International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
ISSN : 2581-9925, Volume 01, No. 04, October - December, 2019, pp.81-86

डिजिटल हस्ताक्षर प्रमाण–पत्र

हरगोविन्द खरेरा*

सार

डिजिटल हस्ताक्षर या डिजिटल हस्ताक्षर योजना किसी डिजिटल संदेश या दस्तावेज की प्रमाणिकता को निरूपित करने के लिए एक गणितीय योजना है। एक मान्य डिजिटल हस्ताक्षर, प्राप्तकर्त्ता को यह विश्वास दिलाता है कि संदेश किसी ज्ञात प्रेषक द्वारा तैयार किया गया है और उसे पारगमन में बदला नहीं गया था। डिजिटल हस्ताक्षर सामान्यतः सॉफ्टवेयर वितरण लेन–देन और ऐसे अन्य मामलों में प्रयुक्त होते हैं, जहाँ जालसाजी और छेड़छाड का पता लगाया जा सकता है।

डिजिटल हस्ताक्षर का इस्तेमाल अक्सर इलेक्ट्रॉनिक हस्ताक्षर कार्यान्वित करने के लिए होता है, जो कि एक ऐसा व्यापक शब्द है, जिसका तात्पर्य ऐसे किसी इलेक्ट्रॉनिक डाटा से है, जो हस्ताक्षर के उद्देश्य के लिए होता है, लेकिन सभी इलेक्ट्रानिक हस्ताक्षरों में डिजिटल हस्ताक्षर का उपयोग नहीं किया जाता है। संयुक्त राज्य अमेरिका सहित कुछ देशों और यूरोपीय संघ में, इलेक्ट्रॉनिक हस्ताक्षरों का कानूनी महत्व है। यद्यपि इलेक्ट्रॉनिक हस्ताक्षर से सम्बन्धित कानून हमेशा यह स्पष्ट नहीं करते कि कानूनी परिभाषा को परे रखते हुए क्या वे डिजिटल बीज–लेखन हस्ताक्षर के अर्थ में यहाँ प्रयुक्त हैं और इसलिए उनका महत्व कुछ हद तक भ्रामक हो सकता है।

डिजिटल हस्ताक्षर एक प्रकार की असममित क्रिप्टोग्राफी हैं। एक असुरक्षित चैनल से प्रेषित एक उपयुक्त रूप से कार्यान्वित डिजिटल हस्ताक्षर, प्राप्तकर्त्ता को यह विश्वास दिलाते हैं कि संदेश, अधियाचित प्रेषक द्वारा ही भेजा गया था। कई मायनों में डिलिटल हस्ताक्षर पारंपरिक हस्तलिखित हस्ताक्षर के बराबर हैं, उचित रूप से कार्यान्वित डिजिटल हस्ताक्षर के साथ जालसाजी, हस्तलिखित किस्म की तुलना में कठिन है। यहाँ प्रयुक्त अर्थ में डिजिटल हस्ताक्षर प्रणालियाँ गुप्त रूप पर आधारित हैं और सही तरीके से लागू किए जाने पर ही ये प्रभावी हो सकती हैं। डिजिटल हस्ताक्षर गैर–अस्वीकरण भी प्रदान कर सकते हैं, यानि हस्ताक्षरकर्त्ता सफलतापूर्वक यह दावा नहीं कर सकता है कि उसने संदेश पर हस्ताक्षर नहीं किए हैं, जबकि साथ में यह दावा हो कि उनकी निजी कुंजी गोपनीय है, साथ ही कुछ गैर–अस्वीकरण प्रणालियाँ डिजिटल हस्ताक्षर के लिए समय की मुहर पेश करती हैं, ताकि निजी कुंजी के उजागर हो जाने पर, हस्ताक्षर फिर भी मान्य रहता है। डिजिटल रूप से हस्ताक्षित संदेश, बिटस्ट्रिंग के रूप में निरूपणीय कुछ भी हो सकते है।

परिचय

हस्ताक्षर किसी भी कार्य को पूरा करने के लिए लेन–देन से सम्बन्धित समस्त दस्तावेजों को पूरा करने के लिए एक पक्षकार दूसरे पक्षकार को कोई अधिकार या दायित्व सौंपता है, तो उस पर अपने हस्ताक्षर करने के पश्चात् ही सौपता है क्योंकि बिना हस्ताक्षर के कोई भी प्रमाण–पत्र वैधानिक रूप से प्रमाणित नहीं होता है।

