

Crimes relating to Digital Signature Certificates

This document is an extract from the book *Cyber Crime & Digital Evidence – Indian Perspective* authored by Rohas Nagpal. This book is available as courseware for the **Diploma in Cyber Law** and **PG Program in Cyber Law** conducted by Asian School of Cyber Laws



www.asianlaws.org

6. Crimes relating to Digital Signature Certificates

6.1 Misrepresentation

According to section 71 of the IT Act

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.

This section applies to:

1. a person, who, for obtaining a digital signature certificate-
 - a. makes a misrepresentation to the Certifying Authority,
 - b. suppresses any material fact from the Certifying Authority.

2. a person obtaining a license to operate as a Certifying Authority-
 - a. makes a misrepresentation to the Controller,
 - b. suppresses any material fact from the Controller.

Let us examine the essential terms of this section.

Misrepresentation implies “presenting information incorrectly, improperly or falsely”. There must be a deliberate intention to deceive.

Illustration

Sameer is applying for a digital signature certificate. He fills in his name as “Siddharth” and also submits photocopies of Siddharth’s passport as proof of identity.

Sameer is liable for misrepresenting information to the Certifying Authority.

Suppress implies “to withhold from disclosure”.

Illustration

Noodle Ltd is applying for a licence to become a Certifying Authority. One of the questions in the application form is “In case any of the company directors been





convicted for a criminal offence, then please mention relevant details.”

One of the Noodle directors has been convicted in the past. But, Noodle officials submit the filled in form with the answer to this question being left blank.

The officials will be liable for suppressing information from the Controller.

Material fact implies something that is relevant, pertinent or essential.

The **punishment** provided is imprisonment up to **2 years** and / or fine up to **Rs 1 lakh**.

Misrepresentation to CA or Controller (Summary)



Actions covered	Misrepresentation to CA or Controller for certificate / license.
Penalty	Imprisonment up to 2 years and / or fine up to Rs 1 lakh
Relevant authority	Judicial Magistrate First Class
Appeal lies to	Court of Session
Investigation Authorities	<ol style="list-style-type: none"> 1. Controller of Certifying Authorities (CCA) 2. Person authorised by CCA 3. Police Officer not below the rank of Deputy Superintendent
Points to mention in complaint	<ol style="list-style-type: none"> 1. Complainant details 2. Suspect details 3. How and when the contravention was discovered and by whom 4. Other relevant information



6.2 False Certificates

According to section 73 of the IT Act

(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.

Let us examine this section through some illustrations.

Illustration 1

Sameer has created a fake digital signature certificate purporting to have been issued by Noodle Certifying Authority. Sameer plans to use this certificate to carry out some financial frauds. He posts this certificate on his website. He is liable under this section.

Illustration 2

Pooja has applied to Noodle Certifying Authority for a digital signature certificate. Noodle in due course issues the certificate to Pooja. She however does not accept it as some of the details are incorrect in the certificate.

In the meanwhile Noodle Ltd publishes her certificate in their online repository. In this case Noodle Ltd will be liable under this section.

Illustration

Pooja is employed with Noodle Ltd. She has obtained a digital signature certificate for official purposes on 1st January. She quits her job on 1st July and her certificate is revoked on that day.

Noodle Ltd continues to keep Pooja's revoked certificate in its online repository even after 1st July. Noodle Ltd will be liable under this section. They will not be liable if the purpose behind keeping Pooja's certificate in their repository is to verify documents signed by Pooja between 1st January and 1st July.

The **punishment** provided for this section is imprisonment up to **2 years** and / or fine up to **Rs 1 lakh**.





Publishing False Certificates (Summary)

Actions covered	Publishing a digital signature certificate false in certain respects.
Penalty	Imprisonment up to 2 years and / or fine up to Rs 1 lakh
Relevant authority	Judicial Magistrate First Class
Appeal lies to	Court of Session
Investigation Authorities	<ol style="list-style-type: none">1. Controller of Certifying Authorities (CCA)2. Person authorised by CCA3. Police Officer not below the rank of Deputy Superintendent
Points to mention in complaint	<ol style="list-style-type: none">1. Complainant details2. Suspect details3. How and when the contravention was discovered and by whom4. Other relevant information

6.3 Fraudulent Use

According to section 74 of the IT Act

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.

Creating a digital signature certificate is technologically not a very difficult task. All that is needed is a computer running the Windows 2003 Server operating system and having Certificate Services installed. This makes it easy for criminals to create and publish digital signature certificates for fraudulent and unlawful purposes. Let us examine some of the terms used in this section.

Creates means “to bring into existence”.

Illustration

Sameer has a computer running the Windows 2003 Server operating system and having Certificate Services installed. He uses this computer to generate a digital signature certificate for himself and Pooja. He has created the said certificates.

Publishes means “to make known to others”.

Illustration

Sameer uploads Pooja’s digital signature certificate onto a publicly accessible part of his website. He has published her certificate.

The concept of **make available** can be explained using a simple illustration.

Illustration

Sameer has a computer running the Windows 2003 Server operating system and having Certificate Services installed. He uses this computer to generate a digital signature certificate in Pooja’s name. He then gives this certificate to Siddharth who plans to misuse it to spoof Pooja’s emails.

Here Sameer has made the certificate available to Siddharth for an unlawful purpose.





The **punishment** provided for violating this section is imprisonment up to **2 years** and / or fine up to **Rs 1 lakh**.

Creating certificate for unlawful use (Summary)

Actions covered	Creating or publishing a certificate for fraudulent or unlawful purpose.
Penalty	Imprisonment up to 2 years and / or fine up to Rs 1 lakh
Relevant authority	Judicial Magistrate First Class
Appeal lies to	Court of Session
Investigation Authorities	<ol style="list-style-type: none"> 1. Controller of Certifying Authorities (CCA) 2. Person authorised by CCA 3. Police Officer not below the rank of Deputy Superintendent
Points to mention in complaint	<ol style="list-style-type: none"> 1. Complainant details 2. Suspect details 3. How and when the contravention was discovered and by whom 4. Other relevant information



www.asianlaws.org

Head Office

6th Floor, Pride Senate,
Behind Indiabulls Mega Store,
Senapati Bapat Road,
Pune - 411016.
India

Contact Numbers

+91-20-25667148
+91-20-40033365
+91-20-64000000
+91-20-64006464

Email: info@asianlaws.org

URL: www.asianlaws.org