Legal Aspects of Digital Signatures

By

Naavi

27th Nov 2014

Agenda

- Legal Definition and Use
- Secured Digital signature
- Duties of a Subscriber
- Offences

Acceptability of Digital Signature

- **Sec-5**
  - Where any law provides that
    - information or any other matter shall be authenticated by affixing the signature or
    - any document should 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.

Section 2 (1)..

- (ta) "electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and **includes digital signature**
- (p)"Digital Signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

Legal Definition

- Sec- 3 of ITA-2000
  - **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.

What is Authentication?...

- Of an Electronic Document ?
- Confirmation of
  - Who said What?
- Who?=Identification
- What?=Content confirmation

Digital Signatures-What they are not

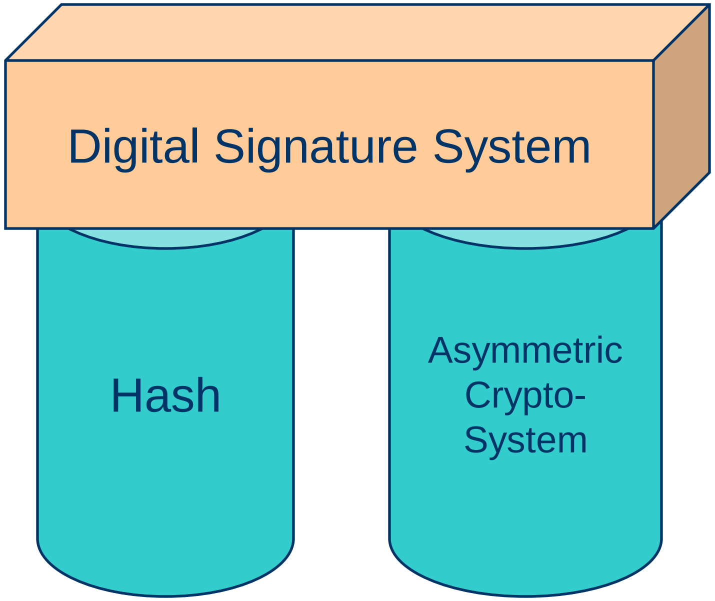
- It is not a Scanned form of a Signature
- It cannot be seen in the common sense
- This is what a digital signature may look like
  - 01001010 01011010 01000010 01000101 01001110
    01011000 01110101 01110000 01010101 01110101
    01010110 00111000 00111000 01101100 01110100
    00110010 01001101 01101100 01110110 01010011
    01010101 01000101 01100100 01001100 01001010
    01001011 01100001 01110010 01001010 00101011
- It is a variable
  - It is document specific

Digital Signature Definition

- Digital Signature
  - Of a document of a person
    - Is
    - The hash value of the document encrypted with the private key of the person

Technology Behind Digital Signatures

- Digital Signature System is built on the foundation of two technologies, Hashing and Asymmetric Crypto System



Section3A: Electronic Signature

- (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)

Section 3A..contd

- (2) 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 fulfills such other conditions which may be prescribed.

Sec 3A ..contd

- (3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated
- (4)The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule;
  - Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable
- (5)Every notification issued under sub-section (4) shall be laid before each House of Parliament

What is Secured Digital Signatures?

Section 15-Secure Electronic Signature

- An electronic signature shall be deemed to be a secure electronic signature if-
  - (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
  - (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed
    - Explanation- In case of digital signature, the "signature creation data" means the private key of the subscriber

Secure Digital Signature (Notification of October 29, 2004)

- A digital signature shall be deemed to be a secure digital signature for the purposes of the Act if the following procedure has been applied to it, namely:-
-
  - (a) that the smart card or hardware token, as the case may be, with cryptographic module in it, is used to create the key pair;
  - (b) that the private key used to create the digital signature always remains in the smart card or hardware token as the case may be;
  - (c) that the hash of the content to be signed is taken from the host system to the smart card or hardware token and the private key is used to create the digital signature and the signed hash is returned to the host system;

Secure Digital Signature (Notification of October 29, 2004)..contd

- (d) that the information contained in the smart card or hardware token, as the case may be, is solely under the control of the person who is purported to have created the digital signature;
- (e) that the digital signature can be verified by using the public key listed in the Digital Signature Certificate issued to that person;
- (f) that the standards referred to in rule 6 of the Information Technology (Certifying Authorities) Rules, 2000 have been complied with, in so far as they relate to the creation, storage and transmission of the digital signature; and
- (g)that the digital signature is linked to the electronic record in such a manner that if the electronic record was altered the digital signature would be invalidated.