* सहायक आचार्य, ई.ए.एफ.एम. विभाग, राजकीय वाणिज्य महाविद्यालय एवं शोधार्थी, आर.आर.बी.एम.यू., अलवर, राजस्थान।

इसलिए यह आवश्यक है कि किसी दस्तावेज को वैधानिक दस्तावेज बनाना हो तो उस पर सम्बन्धित अधिकारी या प्रेषक के हस्ताक्षर होना आवश्यक है। प्राचीन समय से अब तक यह परम्परा चली आ रही है कि एक व्यक्ति दूसरे व्यक्ति को कोई प्रपत्र देता है तो अपने हस्ताक्षर करके या अपना अपना अगूंठा लगाकर देता है। यह माना जाता है कि किसी एक व्यक्ति के द्वारा किए गए हस्ताक्षर उस व्यक्ति की निजी पहचान होती है। जिसका कोई दुरूपयोग नहीं कर सकता है। लेकिन बढ़ती प्रौद्योगिकी एवं अपराध के बढ़ने के साथ–साथ किसी हस्ताक्षर के जाली हस्ताक्षर करके खुलेआम निडरता से आपराधिक गतिविधियों का अंजाम दिया जाने लगा है। इन आपराधिक गतिविधियों में जैसे किसी दूसरे व्यक्ति की सम्पत्ति कोई अपने जाली हस्ताक्षर करके बेच देता है, किसी अन्य व्यक्ति के बैंक अकाउन्ट से दूसरा व्यक्ति जाली हस्ताक्षर करके धन निकासी कर लेता है, किसी निजी या सरकारी कम्पनी के अधिकारी के जाली हस्ताक्षर करके उस कम्पनी का कर्मचारी लेन–देन कर लेता है। किसी सरकारी विभाग में बिलों के भुगतान हेतु आहरण एवं वितरण अधिकारी के हस्ताक्षर होते है, तो ट्रेजरी कोषाधिकारी बिलों का भुगतान करता है। इस प्रकार आहरण एवं वितरण अधिकारी के जाली एवं अवैधानिक हस्ताक्षर करके भुगतान उठाया जा सकता है। उदाहरण के तौर पर बाबू शोभाराम राजकीय कला महाविद्यालय, अलवर में कार्यरत एक प्रवक्ता ने बैंक से गृह ऋण ले लिया और उसकी किश्तों का भुगतान भी नहीं किया। भुगतान में विलम्ब की सूचना बैंक ने प्राचार्य बाबू शोभाराम राजकीय कला महाविद्यालय, अलवर को भेजी तब यह पता चला कि उक्त लोन प्रकरण के सम्बन्ध में प्राचार्य, बाबू शोभाराम राजकीय कला महाविद्यालय, अलवर को पता ही नही है और इस प्रकरण के बारे में सम्बन्धित प्रवक्ता से पूछा तो पता चला कि इस लोन प्रकरण में प्राचार्य के जाली हस्ताक्षर करके लोन उठाया गया है। ऐसे ही अनेक हस्ताक्षर आर्किटेक्चर या विशेषज्ञ होते है जो जाली हस्ताक्षर करके किसी लेन–देन के कार्य अवैधानिक अंजाम देते हैं। इस प्रकार की गतिविधियों को रोकने हेतु एवं बदलते समय के आधार पर विदेशों में अपनाई जा रही डिजिटल हस्ताक्षर तकनीकी प्रणाली को अपनाने या लागू करने की आवश्यकता महसूस की गई।

