



The Legal Capsule

# **LEGAL REPORT**

## **OF**

# **THE LEGAL CAPSULE**

© The Legal Capsule



## VIRTUAL SIGN

### Meaning

Virtual signature is a digital signature which inscribes the normal hand written signature of a person in digital form. It does not require the authentication of any authority for it to be legally binding. It reflects the user's consent on the same. A digital signature is inscribed on a document by using the mouse pad on a computer or the display screen of a touchscreen mobile phone to draw and replicate the handwritten signature by a person.

A virtual signature just like a normal hand written signature represents the person's consent and motive to sign a document and validate its contents thereby making it binding.

The said virtual signature appears on the document by being inscribed on the said document which it is digitally signed at a specific position on the document.

In order to increase the security of the same, the virtual signed document is mapped and can be accessed along with the audit trail. This audit trail mentions the time, place, location of the document at various stages and hence helps to correctly identify and ascertain security towards the signature placed over it. Detailed information regarding the audit trail is mentioned under the sub-topic Audit trail further in this document.

### Validity

Section 10A of the Information Technology Act, 2000 provides that Virtual signature is proper and binding to execute a document for the approval of contents.



**Sec. 10 A. 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 record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.*

Virtual signature is however not mentioned under the Second Schedule of the Information Technology Act, 2000. Hence, for the execution of documents of statutory nature, Virtual signature is not binding.

Nevertheless, it's important to note that repetitive documentation which requires a mere approval from a person can be validly executed using Virtual signature.

Sec. 3 of the Indian Contract Act, 1872 provides that a communication, acceptance or revocation can be done by a person by any method which has the effect of communicating the same. Hence, it can be safely ascertained that a virtual signature having an effect of communicating the intention of a person can be validly used to execute a contract of any nature whatsoever.

**Sec. 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 any 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.*



## E-SIGNATURE USING AADHAAR

### Meaning

E-Signature using Aadhaar is the abbreviation of Electronic Signature executed using Aadhaar Card of the signer or executor.

Using this feature one can electronically sign and authenticate documents from anywhere and anytime using our e-Signature service using Aadhaar based verification from mobile/tablet/PC.

The e-Sign service is provided in association with the Aadhaar card governed by the Unique Identification Authority of India (UIDAI) and Digital Signature Certificate (DSC) governed by the Controller of Certifying Authorities.

E-Signature using Aadhaar is legally valid and is recognized by the Government of India for most documents as per the Information Technology Act, 2000.

It is as legally binding as a handwritten signature for most documents. The IT Act of 2000, acknowledges the e-signature and Dongle based Digital Signature Certificate (DSC).

The person has to be 18 years of age to make a valid signature unless accepted otherwise in a special scenario. Also, just like any handwritten signature, E-Signature using Aadhaar is valid eternally.

### Validity

The Gazette Notification of the Department of Electronics and Information Technology under the Ministry of Communications and Information Technology dated 27<sup>th</sup> January, 2015 numbered as G.S.R. 61(E) provides that execution of



documents using E-Signature using Aadhaar Card is an authorised manner of executing documents.

Additionally, unlike Virtual Signature, E-Signature using Aadhaar Card is mentioned under the Second Schedule of the Information Technology Act, 2000. Hence, the validity of E-Signature using Aadhaar is a very strong and completely secure manner of executing documents. E-Signature using Aadhaar Card along with audit trail makes it a tamper proof signature hence making it more safe and legally valid than a traditional hand signature.

Initially, the Supreme Court in case of Justice K. S. Puttaswamy and Anr. v/s Union of Indian and Anr. Writ Petition Civil no. 494 of 2012 had passed an order saying that Aadhaar authentication under Sec. 57 of the Aadhaar Act, 2016 is unconstitutional only in case where it is not expressly allowed by the law. Later on, the Government of India amended the Aadhaar Act in the Aadhaar and other laws (Amendment) Ordinance on March 2, 2019; wherein under Sec. 4 of the same Aadhaar authentication is permitted if such authentication is permitted under any other law in the territory of India. Since, E-signatures are valid under the Information Technology Act, 2000; E-Signature using Aadhaar is hence a valid authentication based e-signature.

Additionally the Controller of Certifying Authorities (CCA) has developed revised guidelines in line with the above Supreme Court judgment on the authentication and recognition of e-signatures using two modes of verification i.e. Online Aadhaar e-sign authentication and the Offline Aadhaar e-sign verification. The one used on the Legal Capsule portal is the Online Aadhaar e-sign authentication.

Sec. 5 of the Information Technology Act, 2000 provides for the validity and legal binding of E-Signature using Aadhaar.



***Sec. 5. Legal recognition of digital 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 (hen, 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 digital signature affixed in such manner as may be prescribed by the Central Government.*

Apart from Sec. 5, Sec. 3, 3A of the Information Technology Act, 2000 also provide for authentication of electronic records.

Section 10A of the Information Technology Act, 2000 provides that E-Signature using Aadhaar is proper and binding to execute a document for the approval of contents.

