

मध्यप्रदेश शासन
सूचना प्रौद्योगिकी विभाग

e-Gov-2

क्रमांक एफ3/1/207/56

भोपाल, दिनांक 30.08.2012

3/9/2012

प्रति,

- अपर मुख्य सचिव/प्रमुख सचिव/सचिव
समस्त विभाग
मध्यप्रदेश।
2. समस्त विभागाध्यक्ष
मध्यप्रदेश शासन
मध्यप्रदेश।
3. कलेक्टर
समस्त
मध्यप्रदेश

विषय : कम्प्यूटर पर उपलब्ध दस्तावेजों को हस्ताक्षरित करने की प्रणाली
अर्थात् डिजिटल हस्ताक्षर (Digital Signature) के संबंध में विस्तृत
जानकारी।

1. पृष्ठभूमि

Seen - ई-शासन के वर्तमान युग में न केवल व्यक्तिगत कार्यों के लिए, बल्कि विभिन्न ई-गवर्नेन्स
परियोजनाओं के अंतर्गत किये जाने वाले इलेक्ट्रॉनिक संव्यवहारों आदि के अंतर्गत
5/9/12 डिजिटल हस्ताक्षर की प्रासंगिकता, उपयोगिता एवं महत्व दिन-प्रतिदिन बढ़ता जा रहा है।
शासन में उच्च स्तर पर कार्य करने वाले अधिकारियों से लेकर जमीनी स्तर पर कार्य
करने वाले अधिकारियों एवं कर्मचारियों तक अनेक योजनाओं में डिजिटल हस्ताक्षर का
प्रयोग अब अनिवार्य रूप से किया जाने लगा है। उक्त के परिप्रेक्ष्य में यह आवश्यक प्रतीत
होता है कि डिजिटल हस्ताक्षर के संबंध में सभी को स्पष्ट एवं सम्पूर्ण जानकारी हो। इसी
उद्देश्य को दृष्टिगत रखते हुए ई-गवर्नेन्स दिशा निर्देशों की श्रृंखला में द्वितीय निर्देश
डिजिटल हस्ताक्षर के विषय में जारी किये जा रहे हैं।

इस परिपत्र की प्रति

<http://www.mapit.gov.in>

पर भी उपलब्ध है

2. डिजिटल हस्ताक्षर क्या हैं ?

डिजिटल हस्ताक्षर एक इलेक्ट्रॉनिक हस्ताक्षर है, जिनका उपयोग कर किसी डिजिटल संदेश/दस्तावेज को भेजने वाले की पहचान की जाती है और यह सुनिश्चित किया जाता है कि संदेश अथवा दस्तावेज में किसी प्रकार की छेड़छाड़ या जालसाजी नहीं की गई है। डिजिटल हस्ताक्षर युक्त संदेश भेजने के बाद हस्ताक्षरकर्ता संदेश की विषय सामग्री से न तो अनभिज्ञता जाहिर कर सकता है, और ना ही इससे मुकर सकता है। इस प्रकार डिजिटल हस्ताक्षर संदेश भेजने वाले की सही पहचान सुनिश्चित करतें है और संदेश प्राप्तकर्ता को यह विश्वास दिलातें है कि प्राप्त होने वाला संदेश सही प्रेषक द्वारा भेजा गया है और यह अपने मूल स्वरूप में है।

- सूचना प्रौद्योगिकी अधिनियम-2000 की धारा 2(1)(p) में डिजिटल हस्ताक्षर को परिभाषित करते हुए कहा गया है कि डिजिटल हस्ताक्षर का आशय अधिनियम की धारा 3 में विहित प्रक्रिया अथवा किसी इलेक्ट्रॉनिक पद्धति द्वारा किसी इलेक्ट्रॉनिक अभिलेख का किसी सब्सक्राइबर द्वारा प्रमाणीकरण किया जाना है। अधिनियम की धारा 3 में डिजिटल हस्ताक्षर के निर्माण एवं सत्यापन संबंधी सम्पूर्ण प्रक्रिया वर्णित की गई है।
- सूचना प्रौद्योगिकी (संशोधन) अधिनियम-2008 के माध्यम से मूल अधिनियम में नई धारा 2(ta) सम्मिलित की गई है, जिसमें इलेक्ट्रॉनिक हस्ताक्षर को परिभाषित किया गया है। इससे स्पष्ट होता है कि डिजिटल हस्ताक्षर; इलेक्ट्रॉनिक हस्ताक्षर की व्यापक अवधारणा के अंतर्गत सम्मिलित है। तथापि निर्देशों में सुगमता को दृष्टिगत रखते हुए डिजिटल हस्ताक्षर शब्द का प्रयोग किया गया है।

3. डिजिटल हस्ताक्षर क्यों ?

