



1.डिजिटल सिग्नेचर एक परिचय	1-6
<ul style="list-style-type: none"> • डिजिटल हस्ताक्षर क्या हैं ? • डिजिटल हस्ताक्षर क्यों ? • डिजिटल हस्ताक्षर की प्रमुख विशेषताएँ • डिजिटल हस्ताक्षर के प्रमुख उपयोग • डिजिटल हस्ताक्षर की वैधानिक डिजिटल हस्ताक्षर कैसे काम करता है ? • डिजिटल हस्ताक्षर के प्रकार • डिजिटल हस्ताक्षर की वैधता की समाप्ति अथवा खोजाना • डिजिटल हस्ताक्षर कैसे प्राप्त किया जाये ? • डिजिटल प्रमाण पत्र की सामग्री • भारत में सार्वजनिक कुंजी हेतु बुनियादी ढांचा 	
2 .डिजिटल सिग्नेचर को टोकन में स्टोर करना टोकन ड्राइवर इंस्टालेशन सिस्टम चेकिंग	7-12
जावा सेटिंग ब्राउसर डेटिंग	
<ul style="list-style-type: none"> • अनिवार्य प्रणाली की जाँच • जो विंडोज अपने सिस्टम में स्थापित किया गया है की जाँच कैसे करें • अपने इंटरनेट एक्सप्लोरर संस्करण की जाँच कैसे • कैसे जांच करे के लिए यूएसबी टोकन ड्राइवर सही काम कर रहा है • जावा सेटिंग्स! • इंटरनेट एक्सप्लोरर सेटिंग्स • टोकन पिन और अनब्लॉक पासवर्ड बदलना 	
3. डिजिटल हस्ताक्षर के सफल क्रियान्वयन ई शासन में	13-14
4. वन विभाग स्कैन छवियाँ जेपीईजी, GIF के डिजिटल हस्ताक्षर p7signer सॉफ्टवेयर का उपयोग ...	15-18
<ul style="list-style-type: none"> • एकल छवि पर हस्ताक्षर • थोक छवियों को एक फ़ोल्डर में साइन इन करना P7 प्रारूप में • डिजिटल हस्ताक्षर की छवि को खोलना • डिजाइनर हस्ताक्षर की जाँच करना 	
5 वन विभाग के पीडीएफ साइनर साफ्टवेयर के द्वारा पीडीएफ दस्तावेजों पर हस्ताक्षर	19-23
<ul style="list-style-type: none"> ▪ सॉफ्टवेयर द्वारा छवि / डाक्यूमेंट को पीडीएफ में परिवर्तित करना • ऑनलाइन या ईमेल के द्वारा छवि / डाक्यूमेंट को पीडीएफ में परिवर्तित करना • वन विभाग के पीडीएफ साइनर साफ्टवेयर का उपयोग करना • पीडीएफ साइनर साफ्टवेयर में डिजिटल सिग्नेचर लगाना • डिजिटल हस्ताक्षर के साथ हाथ के हस्ताक्षर की छवि लगाना • एडोब रीडर में डिजिटल हस्ताक्षर को मान्य करना 	
6 आउटलुक से इमेल में डिजिटल सिग्नेचर लगाना	25
7 सन्दर्भ - एवं सहायता हेतु आवश्यक फोन नंबर तथा जरूरी इमेल एवं पते	26

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 करते हैं और संदेश प्राप्तकर्ता को यह विश्वास दिलाते हैं 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।

डिजिटल हस्ताक्षर क्यों ?

- ✘ वर्तमान में सभी विभागों एवं कार्यालयों में मैन्युअल 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 पुनः प्राप्ति (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।

डिजिटल हस्ताक्षर की प्रमुख विशेषताएँ

- ✘ **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 पश्चात 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।

डिजिटल हस्ताक्षर के प्रमुख उपयोग

- ✘ प्रकरणों का ऑनलाईन अध्ययन कर स्वीकृति प्रदान करना।
- ✘ कम्प्यूटरिकृत दस्तावेजों का ऑनलाईन सत्यापन करना।
- ✘ प्रमाणिक/अधिकृत रूप से ऑनलाईन आवेदन करना।
- ✘ लायसेंस, परमिट, प्रमाणपत्र, स्वीकृति, इत्यादि ऑनलाईन जारी करना।