Effect of Secure Digital Signature

Proof as to digital signature

- Sec 67 A (IEA):
  - Except in the case of a secure digital signature,
    - if the digital signature of any subscriber is alleged to have been affixed to an electronic record, the fact that such digital signature is the digital signature of the subscriber must be proved.

Secure Digital Signature

- Sec 85B (IEA) :In any proceedings involving a secure electronic record,
  - the Court shall presume unless contrary is proved, that
  - the secure electronic record has not been altered since the specific point of time to which the secure status relates

Secure Digital Signature..2

- (2)In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that -
- (a)the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;
- (b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature

Duties of a Subscriber

Duties of the Subscriber

- **Section 40: Generating Key Pair**
  - Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber,
    - the subscriber shall generate that_key pair by applying the security procedure.

Duties of the Subscriber..2

- **Section 41:Acceptance of Digital Signature Certificate.**
  - 1)A subscriber shall be deemed to have accepted a Digital Signature Certificate
    - if he publishes or authorizes the publication of a Digital Signature Certificate –
      - (a) to one or more persons;
      - (b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

Duties of the Subscriber..3

- Section 41…contd
  - (2)By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that –
    - (a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
    - (b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
    - (c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Duties of the Subscriber…4

- Section 42:**Control of Private key**
  - (1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure.
  - (2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.
    - **Explanation** - For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

Offences

Section 71: Penalty for misrepresentation

- Whoever
- makes any misrepresentation to, or suppresses any material fact
- from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be,
- shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

Section 73: Penalty for publishing Digital Signature Certificate false in certain particulars

- (1)No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that –
  - (a)the Certifying Authority listed in the certificate has not issued it; or
  - (b)the subscriber listed in the certificate has not accepted it; or
  - (c)the certificate has been revoked or suspended,
    - unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation
- (2)Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

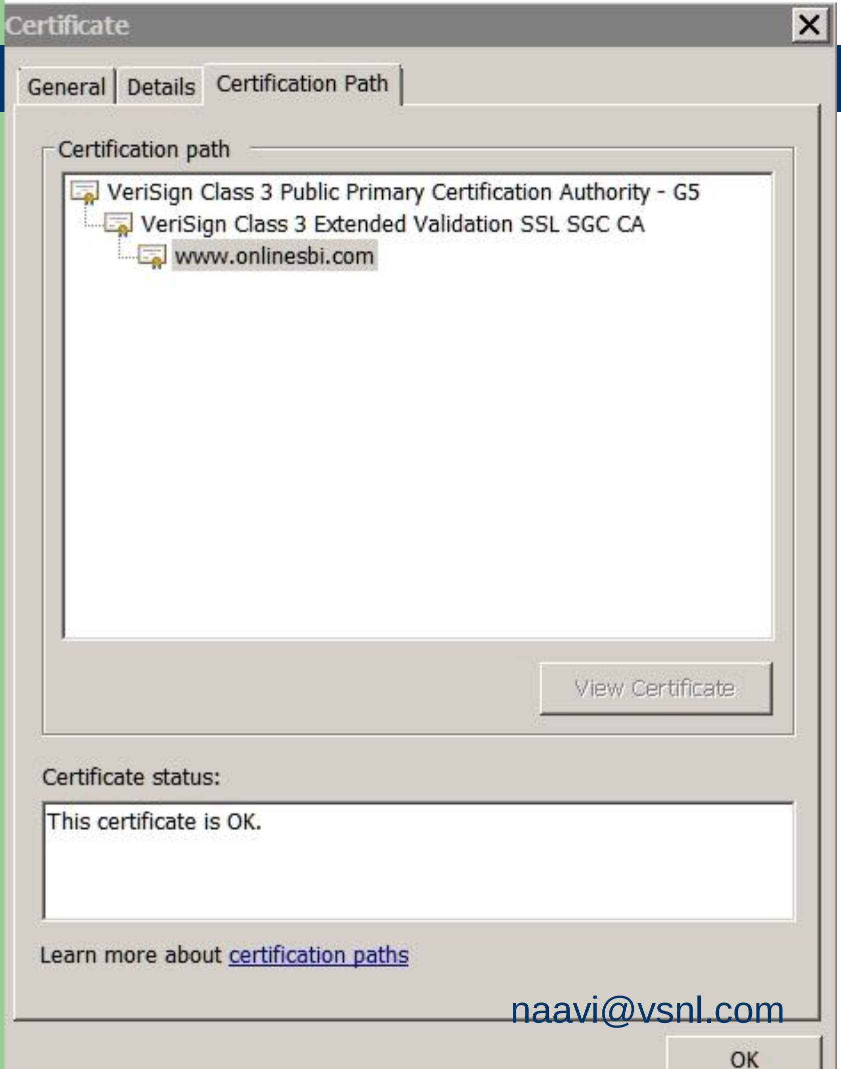
Section 74: Publication for fraudulent purpose

- Whoever
- knowingly
- creates, publishes or otherwise makes available a Digital Signature Certificate
- for any fraudulent or unlawful purpose
- shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

Duties..