वर्तमान में सभी विभागों एवं कार्यालयों में मैनुअल अभिलेखों के साथ-साथ लगभग प्रत्येक कार्य के इलेक्ट्रॉनिक अभिलेख भी रखे जाते हैं। इलेक्ट्रॉनिक अभिलेखों की कॉपी करना, संशोधन करना, अधिक संख्या में मेल या अन्य माध्यमों से वितरित करना, संग्रह करना, डेटा पुनर्प्राप्ति (Data Retrieving) करना सरलता पूर्वक संभव होता है। ऐसी स्थिति में डेटा/इलेक्ट्रॉनिक संव्यवहार की प्रमाणिकता एवं विश्वसनीयता अत्यंत महत्वपूर्ण हो जाती है। अतः जिस प्रकार स्याही हस्ताक्षर से यह सिद्ध होता है कि यह किसी पद विशेष पर पदस्थ किसी अधिकृत अधिकारी द्वारा जारी प्रमाणिक दस्तावेज है, उसी प्रकार इलेक्ट्रॉनिक दस्तावेजों की प्रमाणिकता डिजिटल हस्ताक्षर के माध्यम से ही सिद्ध की जा सकती है।

इस प्रकार डिजिटल हस्ताक्षर ई-गवर्नेन्स एवं ई-कामर्स के क्षेत्र में, इंटरनेट को सुरक्षित माध्यम के रूप में उपयोग करने के लिए अत्यंत आवश्यक है।

4. डिजिटल हस्ताक्षर की प्रमुख विशेषताएँ

4.1 डिजिटल हस्ताक्षर निम्न तीन मुख्य बातें सुनिश्चित करता है-

- ❖ **प्रमाणीकरण (Authentication)** : अर्थात् डिजिटल हस्ताक्षर के माध्यम से इलेक्ट्रॉनिक संदेश/दस्तावेज को प्रेषित करने वाले (Sender) अथवा स्रोत (Source) की पहचान को प्रमाणित करता है।
- ❖ **शुद्धता (Integrity)** : अर्थात् यदि किसी संदेश को डिजिटल हस्ताक्षरित किया गया है तो हस्ताक्षर के पश्चात् उसमें किसी भी प्रकार का परिवर्तन/संशोधन संभव नहीं है। संशोधन की स्थिति में उक्त संदेश एक नवीन संदेश होगा जिसे पुनः डिजिटल हस्ताक्षरित करना होगा।
- ❖ **स्पष्ट उत्तरदायित्व (Non-Repudiation)** : अर्थात् अपने डिजिटल हस्ताक्षर कर किसी संदेश/दस्तावेज को प्रेषित करने वाले (Sender) व्यक्ति/अधिकारी इस बात से इंकार नहीं कर सकते कि उक्त संदेश/दस्तावेज उनके द्वारा नहीं भेजा गया है।

4.2 डिजिटल हस्ताक्षर सामान्यतः केवल व्यक्ति के पक्ष में जारी किये जाते हैं।

5. डिजिटल हस्ताक्षर के प्रमुख उपयोग :

- 5.1 प्रकरणों का ऑनलाईन अध्ययन कर स्वीकृति प्रदान करना।
- 5.2 कम्प्यूटरीकृत दस्तावेजों का ऑनलाईन सत्यापन करना।
- 5.3 प्रमाणिक/अधिकृत रूप से ऑनलाईन आवेदन करना।
- 5.4 लायसेंस, परमिट, प्रमाणपत्र, स्वीकृति, इत्यादि ऑनलाईन जारी करना