डिजिटल हस्ताक्षर किसी सन्देश/दस्तावेज की प्रमाणिकता निरूपित करने के लिए एक गणितीय अंक प्रणाली है। प्रमाणित किया हुआ डिजिटल हस्ताक्षर दस्तावेज प्राप्तकर्त्ता को यह विश्वास दिलाता है कि उक्त संदेश किसी ज्ञात प्रेषक के द्वारा तैयार किया था। उसे परगमन प्रक्रिया में किसी भी तरह से नहीं बदला गया है। डिजिटल हस्ताक्षर एक विशेष प्रकार के असममित क्रिप्टोग्राफी प्रौद्योगिकी है जो परम्परागत हस्ताक्षर प्रणाली से अधिक विश्वसनीय है, क्योंकि डिजिटल हस्ताक्षर प्रायः एक विशेष प्रकार के सॉफ्टवेयर वितरण, वित्तीय लेनदेन तथा ऐसे अनेक प्रकरणों में प्रयुक्त होते हैं, जहाँ जालसाजी, छेड़छाड़, कपट, गबन या चोरी का पता लगाना अधिक महत्वपूर्ण, आवश्यक एवं आसान होता है। डिजिटल हस्ताक्षर तकनीकी सबसे अधिक गुप्त होती है। इस प्रक्रिया में एक प्रेषक किसी दूसरे प्रापक को इलेट्रिकल संदेश भेजता है, जिसकी जानकारी सिर्फ प्रेषक व प्रापक को होती है, क्योंकि प्रेषक जिस तकनीकी से सन्देश भेजता है, उस तकनीकी की गुप्त कुन्जी किसी अन्य व्यक्ति के पास नहीं हो सकती है और अन्य व्यक्ति उसकी कुन्जी की कॉपी नही कर सकता है। यह कुन्जी सिर्फ प्रेषक के पास बहुत ही अधिक गोपनीय होती है।

,frgkfld ifjn'';

डिजिटल हस्ताक्षर प्रमाण–पत्र की अवधारणा का वर्णन सर्वप्रथम व्हाइटफिल्ड डिफ्टी और मार्टिन हेलमैन ने वर्ष 1976 में किया था। उस समय उन्होंने इस प्रौद्योगिकी का केवल अनुमान ही लगाया था। इनके पश्चात् रोनाल्ड रिवेस्ट, रामीर व लेन एडलमेन ने आर.एस.ए. एल्गोरिथद्म का आविष्कार किया। आगे चलकर इस एल्गोरिथद्म का उपयोग डिजिटल हस्ताक्षरों के लिए प्रयोग में लिया जाने लगा। डिजिटल हस्ताक्षर का उपयोग करने से सम्बन्धित डिजिटल हस्ताक्षर सॉफ्टवेयर पैकेज सर्वप्रथम वर्ष 1989 में लोट्स नोट्स 1.0 बाजार में बेचने के लिए उतारा गया, जिसमें भी आर.एस.ए. एल्गोरिथद्म का ही अधिक उपयोग किया गया था। आर. एस.ए. प्रणाली के विकास के पश्चात् अन्य डिजिटल हस्ताक्षर प्रौद्योगिकी भी विकसित की गई। जैसे लैक्पोर्ट हस्ताक्षर, मर्कल हस्ताक्षर (जो मर्कल ट्री या केवल हैश ट्री के नाम से भी जाने जाते हैं) तथा राबिन हस्ताक्षर आदि। संयुक्त राज्य अमेरिका सहित कुछ देश एवं युरोपीय संघ में इलैक्ट्रॉनिक हस्ताक्षरों का कानूनी महत्व है।

विभिन्न देशों में इलैक्ट्रॉनिक/डिजिटल हस्ताक्षर को कानूनी वैद्यता प्रदान करने के पश्चात् भारत में भी डिजिटल हस्ताक्षर के अन्तर्गत विभिन्न कार्यों के संचालन पर जोर दिया जाने लगा। जिसका मुख्य उद्देश्य यह है कि सरकारी कार्यों के संचालन में खर्च होने वाले स्टेशनरी एवं समय की बचत तथा सुरक्षा व्यवस्था को बढ़ाया जा सके। क्योंकि सरकारी कार्य पूरा करने में समय तथा कागज अधिक व्यय होते हैं। डिजिटल हस्ताक्षर प्रमाण–पत्र योजना को सफल बनाने के लिए सरकार ने इसे कानूनी वैधता प्रदान करने के लिए सूचना प्रौद्योगिकी अधिनियम में शामिल किया है।

