, called the Government Receipt Accounting System (G.R.A.S.).[18] G.R.A.S. enables the users to pay on-line stamp duty without the need to visit a bank. The digitally signed receipt of the payment can be appended to the electronic document that is digitally signed.

Other states in India also allow for the payment of stamp duty on-line, but this is different to G.R.A.S, because under G.R.A.S, the customer does not have to attend a bank in person. This alternative method is by means of a public sector company called Stock Holding Corporation of India Limited (SHCIL). This company has been appointed as the sole Central Record Keeping Agency (CRA) in India, and e-stamping is conducted in around 13 states and 4 Union Territories. A Central Record Keeping Agency handles user registration and e-Stamping Application Operations and Maintenance. It also appoints Authorised Collection Centers (ACCs), which act as the intermediary between the CRA and the duty payer. The procedure for SHCIL based stamp duty payments is as follows: The customer approaches an ACC appointed by SHCIL and completes the application form as prescribed in the e-Stamping system. A Stamp Certificate is generated after the realization of funds. After submitting a duly filled and signed application form, the ACC will enter the details into the system and a Stamp Certificate will be generated immediately in case of cash, and in case of a cheque, demand draft, payorder, RTGS/NEFT account to account transfer, only after realization of funds.

The Maharashtra Stamp (Amendment) Act, 2015[19] inserted Section 10D into the principal Act[20] so as to enable the virtual treasury of the Maharashtra Government to collect stamp duty on-line. Section 10D of The Maharashtra Stamp Act, 1958 now states:

> (1) Notwithstanding anything contained in this Act, the State Government may, by notification in the Official Gazette, direct that any State Government Department, institution of local self-Government, semi Government organization, banking or non-banking financial institution or the body owned, controlled or substantially financed by the State Government or any class of them, shall ensure that the proper duty is paid to the State Government through Government Receipt Accounting System (G.R.A.S.) in respect of such instruments, as may be specified in the notification passing through their system or related to their functioning of which registration is not compulsory.
>
> (2) The Chief Controlling Revenue Authority shall authorise a person nominated by such Department or body, etc. as mentioned in sub-section (1) as a proper officer for defacing the challan and making the endorsement on such instruments.
>
> (3) It shall be the duty of the proper officer so authorised under sub-section (2) to make an endorsement on the instruments after defacing the challan, as follows:—'Stamp duty of Rs. _____ paid in *cash/by demand draft/by pay order/e-Challan, vide Receipt/Challan No._____/GRN No._____ CIN_____ dated the _____. Seal of the office. Signature of the Officer.

There was a corresponding amendment in the Maharashtra Tax Laws (Levy and Amendment) Act, 2013 as follows:

becomes invalid. Therefore, the digital signature need not be affixed to every page of the document unless the end user or API wishes to separate the document in future.

[18] The stamp duty can be paid by creating an account on the official website of G.R.A.S., at https://gras.mahakosh.gov.in/echallan/ .

[19] Maharashtra Act No.XX of 2015, notified on 24 April 2015.

[20] The Maharashtra Stamp Act, 1958 (Bombay Act No. LX of 1958).

Maharashtra Act No.VIII of 2013. Section 30A states:

'(1) Notwithstanding anything contained in section 30, where any instrument referred to in clauses (a) to (g) of section 30, is executed on or after the date of commencement of the Maharashtra Tax Laws (Levy and Amendment) Act, 2013(Mah. VIII of 2013), in favour of or by any financial institution such as Bank, Non-Banking Finance Company, Housing Finance Company or alike, which creates any right in favour of any such financial institution, the liability to pay proper stamp duty shall be on such financial institution concerned without affecting their right, if any, to collect it from the other party.

(2) In respect of any such instrument executed before the date of commencement of the Maharashtra Tax Laws (Levy and Amendment) Act, 2013, (Mah. VIII of 2013) and are effective and where proper stamp duty is not paid, then the financial institution shall impound such instrument on or before the 30th September 2013 and forward the same to the Collector for recovery.

(3) Where the financial institution fails to impound such instrument as provided in sub-section (2), then the concerned financial institution shall be liable to pay a penalty equal to the stamp duty payable on such instrument.

When reading a combination of sections 10D and 30A, it is suggested that these provisions impose an obligation on the banks and financial institutions to ensure that the proper duty is paid to the state government through the Government Receipt Accounting System (G.R.A.S.) in respect of such instruments.

This was challenged in Supreme Court of India,[21] whereby the petitioners alleged that this was an unreasonable obligation on the financial institutions. Moreover, the calculation of the applicable stamp duty for the bulk of documents was another question before the court. The Supreme Court upheld the constitutional validity of the enactment. The government agreed to provide financial institutions and banks software which will calculate the applicable stamp duty on the documents. The document has to be scanned and uploaded and the software will calculate the payable stamp duty. Also, the banks will not be liable for any inaccuracy or discrepancy in the payment of stamp duty if the software causes a miscalculation.