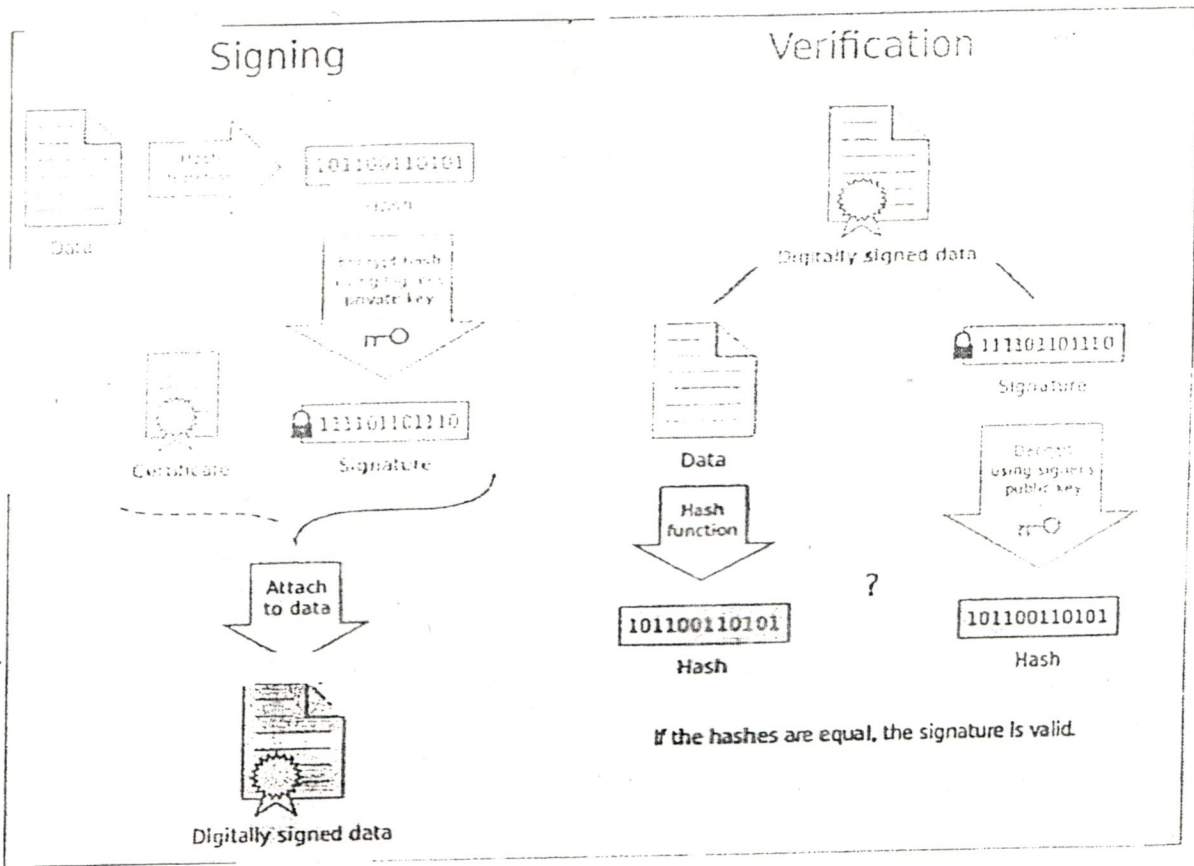
6. डिजिटल हस्ताक्षर की वैधानिक मान्यता

भारत में सूचना प्रौद्योगिकी अधिनियम 2000 एवं 2008 के तहत डिजिटल हस्ताक्षर को वैधानिक मान्यता प्रदान की गई है। डिजिटल हस्ताक्षर वैधानिक रूप से यह घोषणा करते हैं कि इनका प्रयोग कर संदेश भेजने वाले व्यक्ति की पहचान क्या है, संदेश अपने प्राप्तकर्ता के पास पहुंचने तक अपरिवर्तित रहा और संदेश भेजने वाला व्यक्ति इस संदेश में उल्लेखित बातों से मुकर नहीं सकता है।

7. डिजिटल हस्ताक्षर कैसे काम करता है ?

डिजिटल हस्ताक्षर पद्धति में 2 कुंजियों यथा "निजी कुंजी (Private Key) एवं सार्वजनिक कुंजी (Public Key) का इस्तेमाल किया जाता है। 'निजी कुंजी (Private

Key) गोपनीय पासवर्ड की तरह होती है, जिसकी जानकारी केवल डिजिटल हस्ताक्षरकर्ता के पास होती है, जबकि 'सार्वजनिक कुंजी (Public Key) सार्वजनिक होती है, जिसे कंट्रोलिंग अथोरिटी की वेबसाइट पर देखा जा सकता है। जिस दस्तावेज/संदेश पर डिजिटल हस्ताक्षर करना है, सर्वप्रथम उसकी "हेश वैल्यू" (Hash Value) निर्मित की जाती है। "हेश वैल्यू" किसी भी दस्तावेज की अद्वितीय पहचान है, जिसे "निजी कुंजी (Private Key) का उपयोग कर एनक्रिप्ट किया जाता है। "निजी कुंजी (Private Key) से एनक्रिप्ट होने वाले दस्तावेज को केवल उसकी जोड़ीदार 'सार्वजनिक कुंजी (Public Key) से ही डिजिटल किया जा सकता है। दस्तावेज प्राप्तकर्ता अपने कम्प्यूटर पर दस्तावेज की "हेश वैल्यू" दोबारा निर्मित करता है और दस्तावेज के साथ आने वाली एनक्रिप्टेड "हेश वैल्यू" को प्रेषक की 'सार्वजनिक कुंजी (Public Key) से डिजिटल करता है। यदि दोनो "हेश वैल्यू" समान होती है तो यह सुनिश्चित हो जाता है कि दस्तावेज सही व्यक्ति द्वारा भेजा गया है इसमें किसी प्रकार की जालसाजी नहीं हुई है।



7.1 उदाहरण

मान लीजिये, एक व्यक्ति (प्रेषक) दूसरे व्यक्ति (प्राप्तकर्ता), जो किसी दूसरे शहर में निवासरत है, को ईमेल के माध्यम से एक अनुबंध-पत्र भेजना चाहता है। प्रेषक इस बात

का आश्वासन देना चाहता है कि अनुबंध-पत्र सही व्यक्ति द्वारा भेजा गया है, प्रेषण के दौरान इसमें कोई जालसाजी नहीं की गई है और प्रेषक स्वयं अनुबंध पत्र में लिखी गई बातों से मुकरेगा नहीं। ऐसा करने के लिये प्रेषक डिजिटल हस्ताक्षर का उपयोग इस प्रकार करेगा :-