***Sec. 10 A. 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 record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.*

Sec. 3 of the Indian Contract Act, 1872 provides that a communication, acceptance or revocation can be done by a person by any method which has the effect of communicating the same. Hence, it can be safely ascertained that a E-Signature using Aadhaar having an effect of communicating the intention of a person can be validly used to execute a contract of any nature whatsoever.



**Sec. 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 any 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.*

Sec. 85, Sec 85 A, Sec. 85 B, Sec. 85 C of the Indian Evidence Act, 1972 provides that every document containing a digital signature is a valid proof to be binding in the court of law.

**Sec. 85. Presumption as to Electronic Signature Certificates. -** *The Court shall presume, unless contrary is proved, that the information listed in an 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.*

Also, Sec. 47A of the Indian Evidence Act, 1972 provides for authentication of digital signature with approval of Certifying Authority.

Furthermore Sec. 65 A of the Indian Evidence Act, 1972 provides for Special provisions as to evidence relating to electronic record and Sec. 65 B provides for the manner of Admissibility of electronic records. Also, Sec 67 A provides for the purpose of proving the validity of digital signatures.

It is evident to note that the Information Technology Act, Controller of Certifying Authorities and other related authorities also do not put any limit on the amount for which contract is being executed using E-Signature using Aadhaar.



The SEBI circular dated April 24, 2020 on the subject Clarification on Know Your Client (KYC) Process and Use of Technology for KYC; SEBI has directed the use of E-sign using Aadhaar card and confirmed that the documents executed using E-sign feature will be upheld as valid documents in the eyes of law in consonance with Section 5 of the Information Technology Act, 2000.

**DOCUMENTS WHICH CANNOT BE EXECUTED USING DIGITAL SIGNATURE NEITHER E-SIGNATURE USING AADHAAR CARD NOR VIRTUAL SIGNATURE.**

However, one must note that as per Sec. 1(4) of the Information Technology Act, 2000 the below documents are compulsory excluded from the purview of digital, electronic, virtual signatures of any kind whatsoever because of their legal requirements and evidentiary valuations:

- (a) a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
- (b) a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882; (c) a trust as defined in section 3 of the Indian Trusts Act, 1882;
- (d) a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
- (e) any contract for the sale or conveyance of immovable property or any interest in such property;
- (f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.



## AUDIT TRAIL

When executing a document in the traditional format, the signature inscribed on a document is carried out for two main reasons, first to ensure the authenticity of the person to show that it is the same person who has signed the document as mentioned in the agreement; secondly it is safeguard the document so that the signer cannot deny that he had agreed to the contents of the document later. There have been many instances where traditionally hand signed signatures on documents have been forged and have been contested in the court of law. In order to prevent this, the audit trail of a document comes to the rescue.

An Audit trail refers to a document which provides the tracks or logs relating to the execution of a document. It comes into existence at the instance of commencing the drafting of the document and end when the document is executed by all parties who are a part of the same. It contains the date logs i.e. day, month, year; time logs i.e. hours, minutes, seconds; locations logs; geographical logs; and other required tracks and status information of the document. This is done using the trackers put forth for the document. The Audit trail is a tamper proof document as it is automatically coded by the document and hence can be relied upon with utmost certainty. The Audit trail hence can be used to prove the authenticity of the document execution process in the court of law.

Every document comes with an Audit trail; hence one can easily refer the same to judge the authenticity of the signatures of the parties to the document.

Audit trail is hence a highly secured, documented, tamper proof document providing the details of the execution processes of a document. The audit trail provides a manner with which the authenticity of a digital signature can be increased.



### **The Legal Capsule**

Another very essential feature of an Audit trail is that since it tracks the document and takes log of everything. If there are any discrepancies or attempts to hack or malign the document, such instances are identified, hence making the electronically signed digital document extremely tamper proof and secure.

It is a helpful document which goes hand in hand with a document signed using E-Signature using Aadhaar Card and virtual signature. It helps prove the authenticity beyond reasonable doubt of the validity of the signature inscribed on a particular document.

© The Legal Capsule



## E-KYC

e-KYC is the abbreviation of Electronic Know Your Customer. It is a process of verifying the identity of a person in order to prevent the occurrence of identity fraud.

e-KYC is a novel method of conducting the KYC process electronically with the use of Aadhaar Card governed by the Unique Identification Authority of India.

e-KYC can be helpful in assisting corporates to file various compliances easily thereby saving time and money.

### **Mobile OTP based e-KYC**

This process is only valid if the Aadhaar card holder has linked his Mobile number with the Aadhaar Card.

Upon typing the Aadhaar number on the portal, an OTP (One Time Password) will be sent to the mobile number linked with the Aadhaar Card. After successfully entering the OTP; the UIDAI will release the details of the person to the required authorities and also verify the credentials of the person in accordance with their database.

The UIDAI assures and provides a safe encrypted transfer of information from the UIDAI database to the requisite authorities. Hence, there exists no possibility of any leakage of information to any third party.