भारत सरकार ने सूचना प्रौद्योगिकी अधिनियम 2000 में एसिमेट्रिक क्रिप्टोसिस्टमस पर आधारित डिजिटल हस्ताक्षर को आवश्यक वैधानिक अधिकार प्रदान किया है। इसके अन्तर्गत डिजिटल हस्ताक्षर हस्तलिखित हस्ताक्षर के समान सुरक्षित, गोपनीय एवं वैधानिक रूप से स्वीकार योग्य है। जिन इलैक्ट्रॉनिक दस्तावेजों पर डिजिटल हस्ताक्षर किए जाते हैं, उन्हें कागजी दस्तावेज के समान ही समझा जाता है। भारत में सूचना प्रौद्योगिकी अधिनियम में प्रमाणन प्राधिकरण नियंत्रक (सी.सी.ए.) के संचालन के लिए लाइसेंस प्रदान किया जाता है तथा प्रमाणन प्राधिकरण की कार्य विधि को संचालित किया जाता है। प्रमाणन प्राधिकरण (सी.ए.) उपयोगकर्त्ताओं को इलैक्ट्रॉनिक प्रारूप में ही प्रमाणन के लिए डिजिटल हस्ताक्षर सम्बन्धी प्रमाण–पत्र जारी किया जाता है। सूचना प्रौद्योगिकी अधिनियम 2000 में निर्धारित किए गए उद्देश्यों की पूर्ति करने के लिए अधिनियम की धारा 17 के अन्तर्गत केन्द्र सरकार द्वारा प्रमाणन प्राधिकरण नियंत्रक (सी.सी.ए.) की नियुक्ति की गई। सी.सी.ए. ने अपना कार्य वैधानिक रूप से 01 नवम्बर, 2000 से प्रारम्भ कर दिया। जिसका उद्देश्य डिजिटल हस्ताक्षर के उपयोग के माध्यम से ई–कॉमर्स तथा ई–गावर्नेंस (E-commerce and E Governance) का विकास एवं सुरक्षा करना है।

सूचना प्रौद्योगिकी अधिनियम 2000 के अन्तर्गत कार्यरत सी.सी.ए. ने अधिनियम की धारा 18(B) के अन्तर्गत आर.सी.ए.आई. की स्थापना की। RCAI का मुख्य उद्देश्य देश में प्रमाणन प्राधिकरणों की सार्वजनिक कुन्जियों पर डिजिटल हस्ताक्षर कार्यक्रम को विकसित करना है। सूचना प्रौद्योगिकी अधिनियम के अन्तर्गत निर्धारित RCAI को संचालित किया जाता है। सी.सी.ए. स्वयं की निजी कुंजी का उपयोग करके सी.ए. की सार्वजनिक कुंजियों का निर्माण करता है। जिसके द्वारा साइबर स्पेस में उपयोगकर्त्ताओं के लिए यह अर्थ सत्यापित किया जा सके कि जारी किया गया उक्त प्रमाण–पत्र लाइसेन्स धारी सी.ए. द्वारा निर्गमित किया गया है। इसको पूरा करने के लिए रूट सर्टिफाईंग अथोरिटी ऑफ इंडिया (RCAI) का निर्माण किया गया है। इस प्रकार भारत में सूचना प्रौद्योगिकी अधिनियम 2000 लागू किया गया, जिसकी विभिन्न धाराओं में डिजिटल हस्ताक्षर प्रमाण–पत्र योजना को क्रियान्वित किया गया है। भारत में वर्ष 2000 से ही विभिन्न प्रकार के लेन–देन हेतु भारत सरकार, राज्य सरकारों, स्थानीय सरकारों, बैंकिंग संस्थाओं, स्थानीय कोषालयों (Treasury), वित्तीय संस्थाओं, अन्य सरकारी, गैर सरकारी संगठनों और भारत के नागरिकों के द्वारा किये जाने वाले (Online Transfers) ऑन लाइन लेन–देन आदि में किसी न किसी प्रकार के इलैक्ट्रीक दस्तावेज का हस्तान्तरण किया जा रहा है यह अपने आपमें एक डिजिटल हस्ताक्षर प्रणाली का ही रूप है। क्योंकि किसी भी लेन–देन के लिए एक आई.डी. और एक पासवर्ड होता है। जिसके द्वारा एक व्यक्ति दूसरे व्यक्ति को लेन–देन की प्रक्रिया पूरी करता है। अब बदलते तकनीकी युग के साथ–साथ विभिन्न इन्टरनेट बैंकिंग, भीम एप, गूगल पे, पेटीएम, ब्राउजर लिंक पेमेन्ट, पे–मैनेजर, ए.टी.एम. के द्वारा ट्रान्सफर आदि द्वारा किसी न किसी प्रकार से हरेक व्यक्ति या संस्था ऑन लाइन लेन–देन करते है। यह अपने आपमें एक डिजिटल हस्ताक्षर की प्रक्रिया ही है।