- प्रेषक अनुबंध-पत्र को एक ईमेल के रूप में टाईप (या कॉपी पेस्ट) करेगा।
- एक विशेष साफ्टवेयर की मदद से प्रेषक ईमेल की हेस वेल्यू (विशेष पद्धति से निकाला गया गणितीय सारांश) निर्मित करेगा।
- इसके बाद प्रेषक अपने डिजिटल हस्ताक्षर की "निजी कुंजी (Private Key) से हेस वेल्यू को एनक्रिप्ट करेगा।
- एनक्रिप्टेड हेस वेल्यू प्रेषक का डिजिटल हस्ताक्षर बन जायेगा जिसे वह अनुबंध-पत्र के ईमेल के साथ अटैच करके प्राप्तकर्ता के ईमेल आई.डी. पर भेज देगा।
- प्राप्तकर्ता इस ईमेल को खोलेगा और पुनः इसकी हेस वेल्यू निर्मित करेगा। साथ ही अटैचमेंट में प्राप्त डिजिटल हस्ताक्षर को प्रेषक की 'सार्वजनिक कुंजी (Public Key) से डिक्रिप्ट करेगा।
- यदि डिक्रिप्ट होने के बाद प्राप्त होने वाली हेस-वेल्यू और ईमेल संदेश से पुनः निर्मित की गई हेस-वेल्यू समान है तो वैधानिक रूप से यह कहा जायेगा कि ईमेल संदेश में उल्लेखित अनुबंध-पत्र उसके वास्तविक प्रेषक द्वारा ही भेजा गया है, इस ईमेल संदेश के साथ मार्ग में कोई जालसाजी नहीं की गई है और प्रेषक इस अनुबंध पत्र में उल्लेखित बातों से मुकर नहीं सकता है।

8. डिजिटल हस्ताक्षर कैसे प्राप्त किया जाये ?

सूचना प्रौद्योगिकी अधिनियम 2000 के अनुसार डिजिटल हस्ताक्षर जारी करने की कार्यवाही सर्टिफिकेशन एजेंसियों द्वारा की जाती है। कोई भी भारतीय नागरिक जो 18 वर्ष की आयु पूर्ण कर चुका है, वह उपरोक्त में से किसी भी एजेंसी से डिजिटल हस्ताक्षर प्राप्त कर सकता है। भारत में कन्ट्रोलर ऑफ सर्टिफाइंग अथोरिटी कार्यालय द्वारा सर्टिफाइंग अथोरिटी के रूप में कुल 7 संस्थानों को डिजिटल हस्ताक्षर जारी करने के लिये सर्टिफिकेशन अथोरिटी घोषित किया गया है, जिनका विवरण निम्नानुसार है।

S.No.	Certifying Authorities	Website
1	Safescript	www.safescript.com
2	NIC	www.nic.in

3	IDRBT	www.idrbtca.org.in
4	TCS	www.tcs-ca.tcs.co.in
5	MtnlTrustline	www.mtnltrustline.com
6	GNFC	www.ncodesolutions.com
7	e-MudhraCA	www.e-Mudhra.com

एन.आई.सी. द्वारा मुख्य रूप से सरकारी कार्यालयों एवं सार्वजनिक क्षेत्र की कम्पनियों को डिजिटल हस्ताक्षर प्रदान किये जाते हैं। आई.डी.आर.बी.टी द्वारा प्राथमिक तौर पर बैंकिंग एवं वित्तीय संस्थानों को डिजिटल हस्ताक्षर प्रदान किये जाते हैं। शेष 5 सर्टिफायिंग अथोरिटीज द्वारा आम नागरिक की हैसियत से सभी पात्र वयस्कों को डिजिटल हस्ताक्षर प्रदान किये जाते हैं। उल्लेखनीय है कि एनआईसी द्वारा केवल शासकीय विभागों/कार्यालयों/उपकर्मों को ही डिजिटल हस्ताक्षर प्रदान किये जाते हैं।

उदाहरणार्थ :- डिजिटल हस्ताक्षर हेतु एन.आई.सी. द्वारा निर्धारित दरें (Indicative)

	Smart Card Individual/Personal Certificate				USB Token/Key Individual/Personal Certificate			Soft Token SSL Server/Dev ice Cert. (Proc. Charge)	Renewal (Proc. Charges)
	Smart Card	Smart Card + Reader	Proc. Charge	Total	USB Token	Proc. Charge	Total		
	227/-	489/-		716/-	555/-		555/-		
	227/-	489/-	200/-	916/-	555/-	200/-	755/-	200/-	200/-
Two years (Conditions apply)									
On expiry of certificate, processing charge shall be applicable as above to renew/create the certificate on the same media. All other formalities shall be same as for a new DSC applicant, including submission of fresh DSC Application form and fees applicable.									