डिजिटल हस्ताक्षर की वैधानिक

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।

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।

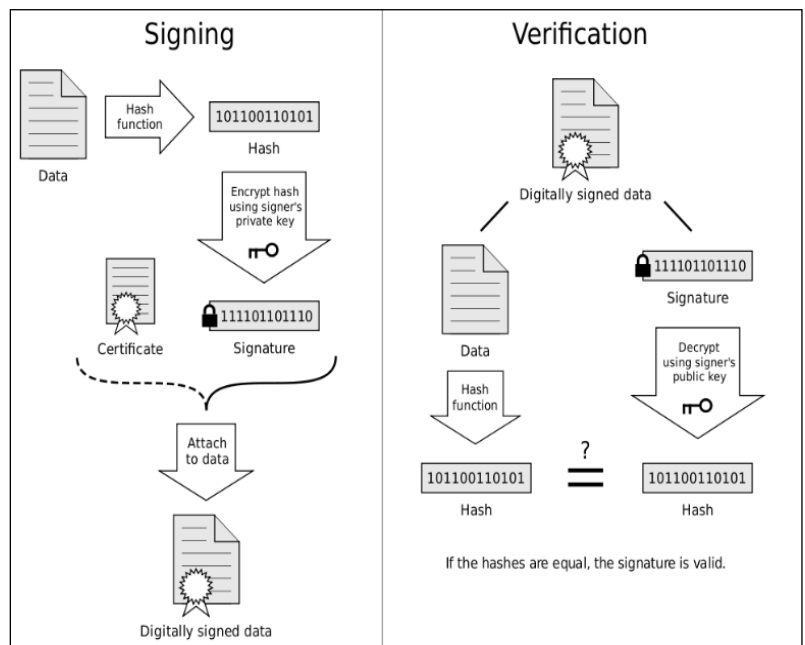
"निजी कुंजी (**Private Key**) से एनक्रिप्ट होने वाले दस्तावेज को केवल उसकी जोड़ीदार 'सार्वजनिक कुंजी (**Public Key**) से ही डिजिफ्ट किया जा सकता है। दस्तावेज प्राप्तकर्ता अपने कम्प्यूटर पर दस्तावेज की "हेश वैल्यू" दोबारा निर्मित करता है और दस्तावेज के साथ आने वाली एनक्रिप्टेड "हेश वैल्यू" को प्रेषक की 'सार्वजनिक कुंजी (**Public Key**) से डिजिफ्ट करता है। यदि दोनों "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।

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 डिजिफ्ट 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 डिजिफ्ट करता है। यदि दोनों "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।

	Handwritten Signature	Digital Signature
Concept		Digital signature using asymmetric encryption / decryption method 1359829304507745830 102030302300330230 00043049504900904 40305234898434857598
Problem	Reusable	Impossible to reuse



डिजिटल हस्ताक्षर के प्रकार

क्रमांक	प्रकार	उपयोग	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 ईमेल अकाउंट को सत्यापित करते हैं। जहाँ उच्च स्तरीय विश्वसनीयता एवं वचनबद्धता की आवश्यकता नहीं होती है वहाँ इस स्तर के सर्टिफिकेट उपयोग में लाये जाते हैं।	1 या 2 वर्ष।
3	Class '2' (Two) Certificate	यह सर्टिफिकेट निजी उपयोग एवं व्यवसायिक 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।	1 या 2 वर्ष।
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 सर्टिफाइंग अथॉरिटी के सामने उन व्यक्तियों की व्यक्तिगत उपस्थिति अनिवार्य होती है।	1 या 2 वर्ष।

डिजिटल हस्ताक्षर की वैधता की समाप्ति अथवा खो जाना

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 अथॉरिटी द्वारा समाप्त की जा सकती है।

डिजिटल सिग्नेचर खो जाने की स्थिति में आप इसे बदल करवा सकते हैं आपको इस सम्बन्ध में अपनी रजिस्टर्ड ईमेल आई डी से वन विभाग के आई टी विभाग के अनुमोदन सहित आपने रजिस्ट्रेशन आथॉरिटी को ईमेल लिखना होगा ईमेल लिखें।

डिजिटल हस्ताक्षर कैसे प्राप्त किया जाये ?

भारत सरकार द्वारा CCA कंट्रोलर आफ सर्टिफाइडिंग आथॉरिटी ने कुछ Certifying आथॉरिटी को डिजिटल सिग्नेचर जारी करने की मान्यता दी है ये Certifying आथॉरिटी अपने रजिस्ट्रेशन आथॉरिटी के माध्यम से सिग्नेचर जारी करती है।

Safescrypt TCS nCode eMudhra Caprocorn Identity IDBRT इत्यादि सर्टिफिंग एजेंसी है तथा ये अपने रजिस्ट्रेशन आथॉरिटी के द्वारा सिग्नेचर उपलब्ध करवाते हैं आपकी रजिस्ट्रेशन आथॉरिटी बालाजी कम्प्युसाफ्ट (बालाजी साल्यूशन) है आप इस सम्बन्ध में dsc@digitalsignature.net.in पर ईमेल कर सकते हैं।



डिजिटल प्रमाण पत्र की सामग्री:

- सीरियल नंबर: अनोखे प्रमाण पत्र की पहचान करने के लिए इस्तेमाल किया।
- विषय: व्यक्ति या संस्था की पहचान की।
- हस्ताक्षर एल्गोरिथम: हस्ताक्षर बनाने के लिए इस्तेमाल एल्गोरिथम।
- हस्ताक्षर: सत्यापित करने के लिए वास्तविक हस्ताक्षर है कि यह जारीकर्ता से आया है।
- जारीकर्ता: इकाई है कि सूचना और सत्यापित प्रमाण पत्र जारी किए हैं।
- वैध-से: तिथि प्रमाण पत्र पहले से वैध है।
- मान्य करने के लिए: समाप्ति की तारीख।
- कुंजी-उपयोग: सार्वजनिक कुंजी (उदाहरण के लिए कूटलेखन, हस्ताक्षर, प्रमाणपत्र हस्ताक्षर) के प्रयोजन।
- सार्वजनिक कुंजी: सार्वजनिक कुंजी एन्क्रिप्शन एन्क्रिप्शन और इसके साथ जुड़े डेटा के डिक्लिप्शन के लिए एक महत्वपूर्ण जोड़ी का उपयोग करता है।
- Thumbprint एल्गोरिथम: सार्वजनिक कुंजी हैश करने के लिए इस्तेमाल किया एल्गोरिथम।
- Thumbprint: हैश ही, सार्वजनिक कुंजी का एक संक्षिप्त रूप के रूप में इस्तेमाल किया।

डिजिटल सिग्नेचर की वैधानिक मान्यता

The Indian Information Technology Act 2000 (<http://www.mit.gov.in/content/information-technology-act>) came into effect from October 17, 2000. One of the primary objectives of the Information Technology Act of 2000 was to promote the use of Digital Signatures for authentication in e-commerce & e-Governance. Towards facilitating this, the office of Controller of Certifying Authorities (CCA) was set up in 2000. The CCA licenses Certifying Authorities (CAs) to issue Digital Signature Certificates (DSC) under the IT Act 2000. The standards and practices to be followed were defined in the Rules and Regulations under the Act and the Guidelines that are issued by CCA from time to time. The Root Certifying Authority of India (RCAI) was set up by the CCA to serve as the root of trust in the hierarchical Public Key Infrastructure (PKI) model that has been set up in the country. The RCAI with its self-signed Root Certificate issues Public Key Certificates to the licensed CAs and these licensed CAs in turn issue DSCs to end users.

Section 5 of the Act gives legal recognition to digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with the handwritten signatures and the electronic documents that have been digitally signed are treated at par with the paper based documents.

An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include other techniques for signing electronic records as and when technology becomes available.



PUBLIC KEY INFRASTRUCTURE IN INDIA

PKI is the acronym for Public Key Infrastructure. The technology is called Public Key cryptography because unlike earlier forms of cryptography it works with a pair of keys one of which is made public and the other is kept secret. One of the two keys may be used to encrypt information which can only be decrypted with the other key. The secret key is usually called the private key. Since anyone may obtain the public key, users may initiate secure communications without having to previously share a secret through some other medium with their correspondent. PKI is thus the underlying system needed to issue keys and certificates and to publish the public information. PKI is a combination of software, encryption technologies, and services that enable enterprises to protect the security of their communications and business transactions over networks by attaching so-called “digital signatures” to them.

The Office of the Controller of Certifying Authorities (CCA), has been established under the Information Technology (IT) Act 2000 for promoting trust in the electronic environment of India. The current PKI organization structure in India consists of the Controller of Certifying Authority as the apex body and as the Root Certifying Authority of India (RCAI) (as shown in the figure on PKI Hierarchy). The CCA is entrusted with the following responsibilities : -

- Licensing Certifying Authorities (CAs) under section 21 of the IT Act and exercising supervision over their activities.
- Controller of Certifying Authorities as the “Root” Authority certifies the technologies and practices of all the Certifying Authorities licensed to issue Digital Signature Certificates
- Certifying the public keys of the CAs, as Public Key Certificates (PKCs).
- Laying down the standards to be maintained by the CAs.
- Conflict resolution between the CAs
- Addressing the issues related to the licensing process including:
 - a) Approving the Certification Practice Statement (CPS);
 - b) Auditing the physical and technical infrastructure of the applicants through a panel of auditors maintained by the CCA.

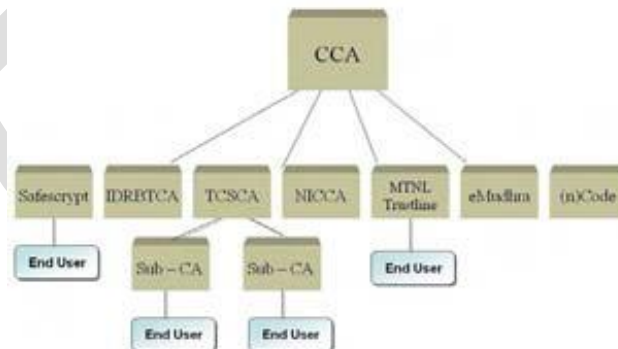
The RCAI is responsible for issuing Public Key Certificates to Licensed Certifying Authorities (henceforth referred to as Certifying Authorities or CA). The CAs in turn are responsible for issuing Digital Signature Certificates to the end users. In order to facilitate greater flexibility to Certifying Authorities, the CCA has allowed the creation of sub-CAs. As per this model, a Certifying Authority can create a sub-CA to meet its business branding requirement. However the sub-CA will be part of the same legal entity as the CA.