- Subscriber should himself pick up the digital certificate
  - Not assign the work to a secretary
  - Never accept the CA rep to deliver a downloaded digital certificate
- Subscriber should Check if the particulars such as Name and E Mail address on the digital certificate is correct
- If Subscriber suspects compromise of private key
  - Should revoke the certificate forthwith
    - Though this would mean a loss of subscription for the unexpired period
- Any negligence may reflect as an “offence”

Issues..



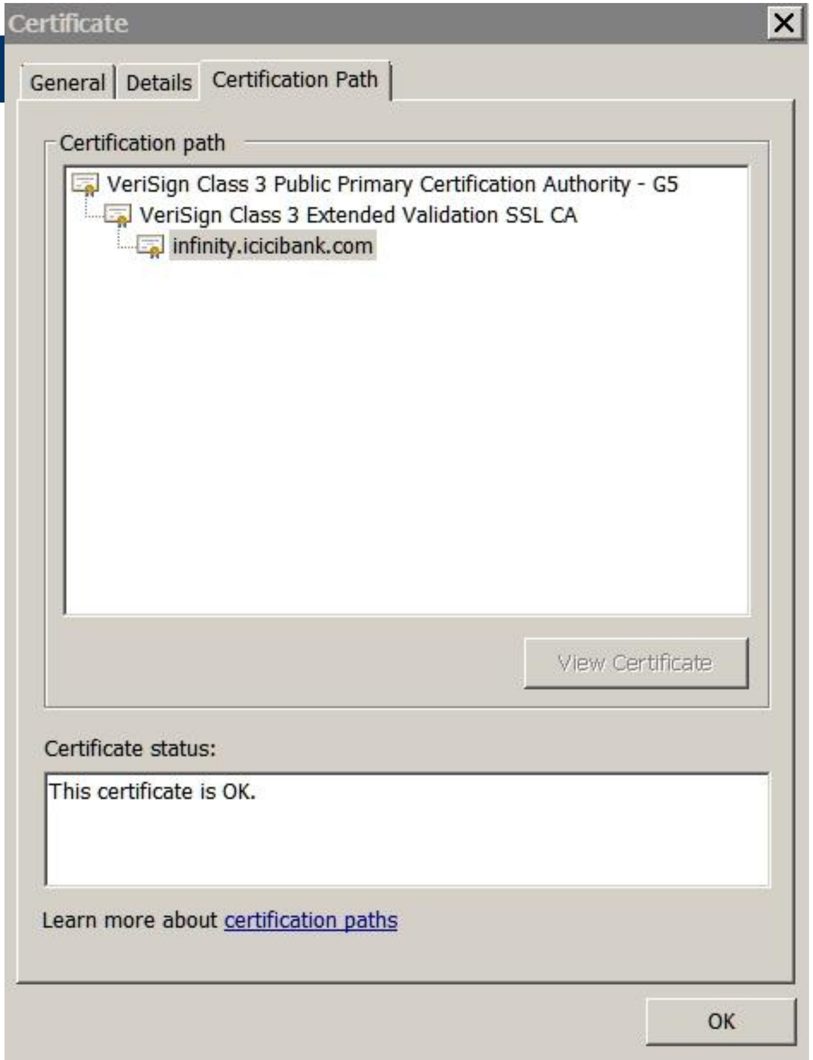
Certification path

- VeriSign Class 3 Public Primary Certification Authority - G5
  - VeriSign Class 3 Extended Validation SSL SGC CA
    - www.onlinesbi.com

Certificate status:

This certificate is OK.