इसी प्रकार अन्य सभी सर्टिफायिंग अथोरिटीज द्वारा भी विभिन्न श्रेणियों में डिजिटल हस्ताक्षर प्रदान करने की दरें निर्धारित की गई हैं जो उनकी वेबसाइट पर देखी जा सकती हैं।

9. डिजिटल हस्ताक्षर हेतु आवेदन एवं रजिस्ट्रेशन किये जाने वाले दस्तावेज :

डिजिटल हस्ताक्षर प्राप्त करने हेतु आवेदन पत्र का प्रारूप उपरोक्त सभी सर्टिफायिंग अथोरिटीज की वेबसाइट से डाउनलोड किया जा सकता है। आवेदन पत्र के साथ आवेदक को अपने दो पासपोर्ट साईज फोटोग्राफ तथा अपना फोटोयुक्त वैधानिक पहचान पत्र

(उदाहरणार्थ : पैनकार्ड, ड्रायविंग लायसेंस, मतदाता पहचान पत्र अथवा कार्यालय द्वारा जारी पहचान पत्र आदि) संलग्न करना आवश्यक होता है। साथ ही आवेदन पत्र में आवेदक के कार्यालय प्रमुख की ओर से प्रमाणीकरण भी संलग्न किया जाना अनिवार्य है। पूर्ण रूप से भरे गये आवेदन पत्र को सर्टिफायिंग अथोरिटी को प्रेषित करने पर संबंधित अथारिटी द्वारा परीक्षण पश्चात डिजिटल हस्ताक्षर जारी कर दिया जाता है।

10. डिजिटल हस्ताक्षर के रूप में भौतिक रूप से निम्न सामग्री प्राप्त होती है

- डिजिटल हस्ताक्षर की Installer CD.
- Crypto Token/Smart Card

11 डिजिटल हस्ताक्षर install करने की प्रक्रिया

Token प्राप्त करने के बाद यूजर को अपने कम्प्यूटर पर Token Driven Software install करना होता है। यह सॉफ्टवेयर सर्टिफाईंग अथारिटी द्वारा जारी किया जाता है तथा यह संबंधित अथारिटी की वेबसाईट से भी डाउनलोड किया जा सकता है। यूजर को सर्वप्रथम अपने Token को अपने कम्प्यूटर के यूएसबी ड्राइव के माध्यम से Insert करना होता है उसके बाद टोकन ड्रायवर सॉफ्टवेयर Install किया जाता है। इस सॉफ्टवेयर में एक Token Administration का ऑप्शन होता है जो यूजर के डिजिटल सिग्नेचर सर्टिफिकेट को प्रदर्शित करता है। यह सर्टिफिकेट इंटरनेट पर Internet Explorer->Tools->Internet Options->Contents->Certificates लिंक ओपन करने पर भी प्रदर्शित होता है। यहाँ यूजर अपने टोकन का पासवर्ड बदल सकते हैं। इसके बाद सिस्टम पूरी तरह तैयार है और यूजर डिजिटल हस्ताक्षर करना प्रारम्भ कर सकते हैं।

12. डिजिटल हस्ताक्षर के प्रकार

डिजिटल हस्ताक्षर 4 प्रकार के होते हैं

क्रमांक	प्रकार	उपयोग	वैधता अवधि
1.	Class '0' (Zero) Certificate	यह सर्टिफिकेट केवल प्रदर्शन/परीक्षण हेतु जारी किया जाता है।	---
2.	Class '1' (One) Certificate	यह सर्टिफिकेट निजी उपयोग के लिये जारी किया जाता है। यह सामान्य स्तर के डिजिटल हस्ताक्षर होते हैं जो मात्र उपयोगकर्ता और उसके इमेल अकाउन्ट को सत्यापित करते हैं। जहाँ उच्च स्तरीय विश्वसनीयता एवं वचनबद्धता की आवश्यकता नहीं होती है वहा इस स्तर के सर्टिफिकेट उपयोग में लाये जाते हैं।	1 या 2 वर्ष।
3.	Class '2'	यह सर्टिफिकेट निजी उपयोग एवं व्यवसायिक	1 या 2 वर्ष।

(Two)
Certificate

उपयोग, दोनों के लिये जारी किया जाता है। यह मध्यम स्तर के डिजिटल हस्ताक्षर होते हैं, जिनका उपयोग छोटे वित्तीय लेनदेन से संबंधित दस्तावेजों या आवेदनों की विश्वसनीयता सिद्ध करने के लिये उपयोग किये जाते हैं।

4 Class '3'
(Three)
Certificate

यह सर्टिफिकेट व्यक्तियों एवं संस्थाओं दोनों को जारी किया जाता है। यह एक अत्यंत उच्च स्तरीय वचनबद्धता के प्रमाण पत्र हैं जो कि मुख्यतः ई-कॉमर्स गतिविधियों हेतु जारी किये जाते हैं। व्यक्तियों के लिए जारी करने से पूर्व सर्टिफाईंग अथॉरिटी के सामने उन व्यक्तियों की व्यक्तिगत उपस्थिति अनिवार्य होती है

या 2 वर्ष।


नोट सामान्यतः शासकीय अधिकारियों/कर्मचारियों के लिए श्रेणी-2 के डिजिटल हस्ताक्षर का प्रयोग किया जाता है।