The sub-CA model will be based on the following principles:

The CAs must not have more than one level of sub-CA

A sub-CA certificate issued by the CA is used for issuing end entity certificates

A CA with sub-CA must necessarily issue end entity certificates only through its sub-CA. The only exception will be for code signing and time stamping certificates, which may directly be issued by the CA.





2.डिजिटल सिग्नेचर को टोकन में स्टोर करना

डिजिटल सिग्नेचर स्टोर करने हेतु माध्यम

- 1 स्मार्ट कार्ड इसमें स्मार्ट कार्ड रीडर की आवश्यकता होती है
- 2 USB eTOKEN इसे पेन ड्राइव के जैसे उपयोग कर सकते है |

We Provide ePass 2003 eToken and a name Label Chain to Identity it



- Auto Plug & Play- No CD required for Driver Installation.
- Supported OS: 32bit and 64bit Windows XP SP3, Server 2003 , Vista, Server 2008, Seven, Eight,
- 32bit and 64bit Linux and MAC OS X
- FIPS 140-2 Level 3 Certified and Cap for each USB Token is Included.
- Memory Space: 64KB (EEPROM) - Can store around 7-10 DSC. and Connectivity: USB 2.0 full speed, Connector type A
- Laser Printed Serial Number on each token.

Make NOTES ----



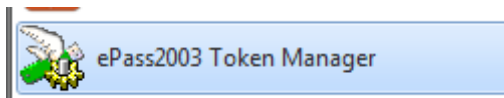
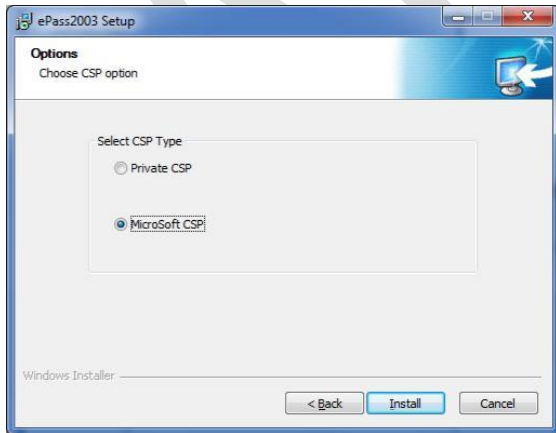
टोकन ड्राइवर इंस्टालेशन सिस्टम चेकिंग जावा सेटिंग ब्राउसर डेटिंग

- अनिवार्य प्रणाली की जाँच
- जो विंडोज अपने सिस्टम में स्थापित किया गया है की जाँच कैसे करें
- अपने इंटरनेट एक्सप्लोरर संस्करण की जाँच कैसे
- कैसे जांच करे के लिए यूएसबी टोकन ड्राइवर सही काम कर रहा है
- जावा सेटिंग्स!
- इंटरनेट एक्सप्लोरर सेटिंग्स
- टोकन पिन और अनब्लॉक पासवर्ड बदलना

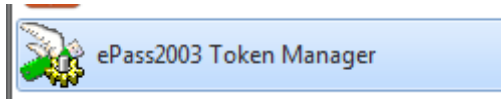
इटोकन में ड्राइवर टोकन में भी है अथवा आप हमारी वेबसाईट www.digitalsignature.net.in/forestit/ में जा के ड्राइवर डाउनलोड कर सकते है |

राईट क्लिक इटोकन इन माई कंप्यूटर → ओपन सेट अप → इंस्टाल → क्लिक आई अग्री → इंस्टाल → नेक्स्ट → इंस्टाल