अब सरकार ने यह निर्णय लिया है कि 30 सितम्बर, 2019 तक ही कागजी दस्तावेज पर हस्ताक्षर से लेन–देन मान्य किए जा सकेगें, लेकिन 01 अक्टूबर 2019 के पश्चात् कोई भी लेन–देन कागजी दस्तावेज पर किए गए हस्ताक्षर मान्य नहीं किए जायेगें। 01 अक्टूबर 2019 के पश्चात् प्रत्येक आहरण एवं वितरण अधिकारी को यदि कोई भुगतान कराना होगा तो उसे सूचना प्रौद्योगिकी अधिनियम 2000 के अन्तर्गत निर्धारित डिजिटल हस्ताक्षर प्रमाण–पत्र (D.S.C.) के द्वारा ही भुगतान कराना होगा नही तो अब कोई भी लेन–देन कागजी दस्तावेज पर हस्ताक्षर से स्वीकार्य नहीं होगा। इसके लिए राजस्थान सरकार 01 अक्टूबर 2019 से पूर्व अपनी सरकार के

सभी आहरण एवं वितरण अधिकारियों को डिजिटल हस्ताक्षर प्रमाण पत्र का प्रशिक्षण दे चुकी है। इसके लिए प्रत्येक आहरण एवं वितरण अधिकारी को उसके शहर में या कहीं से भी डिजिटल हस्ताक्षर प्रमाण–पत्र का एक डोंगल/पेन ड्राइव/डिवाइस लेकर अपने बिलों को इलेक्ट्रिक डिजिटल हस्ताक्षर करना होगा।

fMftVy gLrk{kj iek.k&i= cuku dh ifØ;k

सूचना प्रौद्योगिकी अधिनियम की धारा 21 के अनुसार कोई भी व्यक्ति अंकीय चिन्हक प्रमाण–पत्र जारी करने के लिए अनुज्ञप्ति हेतु नियंत्रक को आवेदन कर सकता है। उप धारा 01 के अधीन कोई अनुज्ञप्ति तब तक जारी नहीं की जाएगी जब तक कि आवेदक, आहर्ता, विशेषज्ञता, जनशक्ति, वित्तीय संसाधन और अन्य अवसंरचनात्मक सुविधाओं के बाबत ऐसी अपेक्षाओं को पूरा नहीं करता हो जो अंकीय चिन्हक प्रमाण–पत्रों/डिजिटल हस्ताक्षर प्रमाण–पत्र को जारी करने के लिए आवश्यक हो और केन्द्रीय सरकार द्वारा विहीत की जाएँ। सूचना प्रौद्योगिकी अधिनियम 2000 की धारा 22 के अनुसार अनुज्ञप्ति के लिए आवेदन ऐसे प्रारूप में किया जाएगा जो केन्द्रीय सरकार द्वारा विहीत किया जाएगा। धारा 23 के अनुसार नवीनीकरण निर्धारित प्रारूप में होगा, जिसकी फीस 5000/– रू. होगी जो केन्द्रीय सरकार द्वारा विहीत की जाए और अनुज्ञप्ति की विधिमान्यता की अवधि के अवसान से 45 दिन तक किया जाएगा। आहरण एवं वितरण अधिकारी अथवा ऐसा कोई भी व्यक्ति या संस्था जिसे अपने विभागीय बिलों का भुगतान प्राप्त करना या भुगतान कराना हो तो उसे अपने क्षेत्र, कस्बा, शहर या महानगर में सूचना प्रौद्योगिकी अधिनियम 2000 की धारा 21 के अन्तर्गत लाइसेन्स प्राप्त कर डिजिटल हस्ताक्षर प्रमाण–पत्र बनाने का कार्य पूरा करना होगा। वह व्यक्ति निर्धारित फीस लेकर एक ऐसा डिवाइस/अंकीय चिन्ह बनाकर देता है, जिसके द्वारा आहरण एवं वितरण अधिकारी इलेक्ट्रिक दस्तावेज पर अपने डिजिटल हस्ताक्षर करके विभागीय बिलों के भुगतानों को प्रमाणित कर सकता है। इसके लिए उसे एक आई.डी. और पासवर्ड दिया जाता है। इस आई.डी. व पासवर्ड की पूर्णतया गोपनीयता रखी जाती है, जिसकी जानकारी केवल धारक को ही होती है। इस आई.डी. व पासवर्ड के द्वारा किए गए हस्ताक्षर का तात्पर्य यह है कि हस्ताक्षरकर्त्ता ने पूरे इलेक्ट्रिक दस्तावेजों को पूर्णतया पढ़ लिया और समझ लिया है। यदि फिर भी कोई त्रुटि रह जाती है तो इसके लिए हस्ताक्षरकर्त्ता का पूर्णतः उत्तरदायित्व रहेगा, क्योंकि इस हस्ताक्षर की निजी कुंजी केवल धारक या निर्धारित व्यक्ति के पास ही रहती है और वह किसी प्रकार के बहाने नही बना सकता है।