The RBI ratified the Supreme Court judgment and granted excess to large number of bodies to use the e-KYC Aadhaar based platform to carry on the KYC process in May 2019.



## The Legal Capsule

However, in October 2019, the RBI clarified that Digital Service Agents (DSA) will not be allowed to carry out the process of e-KYC anymore in order to prevent any leakage of secure information of people to any third party. Due to this recent reform, each body using e-KYC facility must appoint an authorized representative of their own to carry out this e-KYC procedure.

The Notification of the Reserve Bank of India dated January 9, 2020 formally accepted the Video E-KYC as a legal method KYC process.

The Notification issued by the Ministry of Finance in accordance with the Prevention of Money Laundering (Maintenance of Records) Third Amendment Rules, 2019 provides for the concept of Digital KYC. Hence, making E-KYC a valid form of Know Your Customer process.

Furthermore, in the SEBI circular dated April 24, 2020 on the subject Clarification on Know Your Client (KYC) Process and Use of Technology for KYC; SEBI has directed the use of Online KYC process for establishing verification of customers swiftly and nullify the hassles caused.



## E-STAMP

Stamp duty refers to a specific amount to be paid for the execution of a document as per the Indian Stamp Act, 1899.

Stamp duty on some document comes under the ambit of the Indian Stamp Act, 1899 which is a central legislation. While some other documents comes under the ambit of the respective state.

E-Stamp refers to a digital stamp inscribed on a paper to resemble the payment of the value of the stamp. The Central Government has passed legislations validating E-stamp papers. Most of the states in India have already shifted to E-stamp paper while some states are in the process of shifting to E-stamp.

States and Union Territories like Haryana, Telangana, Karnataka, Uttar Pradesh, Punjab, Chhattisgarh, Andhra Pradesh, Bihar, Delhi, Gujarat, Andaman & Nicobar Islands, Assam, Chandigarh, Dadra and Nagar Haveli, Daman and Diu, Himachal Pradesh, Jammu & Kashmir, Jharkhand, Ladakh, Odisha, Puducherry, Rajasthan, Tamil Nadu, Tripura, Uttarakhand have moved to E-Stamp on the Stock Holding Corporation of India Limited. While states like Maharashtra have their own personalised portal.

The general validity of the E-Stamp is six months. However this may vary depending upon the state and document so stamped.

E-stamp hence is a computer based secured manner of paying stamp duty to the Government. Each E-stamp possesses a Unique Identification Number which is a system generated number which can be used to check the authenticity of the E-Stamp.



## **The Legal Capsule**

The Central Record Keeping Agency is the agency that handles the process of issuing E-stamp.

E-Stamp is a very safe, secure process of stamping documents as while procuring the stamp paper all details of the document and the parties to it are noted by the registry. These records can be shown in court to prove the authentication of the E-Stamp.

© The Legal Capsule



## E-NACH

E-NACH is an electronic process to collect payment electronically. The abbreviation E-NACH stands for electronic-National Automated Clearing House.

E-NACH assists organisations to complete or collect payment within a span of few hours. The system also helps in eliminating paper work and human interaction is very minimum. This helps the process become smooth and very secure difficult to tamper with.

E-NACH system is provided by the National Payments Corporation of India which is a regulatory body constituted by the Government of India to regulate all retail payment in India.

The E-NACH system helps in securing the payment and intimating the same to the concerned parties. The full process is connected from the source bank to the destination bank.

The process commences with the creation of a mandate created by an individual through filling an electronic form. Then it goes to creation of the mandate with date specified.

Since, E-NACH is an electronic system governed by a body under the Government. It is a very safe and secure manner of collecting and making recurring payments.

Furthermore, in pursuance to Circular No. NPCI/2020-21/NACH/Circular No. 001 issued by the National Payments Corporation of India (NPCI), the NPCI has permitted the use of Aadhaar authenticated signature for all NACH members. Making both complimentary to each other.



## DIGITAL DOCUMENTS

The Information Technology Act, 2000 provides for the validity of digital, virtual and electronic documents. Thereby making them legally valid and binding in a court of law.

### ***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.*

***Sec. 4. Legal recognition of electronic records.-*** *Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—*

- (a) rendered or made available in an electronic form; and*
- (b) accessible so as to be usable for a subsequent reference.*

Section 7 of the Information Technology Act, 2000 provides for Retention of electronic records.

Section 11 of the Information Technology Act, 2000 provides for Attribution of electronic records.



**The Legal Capsule**

Chapter 4 of the Information Technology Act, 2000 provides for Attribution, Acknowledgment and Despatch of Electronic Records.

In the SEBI circular dated April 24, 2020 on the subject Clarification on Know Your Client (KYC) Process and Use of Technology for KYC; SEBI has explained that in pursuance to the Prevention of Money-Laundering (Maintenance of Records) Rules, Rule 2 (1) (cb) “equivalent e-document” means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature, including documents issued to the Digital Locker account of the investor as per Rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

© The Legal Capsule