इंस्टाल करते समय इंग्लिश लेंगुअज चुने तथा माइक्रोसाफ्ट CSP चुनिए

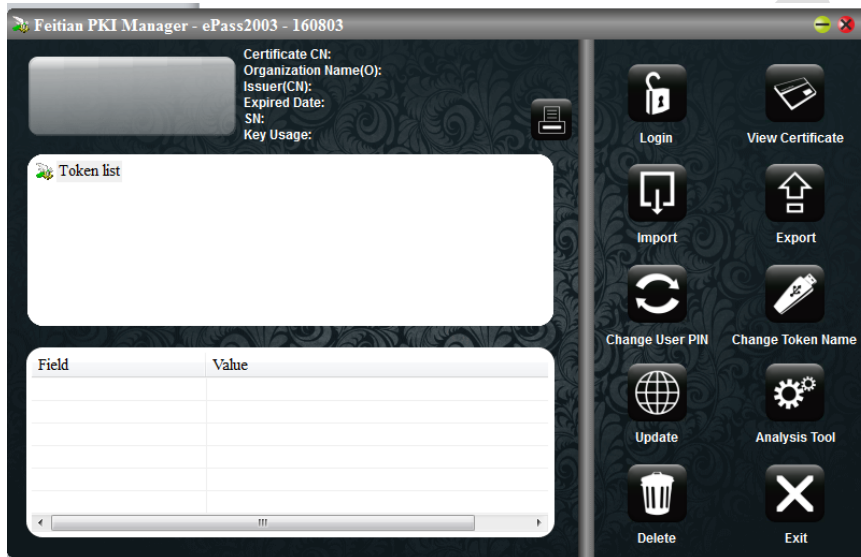


शोर्ट कट ऑफ़ टोकन मेनेजर डेस्कटाप में
इंस्टाल हो जाएगा



Click the ICON to OPEN Token Manager

इ टोकन में अपने सिग्नेचर को कैसे देखे अथवा पासवर्ड कैसे बदले - पासवर्ड बदलने के लिए चेंज यूजर पिन पर क्लिक करे तथा पुराना पिन जो की डिफाल्ट में 12345678 रहता है की जगह नया बना ले



You can also view the details of the certificate by opening the Feitian PKI Manager as shown in the figure below: अपने सर्टिफिकेट की जानकारी भी आप टोकन को क्लिक कर के डिटेल्स में जा के देख सकते है |

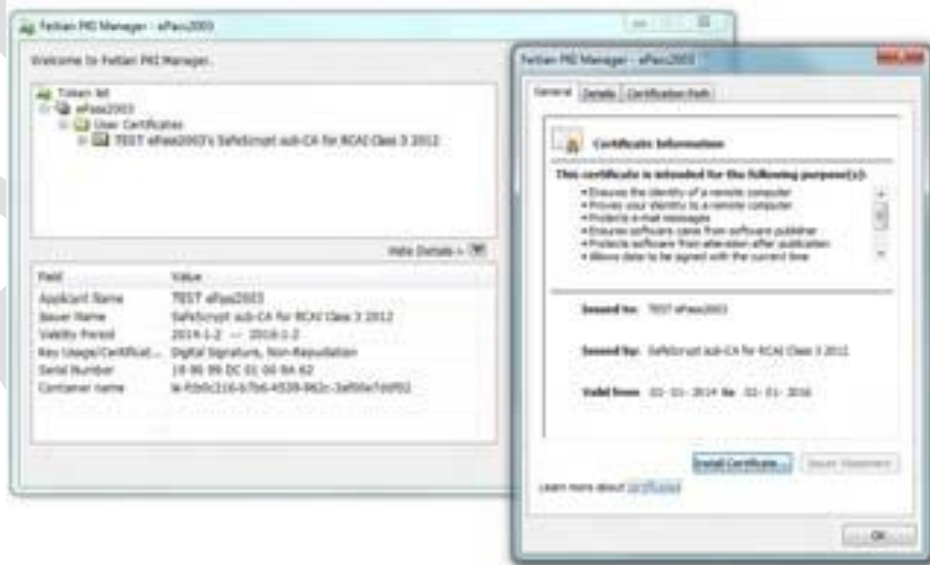


Fig. 1.25: Certificate details from the Feitian PKI Manager ePass 2003

अपने टोकन को पासवर्ड आप चाहेतो बदल सकते है दस बार गलत पासवर्ड डालने पर आपका का पासवर्ड ब्लॉक हो जाता है। टोकन गुम जाने पर अथवा पासवर्ड ब्लॉक होने पर नीचे दिये हुई ई-मेल पर संपर्क करें।