fMftVy gLrk{kj iek.k&i=

प्रत्येक कस्बे, शहर, नगर, महानगर आदि सभी स्थानों पर डिजिटल हस्ताक्षर प्रमाण–पत्र बनाने के लिए सूचना प्रौद्योगिकी अधिनियम 2000 के अन्तर्गत अनुज्ञापत्र धारक शाखाएँ खुली हुई होती हैं। इन शाखाओं में कोई भी व्यक्ति/संस्था अपने विभाग से सम्बन्धित लेन–देन प्रक्रिया पूरी करने के लिए निर्धारित प्रारूप में फॉर्म मय दस्तावेज भरकर जमा कराने पर उस ब्रॉंच से एक डिवाइस/पेन ड्राइव या सिगनेचर कॉर्ड विभिन्न दस्तावेजों के आधार पर बनाकर देता है, जो गणीतीय एल्फा न्यूमेरिक नम्बरों के द्वारा तैयार किया जाता है। डिजिटल हस्ताक्षर प्रमाण–पत्र के लिए निम्न 2 प्रकार की कुंजी तैयार की जाती है।

- futh dqath

जिस आई.डी. व पासवर्ड के आधार पर डिजिटल हस्ताक्षर प्रमाण–पत्र का उपयोग किया जाता है। उसे निजी कुंजी कहते है अर्थात् ऐसी कुंजी जिसका उपयोग केवल एक व्यक्ति या धारक ही करता है। डिजिटल हस्ताक्षर प्रमाण–पत्र का उपयोग करने वाले अधिकारी अपने कम्प्यूटर में इन्टरनेट एक्सपलोरर में कम से कम 8 या इससे अधिक के ब्राउजर पर लॉगिंन करके अपने डिजिटल हस्ताक्षर प्रमाण–पत्र का प्रयोग कर सकता है। इस आई.डी. और पासवर्ड की जानकारी केवल एक व्यक्ति को ही होती है। अन्य कोई व्यक्ति इसका दुरूपयोग या जालसाजी नहीं कर सकता है तथा इसकी सुरक्षा वैधानिक तौर पर बहुत अधिक होती है। डिजिटल हस्ताक्षर प्रमाण–पत्र एक स्मार्ट कार्ड जो कि हस्तक्षेप प्रतिरोधी तरीके से डिजाइन किए जाते हैं। एक डिजिटल हस्ताक्षर कार्यन्वयन विभिन्न दस्तावेजों के आधार पर तैयार किया गया स्मार्ट कार्ड है जिसका उपयोगकर्त्ता अपने सी.पी.यू. के संग्रहित निजी कुंजी का उपयोग करते हुए हैश को एन्क्रिप्ट करता है। अर्थात