Learn more about certification paths



Certification path

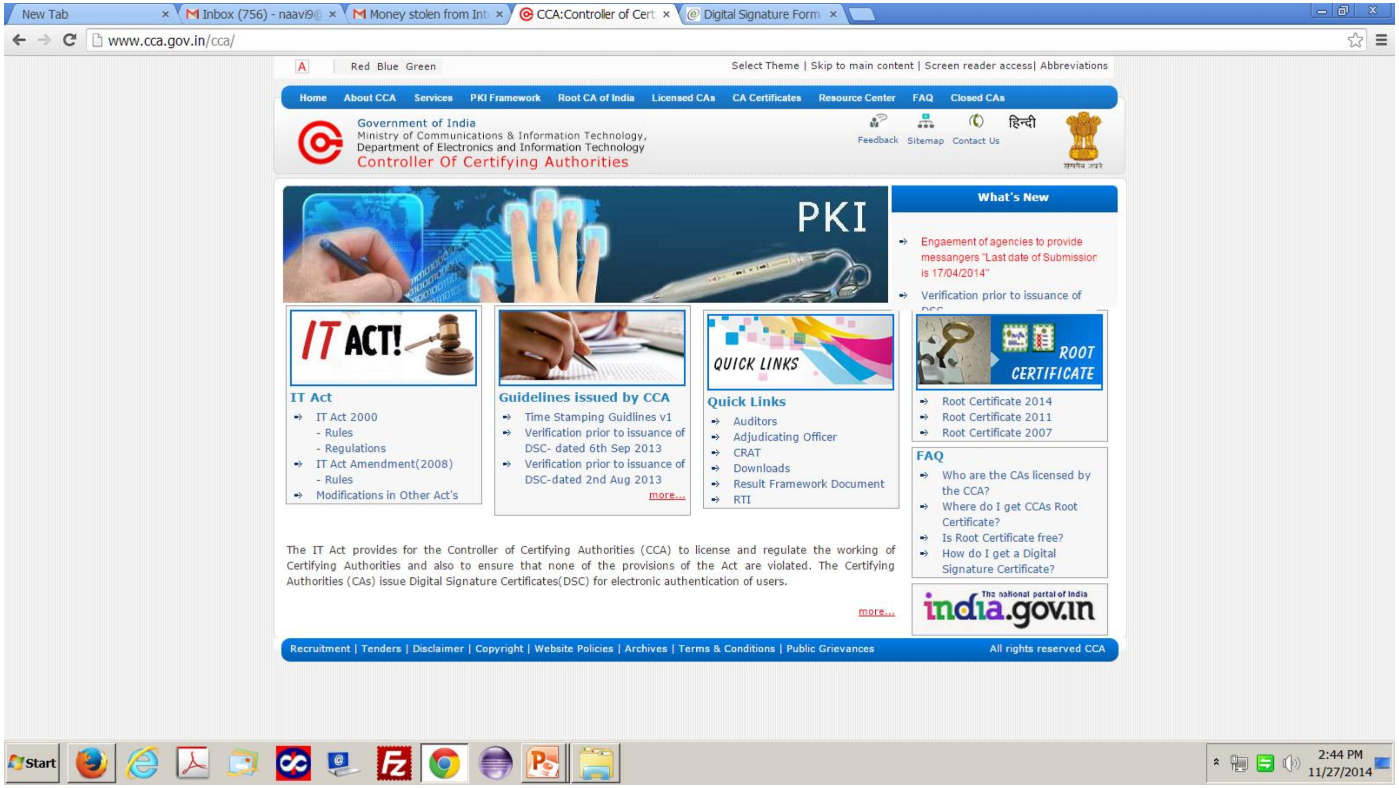
- VeriSign Class 3 Public Primary Certification Authority - G5
  - VeriSign Class 3 Extended Validation SSL CA
    - infinity.icicibank.com

Certificate status:

This certificate is OK.

Learn more about certification paths

Where is CPS?



Government of India
Ministry of Communications & Information Technology,
Department of Electronics and Information Technology
Controller Of Certifying Authorities

What's New

- Engaement of agencies to provide messangers "Last date of Submission is 17/04/2014"
- Verification prior to issuance of DSC

IT Act

- IT Act 2000
  - Rules
  - Regulations
- IT Act Amendment(2008)
  - Rules
- Modifications in Other Act's

Guidelines issued by CCA

- Time Stamping Guidlines v1
- Verification prior to issuance of DSC- dated 6th Sep 2013
- Verification prior to issuance of DSC-dated 2nd Aug 2013

more...

Quick Links

- Auditors
- Adjudicating Officer
- CRAT
- Downloads
- Result Framework Document
- RTI

- Root Certificate 2014
- Root Certificate 2011
- Root Certificate 2007

FAQ

- Who are the CAs licensed by the CCA?
- Where do I get CCAs Root Certificate?
- Is Root Certificate free?
- How do I get a Digital Signature Certificate?

The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities and also to ensure that none of the provisions of the Act are violated. The Certifying Authorities (CAs) issue Digital Signature Certificates(DSC) for electronic authentication of users.

more...

The national portal of India india.gov.in

Recruitment | Tenders | Disclaimer | Copyright | Website Policies | Archives | Terms & Conditions | Public Grievances   All rights reserved CCA

Dual Key Sets

- One set for Encryption
- One set for digital signing
  - Is the client equipped?
  - Escrowing..Will digital signing key is also escrowed?
  - Where is the audit report of a CA’s system?

Thank You

For More Information

Course on

“Certified Cyber Law Professional”

At
ApnaCourse.com