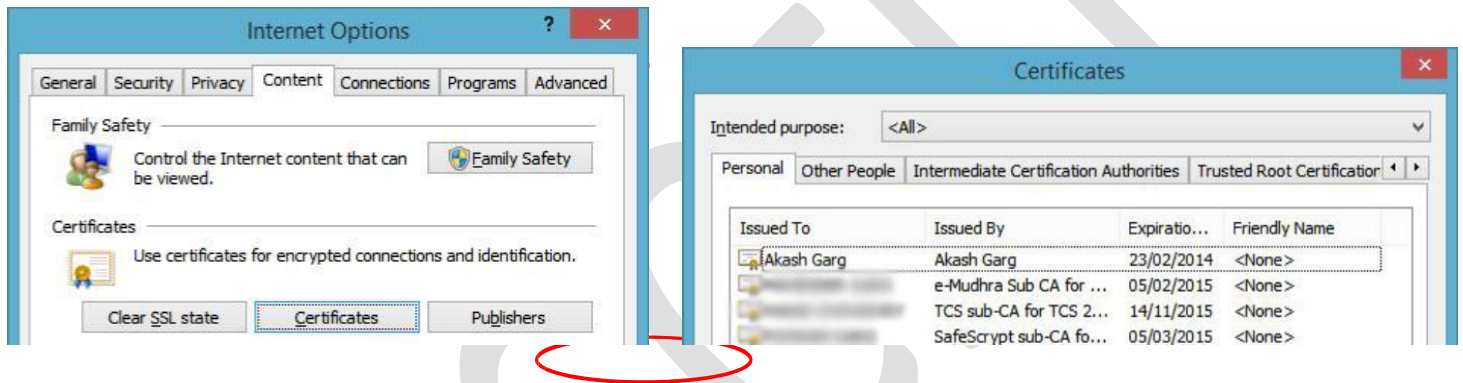
DROP A EMAIL dsc@digitalsignature.net.in to raise Ticket with the Approval from APCCFIT to Block and revoke the etoken

How to check whether USB Token driver is successfully installed and working in your system? यह आवश्यक जांच कर ले की आप का यू.एस.बी टोकन सही काम कर रहा है।

- Insert USB Token in any USB port.
- Wait for a while till computer recognizes and reads your USB Token. c.

Now open Internet Explorer Browser.

- Go to Tools> Internet Options (or just press Alt + T + O)
- Navigate to Content Tab > Certificates.
- If you can see your Digital Signature Certificate name here, then your USB Token is working fine. Otherwise install your USB Token driver first and then proceed with this point again.



डिजिटल सिग्नेचर के उपयोग के दौरान आने वाली विभिन्न तकनीक समस्या का कारण सही ऑपरेटिंग सिस्टम न होना जावा अपडेट न होना सही ड्राइवर नहीं डाला होना अथवा वेब ब्राउजर की सेटिंग सही से न होना है। जिस कारण सही इंस्टाल होने के बाद भी टोकन नहीं चलता है इसलिए निम्न जांच कर ले

- आप का सिस्टम अगर पुराना है एक्स पी तो उसे सर्विस पैक 3 से अपडेट करे | टोकन विंडो सेवन सर्विस पैक वन में सही काम करते है
- जावा इंस्टाल नहीं है तो उसे इंस्टाल करे
- जावा की सेटिंग्स करे कंट्रोल पैनल → ओपन जावा → सिक्युरिटी मिनिमम रखे
- कई बार टोकन ब्लाक रहता है तो स्मार्ट कार्ड इनेबल करे
- रन → सर्विसेज.msc → स्मार्ट कार्ड इनेबल → रिस्टार्ट सिस्टम