13. डिजिटल हस्ताक्षर एवं स्याही के हस्ताक्षर में अंतर

हस्तलिखित हस्ताक्षर को स्कैन कर कम्प्यूटर द्वारा किसी डिजिटल दस्तावेज पर लगाया जाना डिजिटल हस्ताक्षर नहीं है। डिजिटल हस्ताक्षर क्रिप्टो एल्गोरिदम (Crypto Algorithm) से किसी दस्तावेज की हेश वेल्यू का एन्क्रिप्टेड स्वरूप है। स्याही द्वारा निर्मित हस्ताक्षर को जालसाजी द्वारा पुनः निर्मित करना संभव है किन्तु डिजिटल हस्ताक्षर को जालसाजी द्वारा निर्मित करना लगभग असंभव है। जालसाजी से बचने के लिये स्याही द्वारा निर्मित हस्ताक्षर दस्तावेज के प्रत्येक पृष्ठ पर अंकित करना अनिवार्य होता है, जिसमें समय एवं श्रम दोनों की आवश्यकता होती है। किन्तु डिजिटल हस्ताक्षर करते समय पृष्ठों की संख्या या दस्तावेज के प्रकार से कोई फर्क नहीं पड़ता है।

अंतर

क्रमांक	विशेषता	इंक (स्याही) हस्ताक्षर	डिजिटल हस्ताक्षर
2.	प्रमाणीकरण (Authentication)	जालसाजी से बदले जा सकते हैं	किसी प्रकार की जालसाजी संभव नहीं
	शुद्धता (Integrity)	हस्ताक्षर, दस्तावेज में अंकित मैटर पर निर्भर नहीं होते।	हस्ताक्षर, दस्तावेज में अंकित मैटर पर निर्भर होते हैं। मैटर में किसी प्रकार का संशोधन/छेड़छाड़ संभव नहीं है।
3.	स्पष्ट उत्तरदायित्व (Non-Repudiation)	सही हस्ताक्षर के मिलान के लिए हस्तलेखन विशेषज्ञों/नोटरी/गवाह की सेवाएँ लेना पड़ती हैं	पूर्णतः त्रुटि रहित हैं और कोई भी कम्प्यूटर उपयोग करने वाला हस्ताक्षर की सत्यता को आसानी से पहचान सकता है।

	Handwritten Signature	Digital Signature
Concept		Digital signature using asymmetric encryption / decryption method 13808263048077766830 1020303023030230230 40204060030030003003 00043040384030400004 40300234808404807008
Problem	Reusable	Impossible to reuse

Handwritten Versus Digital Signatures

14. डिजिटल हस्ताक्षर की वैधता की समाप्ति :

डिजिटल हस्ताक्षर प्रमाण पत्र अधिकतम 2 वर्ष तक की अवधि के लिये वैध होते हैं। किन्हीं विशेष परिस्थितियों, जैसे नाम में परिवर्तन, डिजिटल हस्ताक्षर उपयोगकर्ता का सेवा से पृथक होना, "प्रायवेट की" की गोपनीयता भंग होने की आशंका होना, आदि में अवसान तिथि के पूर्व भी इनकी वैधता सर्टिफायिंग अथोरिटी द्वारा समाप्त की जा सकती है।

15. डिजिटल सर्टिफिकेट क्या है ?

डिजिटल सर्टिफिकेट किसी व्यक्ति विशेष की पहचान को प्रमाणित करने वाला इलेक्ट्रॉनिक दस्तावेज है जिसे हम ड्राइविंग लायसेंस, पासपोर्ट अथवा अन्य किसी कार्ड के इलेक्ट्रॉनिक पूरक के रूप में परिभाषित कर सकते हैं। डिजिटल सर्टिफिकेट व्यक्ति की पहचान को प्रमाणित करता है जिससे किसी सूचना अथवा सेवा को ऑनलाइन प्राप्त करने का अधिकार हमें प्राप्त हो सकता है। ई-बैंकिंग, ई-कॉमर्स एवं अन्य इलेक्ट्रॉनिक सेवाओं, जिन्हें कि अब सीधे घर बैठे प्राप्त किया जा सकता है, के परिप्रेक्ष्य में संव्यवहार की गोपनीयता, संरक्षा तथा पहचान के प्रमाण हेतु इसे अब बहुतायत में प्रयोग किया जाता है। डिजिटल सर्टिफिकेट किसी भी अधिकृत सर्टिफिकेशन अथोरिटी के द्वारा जारी किया जा सकता है।

16. डिजिटल हस्ताक्षर के प्रयोग में आवश्यक सावधानियाँ :

सूचना प्रौद्योगिकी अधिनियम 2000 के तहत डिजिटल हस्ताक्षर को वैधानिक मान्यता प्रदान की गई है। किसी दस्तावेज पर डिजिटल हस्ताक्षर करने के बाद हस्ताक्षरकर्ता का दस्तावेज में उल्लेखित तथ्यों से मुकरना कानूनन दण्डनीय कृत्य है। अतः डिजिटल हस्ताक्षर का उपयोग करते समय सामान्यतः निम्न बातों का ध्यान रखना चाहिये :-

1. प्रायः उपयोगकर्ता डिजिटल हस्ताक्षर करने हेतु अपना किप्टो टोकन अपने निज सचिव या अधीनस्थों को दे देते हैं जो कि एक गंभीर लापरवाही है। "प्रायवेट की" किसी भी दशा में अन्य व्यक्ति को नहीं दी जाना चाहिये।