उपयोगकर्त्ता द्वारा व्यक्तिगत पहचान संख्या या पेन नम्बर्स के प्रयोग द्वारा अपने डिजिटल हस्ताक्षर कार्ड को सक्रिय किया जाता है और उसके आई.डी. एवं पासवर्ड गुप्त रखे जाते है। निजी कुंजी जैसे Email, Gmail, Online Banking, various portal, Facebook, Paytm, Google Pay, Phone Pay, Bhim App आदि।

- lkoZtfud dqath

किसी डिजिटल हस्ताक्षर के उपयोग करने वाले व्यक्ति के अतिरिक्त ऐसे व्यक्ति या संस्था जो प्रेषक के इलेक्ट्रिक दस्तावेज के संदेश को स्वीकार करने के लिए उपयोग करता है अर्थात् संदेश प्रापक के पास उपलब्ध आई.डी. व पासवर्ड की कुंजी सार्वजनिक कुंजी कहलाती है। सार्वजनिक कुंजी का सत्यापनकर्त्ता सक्षम अधिकारी ही होना चाहिए। सार्वजनिक कुंजी का उपयोग (उपयोगकर्त्ता संघ का अधिप्रमाणन) PKI के द्वारा किया जाता है। सार्वजनिक कुंजी की सुरक्षा बहुत अधिक होती है, क्योंकि इसका उपयोग निर्धारित व्यक्ति/संस्था अपने आई.डी. और पासवर्ड के आधार पर करता है, लेकिन इसका उपयोग निजी कुंजी के द्वारा प्राप्त संदेश के आधार पर ही किया जाता है। सार्वजनिक कुंजी का उपयोग जैसे ट्रेजरी में बिल पास करने, पे–मेनेजर पर काम करने, पी.एफ.एम.एस. पोर्टल पर शीर्ष संस्था द्वारा काम करना इसी प्रकार विभिन्न प्रकार की छात्रवृत्तियाँ जैसे समाज कल्याण की छात्रवृत्ति, सी.एम. छात्रवृत्ति, एम.एच.आर.डी. की छात्रवृत्ति आदि 71 प्रकार की छात्रवृत्तियाँ होती है। जिन्हें पास करने के लिए जिस आई.डी. एवं पासवर्ड का प्रयोग किया जाता है, वह सार्वजनिक कुंजी होती है।

fMftVy gLrk{kj dh lqj{kk

डिजिटल हस्ताक्षर की सुरक्षा के सम्बन्ध में गोल्डवासर, मिकाली तथा रिवेस्ट आदि ने डिजिटल हस्ताक्षर के लिए विशेष प्रकार के मॉडल्स बनाए है।

- डिजिटल हस्ताक्षर की केवल सार्वजनिक कुंजी ही अन्य व्यक्ति को दी जाती है।
- प्राप्त संदेश में ऐसे डिजिटल हस्ताक्षर तैयार किए जाते है, जिन्हें जालसाजी करने वाला किसी भी प्रकार से कॉपी नहीं कर सकता है।
- डिजिटल हस्ताक्षर उपयोगकर्त्ता के कम्प्यूटर की सुरक्षा व्यवस्था पर निर्भर करता है।

fMftVy gLrk{kj izek.k i= dk ykHk

डिजिटल हस्ताक्षर प्रमाण पत्र या ई–हस्ताक्षर वर्तमान परिप्रेक्ष्य में डिजिटल इंडिया के विकास का एक भाग है। यह पेपर पेन के बिना ही किसी भी डिजिटल हस्ताक्षर के द्वारा पेपर संदेश भेजा जा सकता है।