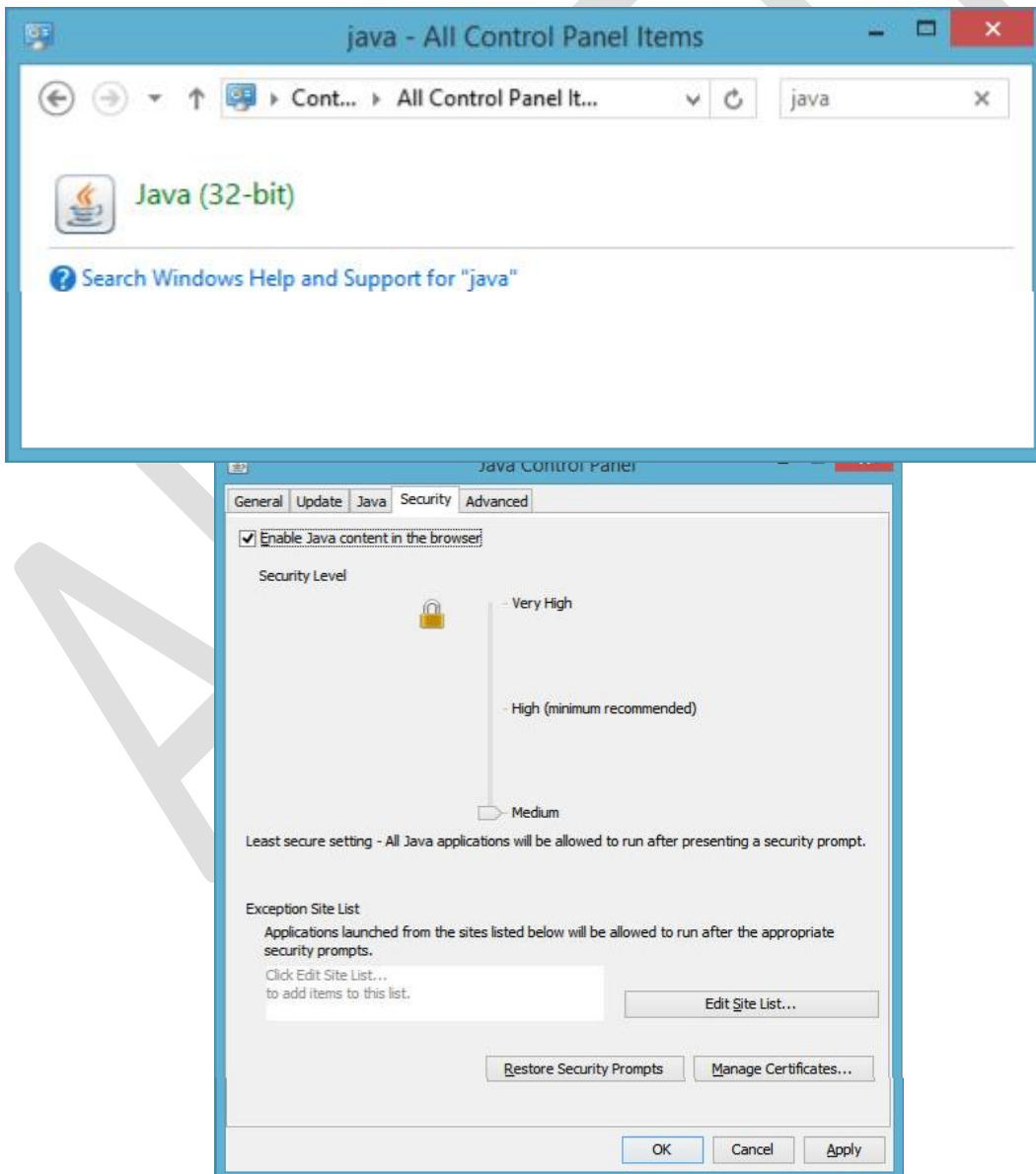
अगर ब्राउसर में टोकन युस करना है तो ब्राउसर की सेटिंग्स करनी होगी तथा जावा में वेबसाईट को जोड़ना होगा | हमारी वेबसाईट में सारा विस्तृत सचित्र स्टेप सहित साड़ी सेटिंग्स तथा अन्य तकनीक स्जान्कारी आप डाउनलोड कर सकते है

www.digitalsignature.net.in/forestit



If there is more than one JAVA installed, remove all JAVA versions from your system by uninstalling all of them. After uninstalling all java, download and install latest java version of 32 bit only. It does not matter if your system is 64 bit. At present latest JAVA is JRE 7 update 51. Then restart your system. After restart, open Java in control panel. Double Click on Java (32-bit) icon. A dialog box will appear

- सम्युरेटी वाले टेब में सूरक्षा का तीर सबसे नीचे करें
- जिस वेबसाइटको आप युज करे रहो हो उसको एक्सेसेपाशन साईट में जोड़ दे इंटरनेटन एक्सप्रोलर की सेटिक कैसे करें।
- सम्युरेटी टेब के कास्टम लेबल में जाकर सारे एक्यूएक्स इनेबल करें जो नोट सिक्यूरो है उन्हें प्राम्ट करें।
- ट्रस्टेड साईट में जिस वेबसाईट में डिजिटल सिगनेचर उपयोग करना हो फिर जोड़े नीचे दिये चित्र के अनुसार आप सेंटिंग कर सकते है।



E-Governance is at the center of Digital Transformation for Governments and digital signatures can enable Digital Transformation by making Government to Citizen services and vice versa completely paperless.

The following are the lessons learnt and the road ahead suggested for implementation of digital signatures in the e-Governance programmes:-

The digital signature implementation must be end to end available without any dependency on proprietary OS.

The verifications must happen on the local application servers, else the implementation model may fail in the remote applications in the rural landscape.

The State Government needs to develop its own franchisee model for management of digital signatures on a day to day basis, else it may impede decision making.

No physical signature should be promoted on print outs of any digitally signed certificates/documents

Awareness campaign should be launched in national and local media (in local languages) regarding what is digital signature and how it benefits the citizens.



GOVERNMENT OF ASSAM
OFFICE OF THE SUB-DIVISIONAL OFFICER
BISWANATH CHARIALI, SONITPUR DISTRICT



Assam e-Governance Project
an initiative under the
National e-Governance Plan

PERMANENT RESIDENT CERTIFICATE



Date: 17-06-2019

This is to certify that the person with the following details :

Name	BABLY KHATUN
Name of Father	MD. ABDUL BAREK BEPARI
Name of Mother	SALEMA KHATUN
Revenue Circle	BISWANATH
Village / Town	AMBARIPAVOURROAD
Post Office	CHARIALI
Police Station	BISWANATH CHARIALI
Sub - Division	BISWANATH CHARIALI
Purpose of Issue	Admission into higher educational institutions

is Permanent Resident of **SONITPUR**

This certificate shall not be valid for any other purpose other than the purpose stated above.