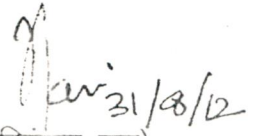
2. यदि हस्ताक्षर करने हेतु किसी अन्य व्यक्ति को अधिकृत किया जाना है, तो अधिकृत किये गये व्यक्ति को स्वयं के डिजिटल हस्ताक्षर का उपयोग करना चाहिये।
3. किसी भी संबंधित अधिकारी/कर्मचारी के निलंबित होने या सेवा से पृथक होने/विभागीय जाँच/अनियमितताओं की पुष्टि होने अथवा आपराधिक प्रकरण दर्ज होने की दशा में उसका डिजिटल हस्ताक्षर प्रमाण पत्र सभी ई-गवर्नेन्स एप्लीकेशन्स से अस्थाई तौर पर तुरंत निष्क्रिय किया जाना चाहिये। स्थानांतरित अधिकारी अपनी नवीन पदस्थापना पर यथावत अपने वर्तमान डिजिटल हस्ताक्षर का प्रयोग कर सकेंगे। नये अधिकारी द्वारा कार्यभार ग्रहण करने के पहले कार्यभार प्रदान करने वाले अधिकारी को जारी डिजिटल हस्ताक्षर प्रमाणपत्र को उक्त पदस्थापना स्थल पर स्थानांतरित हुए अधिकारी द्वारा जिन ई-गवर्नेन्स एप्लीकेशन्स में अपने डिजिटल हस्ताक्षर प्रयोग किये जा रहे थे, उन सभी के निष्क्रिय करने की कार्यवाही पूर्ण की जाना चाहिये। साथ ही उसके कंटेन्शियल जो ईगवर्नेन्स एप्लीकेशन में दर्ज है, उन्हे भी निष्क्रिय कर देना चाहिये, जिससे प्रमाणपत्र निरस्त होने की अवधि तक वह एप्लीकेशन का प्रयोग न कर सके।
4. यदि डिजिटल हस्ताक्षर से संबंधित गोपनीयता भंग हो चुकी है या इसकी आशंका है, तो भी डिजिटल हस्ताक्षर प्रमाण पत्र को निष्क्रिय करने के लिये सर्टिफायिंग अथोरिटी से तुरंत अनुरोध किया जाना चाहिये।
5. डिजिटल हस्ताक्षर के लिए भौतिक रूप से प्राप्त Crypto Token/Smart Card के गुम जाने अथवा चोरी हो जाने की स्थिति में यथा शीघ्र इसकी लिखित सूचना संबंधित क्षेत्र के नजदीकी पुलिस स्टेशन पर दी जानी चाहिए।
6. कार्यालय/विभाग द्वारा अपने अधिकारियों को प्रदान किये गये डिजिटल हस्ताक्षर और जिन कार्यों में इनका उपयोग किया जाना है, इसकी विस्तृत जानकारी इलेक्ट्रॉनिक डाटाबेस के रूप से संधारित की जाना चाहिये। कार्यालय की ईगवर्नेन्स एप्लीकेशन डिजिटल हस्ताक्षर का उपयोग करने का विकल्प देने के पूर्व उक्त डाटाबेस में उल्लेखित अनुमतियों के संदर्भ जरूरी पुष्टियां करेगी।
17. डिजिटल हस्ताक्षर के संबंध में सामान्य जिज्ञासाओं का स्पष्टीकरण (FAQs) :
 - डिजिटल हस्ताक्षर का आकार : डिजिटल हस्ताक्षर का आकार संबंधित दस्तावेज की हेश वेल्यू के आकार पर निर्भर करता है। यह कुछ बाईट का हो सकता है।

- एक से अधिक डिजिटल हस्ताक्षर : एक व्यक्ति एक से अधिक डिजिटल हस्ताक्षर प्रमाणपत्रों का उपयोग कर सकता है। जैसे एक निजी उपयोग के लिये और दूसरा कार्यालयीन उपयोग के लिये।
- डिजिटल हस्ताक्षर से संबंधित विवादों का निराकरण : सूचना प्रौद्योगिकी अधिनियम 2000 में डिजिटल हस्ताक्षर को स्याही से हस्तलिखित हस्ताक्षर के समान माना गया है। अतः विवाद की दशा में न्यायलयीन प्रक्रिया भी समान होगी।
- डिजिटल हस्ताक्षर का स्वरूप : डिजिटल हस्ताक्षर का स्वरूप संबंधित दस्तावेज के अनुसार बदलता रहता है, लेकिन यह प्रत्येक दस्तावेज के लिये यह अद्वितीय होता है।
- किसी दूसरे व्यक्ति द्वारा आपके डिजिटल हस्ताक्षर का उपयोग किया जाना : सूचना प्रौद्योगिकी अधिनियम 2000 के अनुसार यदि आपका डिजिटल हस्ताक्षर किसी अन्य व्यक्ति द्वारा उपयोग किया जाता है तो ऐसे हस्ताक्षर से जारी इलेक्ट्रानिक दस्तावेज आपके हस्ताक्षर से जारी माने जायेंगे और इसका सम्पूर्ण उत्तरदायित्व आपका होगा।
- डिजिटल हस्ताक्षर का सत्यापन : डिजिटल हस्ताक्षर के सत्यापन के लिये 3 चीजों तथा "पब्लिक की", फुल टैम पैर की,आर.एल (सर्टिफिकेशन रिजोलेशन सिस्ट) की आवश्यकता होती है। अतः ईमार्केटप्लेस एप्लीकेशन में उपरोक्त से संबंधित डाटावेज लेना चाहिये, जिससे कि डिजिटल हस्ताक्षरों को सत्यापन किया जा सके।
- पृथक-पृथक कम्प्यूटरों पर डिजिटल हस्ताक्षर का उपयोग :- यदि कोई उपयोगकर्ता पृथक-पृथक कम्प्यूटरों पर डिजिटल हस्ताक्षर का उपयोग करता है तो इसमें सुरक्षा से संबंधित कोई जोखिम नहीं है यदि "प्रायवेट की" स्मार्टकार्ड या फिफ्टो टोकन में निहित है और उपयोगकर्ता इसे कम्प्यूटर पर नहीं छोड़ता है।