Repayment mechanism

Currently the repayment mechanism is based upon the National Automated Clearing House (NACH), which is a centralized clearing system run by the National Payments Corporation of India. At present, the system uses paper documents.

Interestingly, there are various arrangements of e-commerce websites and other entities[22] with the banks for collection of their EMIs[23] on their products. In this process, the customer has to enter his credit/debit card details, account number, bank name and IFSC code,[24] etc. to buy the product or service on EMIs. This arrangement of the e-commerce website with the bank works on the similar lines as that of an ECS/NACH mandate. The details entered by the customer give a standing instruction to the bank to debit the EMI amount periodically.

To attain complete digitisation in financial institutions, it is necessary that they work with the banks separately for repayments on the similar lines as that of e-commerce entities, unless the Reserve Bank of India introduces guidelines on any such mechanism of repayment.

Implementing safeguards

On-line transactions and the digitisation process pose new threats to the security of electronic documents such as unauthorized access to proprietary systems, downloading or manipulating confidential information.[25] To tackle this, the Government of India

[21] *Fullerton India Credit Co. Ltd. v State of Maharashtra*, 2016 SCC Online SC 1396 (Supreme Court of India).

[22] For instance, https://www.flipkart.com/pages/payments (Flipkart) and https://www.bajajfinserv.in/finance/emi-cards/salaried-emi-cards-faq-questions.aspx (Bajaj FinServ).

[23] An equated monthly instalment (EMI) is a fixed payment amount made by a borrower to a lender at a specified date each calendar month. Equated monthly instalments are used to pay off both interest and principal each month so that over a specified number of years, the loan is paid off in full.

[24] IFSC is an abbreviation for Indian Financial System Code. It consists of 11 digit characters that identify individual bank branches participating in the various on-line money transfer options like National Electronic Funds Transfer (NEFT) and Real-time Gross Settlement Systems (RTGS).

[25] Kristin N. Johnson, 'Cyber Risks: Emerging Risk Management Concerns for Financial Institutions', 50 Ga. L. Rev. 131, 142 (2015).

has introduced the National Cyber Security Policy with the vision to build a secure and resilient cyberspace for citizens, businesses and government.[26] Additionally, the Reserve Bank of India has released a framework for banks[27] and non-banking financial companies[28] to enhance the security and efficiency of the IT framework adopted by them.[29] In the light of these regulatory mechanisms, it becomes mandatory for all the financial institutions to adopt appropriate security measures while going fully digital.

Conclusion

The introduction of e-Signatures as a method of authentication of electronic documents will eventually change the landscape for loan documentation in India. The low cost of signing electronically is likely to encourage financial institutions to prefer it over paper transactions. However, in the process, there will be certain obstacles such as financial literacy and financial inclusion to consider, but they are certainly improving in the Indian context, although there are also other problems such as the higher cost of the infrastructure needed, especially for the biometric eKYC, and for setting up and manning the authorised centres. Further, unless security measures for the on-line systems are improved, the chances of tampering with on-line data or transactions have the potential to be significant. It is strongly suggested that state governments consider implementing the Maharashtra Model as G.R.A.S. enables fully digital payment of stamp duty.

Finally, an observation for the not too distant future, is should be noted that vehicle finance forms a vital part of financing in India. It is estimated that India's new passenger vehicle finance market will double to over Rs 160,000 crores from 2014-2015 levels by the turn of the decade. The auto finance market in India is a growing market, with 74 per cent finance penetration. The importance of vehicle finance (which statutorily requires filling of paper Road Transport Authority 'RTO' forms) cannot be more emphasised. It is pertinent to note that if RTO forms are not digitised, full digitisation is not at all possible for vehicle finance, because it will be necessary for the customer to manually sign the paper forms.

Rishabh Sant Tiwari is pursuing a B.A. LL.B. (Business Law Honours) course from National Law University, Jodhpur, India. This is a five year course in which he is currently in his fourth year, having opted for Business Law Honours.

rishabhsanttiwari@gmail.com

Deepansh Goyal is pursuing a B.B.A. LL.B. (Business Law Honours) course from National Law University, Jodhpur, India. In his fourth year of a five year course, he has opted for Business Law Honours.

deepanshgoyal@gmail.com

[26] Ministry of Electronics and Information Technology, Government of India, *National Cyber Security Policy – 2013*, available at http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf .

[27] *Cyber Security Framework in Banks*, RBI/2015-16/418, dated 2 June 2016.

[28] *Master Direction – Information Technology Framework for the NBFC Sector*, RBI/DNBS/2016-17/53, dated 8 June 2017.

[29] The Reserve Bank of India also stated that 'banks may consider implementation of digital signature for large value payments for all customers, to start with for RTGS transactions', in its circular titled *Security and Risk Mitigation Measures for Electronic Payment Transactions* numbered RBI/2012-13/424DPSS (CO) PD No.1462/02.14.003/2012-13 dated 28 February 2013, available at https://rbi.org.in/scripts/NotificationUser.aspx?Id=7874&Mode=0 .