- डिजिटल हस्ताक्षर प्रमाण पत्र से समय की बचत होती है।
- फॉर्म डाउन लोड करने, प्रिन्ट करने तथा शीर्ष संस्था को भेजने आदि प्रक्रिया से राहत मिलती है।
- डिजिटल हस्ताक्षर के द्वारा क्लिक करते ही संदेश शीर्ष संस्था के पास पहुंच जाता है।
- इलेट्रिक दस्तावेज पर एक बार हस्ताक्षर कर दिया जाता है तो उसे मार्ग में परिवर्तित करना असम्भव होता है।
- डिजिटल हस्ताक्षर एक एनक्रिप्टेड कोड के रूप में काम करता है, जिससे इसमें किसी भी प्रकार के परिवर्तन की सम्भावना नहीं होती है।
- डिजिटल हस्ताक्षर किसी अन्य व्यक्ति के द्वारा तैयार किया जाता है, लेकिन भारतीय सूचना प्रौद्योगिकी अधिनियम 2000 के अन्तर्गत वह व्यक्ति इसका उपयोग नहीं कर सकता है और ना ही किसी को सार्वजनिक कर सकता है।
- डिजिटल हस्ताक्षर का प्रथम बार प्रयोग करते है तब सम्बन्धित आई.डी. पर नया पासवर्ड जनरेट हो जाता है, जिससे प्रमाण–पत्र बनाने वाला व्यक्ति इससे अनभिज्ञ हो जाता है।
- डिजिटल हस्ताक्षर, प्रमाण पत्र भारतीय सूचना प्रौद्योगिकी अधिनियम 2000 के अन्तर्गत पूर्णतया कानूनी और वैध है।

fMftVy gLrk{kj izek.k i= dh leL;k,¡

भारत में सूचना प्रौद्योगिकी अधिनियम 2000 एवं विभिन्न संशोधन के आधार पर डिजिटल हस्ताक्षर का निर्माण विशेष सुरक्षा तकनीकियों के द्वारा किया जाता है, लेकिन फिर भी कही न कहीं हमारे द्वारा इसके उपयोग में कमियाँ रह जाती है, जिससे समस्यायें उत्पन्न होती हैं, जैसे –

- डिजिटल हस्ताक्षरकर्त्ता तकनीकी ज्ञान के अभाव में इसका उपयोग नहीं कर सकता है।
- यदि किसी संस्था में आवश्यकतानुसार कम्प्यूटर एवं हाई स्पीड इन्टरनेट एवं इससे सम्बन्धित उपकरण नही होगें तो डिजिटल हस्ताक्षर का उपयोग नहीं किया जा सकता है।
- यदि डिजिटल हस्ताक्षर का उपयोग किसी सार्वजनिक या भीड़ वाले स्थान पर किया जाता है तो निजी कुंजी चोरी होने की सम्भावना बढ़ जाती है।
- यदि डिजिटल हस्ताक्षरकर्त्ता अधिकारी/आहरण वितरण अधिकारी कही अवकाश के दौरान विभाग से बाहर रहे तो उनके स्थान पर अन्य कोई इसका उपयोग नहीं कर सकता है। जिससे विभागीय कार्य बाधित होने की सम्भावना बढ़ जाती है।
- डिजिटल हस्ताक्षर के विकास एवं उपयोग के साथ–साथ साइबर क्राइम बढ़ने की सम्भावना बढ़ जाती है।

References

- The information technology Act. 2000.
- The information technology Amendment Act. 2008.
- The information technology (Amendment) Bill 2018.
- The India institutes of information technology (Amendment) bill 2017.
- Information technology Amendment Act. 2019.
- The National Investigation Agency (Amendment) Act. 2019.
- Signature schemes and applications to cryptographic protocol design, Anna Lysyantskya, deptt. of Electrical Engineering and computer science, Assachosetts institute of technology. Sept. 2002.
- A Certified digital signature, Rolf Markl, in Gils Brasard, No., and Advances in Cryptology-Crypto 89 Lecturer notes in computer science part 435. Page 218-238, spring Verilog, 1990.
- Digitized signatures S Intractable S Factorization, Michal O Robin, Technic Report MIT/LCS/TR-212, MIT Laboratory of Computer Science, Jan. 1979.
- Introduction to Modern Cryptography, J. Ketz and Y. Linden, Cepmen and Holl/CRC press, 2007.
- E-commerce and law of digital signatures, Denis Cempvel, Editor, Oshiyana Publications, 2005.
- Digit – IT gadgets and mobile phones
- Electronics For You – technology monthly
- Express Computer – monthly information technology
- India Today
- Intelligent Computing CHIP magazine
- Outlook, Vigyan Pragati
- Rajasthan Patrika, Daink Bhaskar
- Times of India, The Hindu
- https://hi.wikipedia.org/wiki
- https://kaiseinhindi.com/digital-signature-kya-hai-in-hindi/
- https://www.shuddhgyan.com/digital-signature/
- https://www.google.co.in/
- https://hi.gadget-info.com

❖◆❖