BEST PRACTICES IN USE OF DIGITAL SIGNATURE

Presented by,
Vicky Shah

AGENDA

- Issues in E-Contracts
- Concerns
- Myths and Reality
- Legal Recognition of Digital Signature
- Digital Certificate – Digital Signature
- Precaution to Protect Digital Signature

ISSUES IN E-CONTRACTS

- Like it or not, it's common for clients to dispute a contract by questioning its original validity.

- Such a client could claim that a digital signature fails to comply with the provisions of law in place and run with it all the way to court.

- The root of most potential legal problems with an electronically signed document relate to the enforceability of that contract.

- This is one of the reasons, when you're ordering goods or agreeing to services online, for so many check-boxes acknowledging that you accept the terms of the agreement.

- **A user who checks those boxes will have a hard time arguing later that they didn't understand what they were signing**.

- The language of the contract can also be a problem.

CONCERNS

1. **How can you be certain that your e-signed documents will hold up in a court of law?**

2. Which best practices should you follow when using digital signatures in your business?

FREE EMAIL SERVICE PROVIDER TERMS - GOOGLE

- **Our Warranties and Disclaimers: - we don't make any commitments about the content within the Services, the specific functions of the Services, or their reliability, availability, or ability to meet your needs. We provide the Services "as is".**

- **Liability for our Services:** When permitted by law, Google, and Google's suppliers and distributors, will not be responsible for lost profits, revenues, or data, financial losses or indirect, special, consequential, exemplary, or punitive damages.

To the extent permitted by law, the total liability of Google, and its suppliers and distributors, for any claims under these terms, including for any implied warranties, is limited to the amount you paid us to use the Services (or, if we choose, to supplying you the Services again).

In all cases, Google, and its suppliers and distributors, will not be liable for any loss or damage that is not reasonably foreseeable.

- **Business uses of our Services: If you are using our Services on behalf of a business, that business accepts these terms. It will hold harmless and indemnify Google and its affiliates, officers, agents, and employees from any claim, suit or action arising from or related to the use of the Services or violation of these terms, including any liability or expense arising from claims, losses, damages, suits, judgments, litigation costs and attorneys' fees.**

MYTHS

- When I send a document in pdf format in an email it is a legal document.

- When I send a document in a pdf format using my email (free email service provider) it is a legal document.

REALITY

- When I send a document in a pdf format affixing my digital signature it is a legal document.

- When I send a document in a pdf format affixing my digital signature and also the email is digitally signed than it is a legal document.

- When I send a document in a pdf format affixing my digital signature, email affixing my signature and using my company/private email domain it is a legal document.

- **All three are valid but the third one is best practice.**

LEGAL RECOGNITION OF DIGITAL SIGNATURE

As per Section 3 Authentication of electronic records –

affixing his digital signature.

A document can be signed by digital signature and it will be valid.

As per Section 4 Legal recognition of electronic records –

In writing, or in typewritten or printed form.

E.g: Electronic Record, Publication of Notification in Gazette, etc…

USE OF DIGITAL SIGNATURE

SSL certificate for Website/Server (43A of IT Act)

- It authenticates the identity of the website (this guarantees visitors that they're not on a bogus site)
- It encrypts the data that's being transmitted.
- Any individual or organization that uses their website to require, receive, process, collect, store, or display confidential or sensitive information. Some examples of this information are:
  - logins and passwords
  - financial information (e.g., credit card numbers, bank accounts)
  - personal data (e.g., names, addresses, social security numbers, birth dates)
  - proprietary information
  - legal documents and contracts
  - client lists
  - medical records

Digital Signature Class 1,2,3

Class 1 Certificate: Class 1 certificates shall be issued to individuals/private subscribers.

Class 2 Certificate: These certificates will be issued for both business personnel and private individuals use.

Class 3 Certificate: This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.

E-HASTAKSHAR

e-Hastakshar: C-DAC's On-line Digital Signing Service

- e-Hastakshar offers on-line platform to citizens for instant signing of their documents securely in a legally acceptable form, under the Indian IT Act 2000 and various Rules and Regulations therein.
- C-DAC through its e-Hastakshar initiative enables citizens with valid Aadhaar ID and registered mobile number to carryout digital signing of their documents on-line.
- The digital certificate offered by C-DAC CA through the eSign service to the applicant is for one-time signing usage and shall be of class "Aadhaar-eKYC-OTP".
- C-DAC utilizes the service of Unique Identification Authority of India (UIDAI) for on-line e-authentication and Aadhaar eKYC Service.
- As a provider of Digital Signature Certificates (DSC) and eSign services, C-DAC plays the role of a Certifying Authority (CA) under the Controller of Certifying Authorities (CCA).

BEST PRACTICES

Make sure your signers know they are signing electronically.

- It is super important when it comes to creating an enforceable electronic signature on a contract.
- Anytime someone is signing a contract electronically, they must intend to do so.
- A lot of times intent is implied, although when dealing with consumers, you'll need to take extra steps to make sure.

Authenticate the identity for electronic signatures.

- Just as with traditional pen and paper signatures, you need to make sure the person signing is the right person.
- You can do this by emailing a secure link, or using some form of multi-factor authentication.

Keep good electronic records of all contracts signed electronically.

- You'll need a durable record of the contract, who signed it, and how they signed it.
- Make sure that your signers have a copy of the same electronic record.

IMPORTANT NOTE

- Only authorised person should have access to Digital Signature

- Take a undertaking/authorization before using the signature of others. (NOT RECOMMENDED) However, many business allow their accounts to use the Digital Signature and they on behalf of the company authenticate the documents.

- Many Chartered Accountants also do the same.

- Liability in such case is always with Company/Owner of Digital Signature.

THANK YOU

consult@vickyshah.in

+91-98201-05011