डिजिटल हस्ताक्षर के संबंध में उपरोक्त विस्तृत जानकारी प्रदान करने का उद्देश्य आपको डिजिटल हस्ताक्षर एवं इसके अनुप्रयोग से अवगत कराना है साथ ही यह सुनिश्चित करना भी है कि डिजिटल हस्ताक्षर का उपयोग करते समय संबंधित अधिकारी द्वारा जरूरी सावधानियाँ बरती जायेंगी। समस्त विभाग अपने अधीनस्थ समस्त शासकीय निगम/मंडलों तथा विभाग में डिजिटल हस्ताक्षर के वर्तमान एवं संभावित भावी शासकीय उपयोगकर्ताओं को इस परिपत्र की छायाप्रतियाँ उपलब्ध करायें। को भी आवश्यकतानुसार इस विषय पर एन.आई.सी. के सहयोग से संक्षिप्त प्रशिक्षण बैठक भी आयोजित की जा सकती है जिससे संबंधित उपयोगकर्ताओं को स्पष्ट जानकारी प्रदान करने के साथ-साथ उनकी जिज्ञासाओं का भी समाधान हो सके। डिजिटल हस्ताक्षर संबंधी कार्यवाहियों के

प्रशासन के लिए यथा स्थिति जिला सूचना विज्ञान अधिकारी अथवा प्रभारी अधिकारी, जिला ई-गवर्नेन्स सोसायटी को नोडल अधिकारी के रूप में नामांकित किया जा सकता है।

आपके विभाग/कार्यालय में डिजिटल हस्ताक्षर के प्रयोग में यदि किसी प्रकार की कठिनाई आ रही हो अथवा आप इस संबंध में कोई सुझाव देना चाहते हैं तो कृपया सूचना प्रौद्योगिकी विभाग को अवश्य प्रेषित करें ताकि डिजिटल हस्ताक्षर संबंधी वर्तमान व्यवस्थाओं में आवश्यक संशोधन/परिवर्धन कर इसे अधिक उपयोगी तथा User Friendly बनाया जा सके। डिजिटल हस्ताक्षर के संबंध में और अधिक जानकारी/जिज्ञासा समाधान/कठिनाईयों से अवगत कराने के लिए श्री नन्दकिशोर ब्रम्हे, विशेष कर्तव्यस्थ अधिकारी, म.प्र. राज्य इलेक्ट्रॉनिक्स विकास निगम से ई-मेल brahme@mpsedc.com अथवा मोबाईल नं. 09425008086 पर सम्पर्क किया जा सकता है।


(हरिरजन राव)

सचिव

मध्यप्रदेश शासन

सूचना प्रौद्योगिकी विभाग

पृ.क. एफ 3 /207/56
प्रतिलिपि :

भोपाल, दिनांक 30.08.2012
31/9/2012

1. प्रबंध संचालक, म.प्र. राज्य इलेक्ट्रॉनिक्स विकास निगम, भोपाल
2. मुख्य कार्यपालन अधिकारी, म.प्र. एजेन्सी फॉर प्रमोशन ऑफ इन्फारमेशन टेक्नोलॉजी, भोपाल
3. राज्य सूचना विज्ञान अधिकारी, एन.आई.सी., विन्ध्याचल भवन, भोपाल
4. श्री नन्दकिशोर ब्रम्हे, विशेष कर्तव्यस्थ अधिकारी, म.प्र. राज्य इलेक्ट्रॉनिक्स विकास निगम की ओर सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।
5. श्रीमती संहिता पेंडसे, उप प्रबंधक, म.प्र. एजेन्सी फॉर प्रमोशन ऑफ इन्फारमेशन टेक्नोलॉजी (मैप-आई.टी.) की ओर उक्त परिपत्र को विभाग एवं मैप-आई.टी. की वेबसाइट पर उपलब्ध कराने हेतु प्रेषित।


(सुधीर कुमार कोचर)

अवर सचिव

मध्यप्रदेश शासन

सूचना प्रौद्योगिकी विभाग

M.A.P. 11
Sl.No. 3587
Date 5/9/12