Signature of the Approving Authority

Signature valid

Digitally signed by Anuskar Phukan
Date: 2019.06.17 11:29:42 IST
Reason: e-Office Portal
Location: Assam

NOTE :

- This order is digitally signed and therefore needs no physical signature.
- Authenticity of this order can be verified from <http://cdistrict.assamgov.in>. This Order is legally valid as per the Information Technology ACT, 2008 and its subsequent amendments.
- Tampering of this order will attract penal action.

Figure: Screenshot of a Digitally Signed Residence Certificate

3.डिजिटल हस्ताक्षर के सफल कार्यान्वयन

S.No	Project	Use of Digital Signatures
1.	eDistrict – ई जिला	Digital Signatures are being used for electronically signing the Certificates being issued through eDistrict Centres / CSCs etc The approving authority puts his Digital Signatures at the time of approving the certificate and the related information is printed on the certificate also. This not only ensures that the details of the signing authority is displayed, even the DSC of the signatory can be verified over the Internet.
2	<u>Online Counselling</u> <u>ऑनलाइन काउंसलिंग</u> admission to seats of Engineering, Medical, Polytechnic & B.Ed. courses.	The Digital Signatures are being used by the Counselling In-charge for document verification, fee submission, registration & for choice locking opted by the candidates which are finally locked by the invigilators using DSC. Class II DSC are being used for these activities In case of any modification in the student record, the same can be carried out only through digital signatures in order to ensure the same is recorded in the
3	<u>eProcurement</u> <u>आनलाइन टेंडरिंग</u> is an online tender processing system for the state/central government departments. More than 1000 tenders published so far.	The Digital Signatures are being used both by the vendors and government officials for tender submission and processing. The vendors/traders are using it for applying tenders online, while the government officials are using it at time of opening the tenders and during finalizing of the tenders. Class II signatures are being used both for
4	<u>Voters List Adhar Preparation</u> field data along with the photo ID will be digitized and the same will be digitally signed assuring the correctness of data.	The DSC will be used to counter verify the digitised data of voters list and the photo ID. This can be used by other applications such as eDistrict for online verification of citizen details.

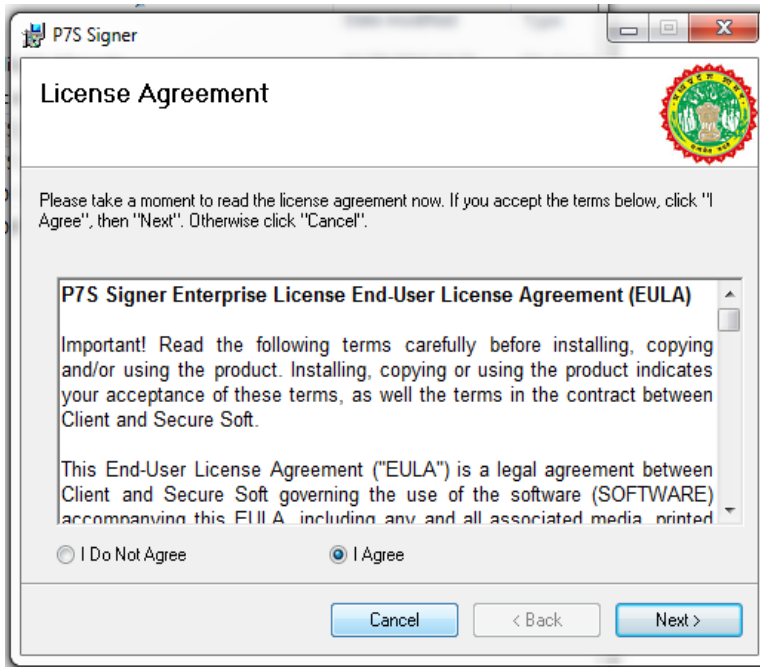
4. DIGITAL SIGNING OF IMAGES GIF/JPEG FMFTVY FLSAXUSPJ DS }KJK BEST BR;KFN GLRKK{KFJR DJUK

This is registered to MP Forest and can be obtained from Forest Website by Contacting IT Department APCCFIT

मध्य प्रदेश वन विभाग हेतु प्रदत्त साफ्टवेयर द्वारा स्कैन इमेज नक़्शे डाक्यूमेंट आप सत्यापित कर सकते हैं

STEP INSTALL P7S SIGNER SOFTWARE –Click ICON to install p7s Signing SW and select I agree to install it

P7S SIGNER SOFTWARE पीसेवन सॉफ्टवेयर को ओपन करे और स्टॉल करें



*Image Signer Software is
Registered Software for MP
Forest Department
Images of JPEG and GIF
Format will be saved in p7s
format with Authentication
provided from Digital
Signature of Signing Officer*

Once you have installed the SW it will be saved in DESKTOP

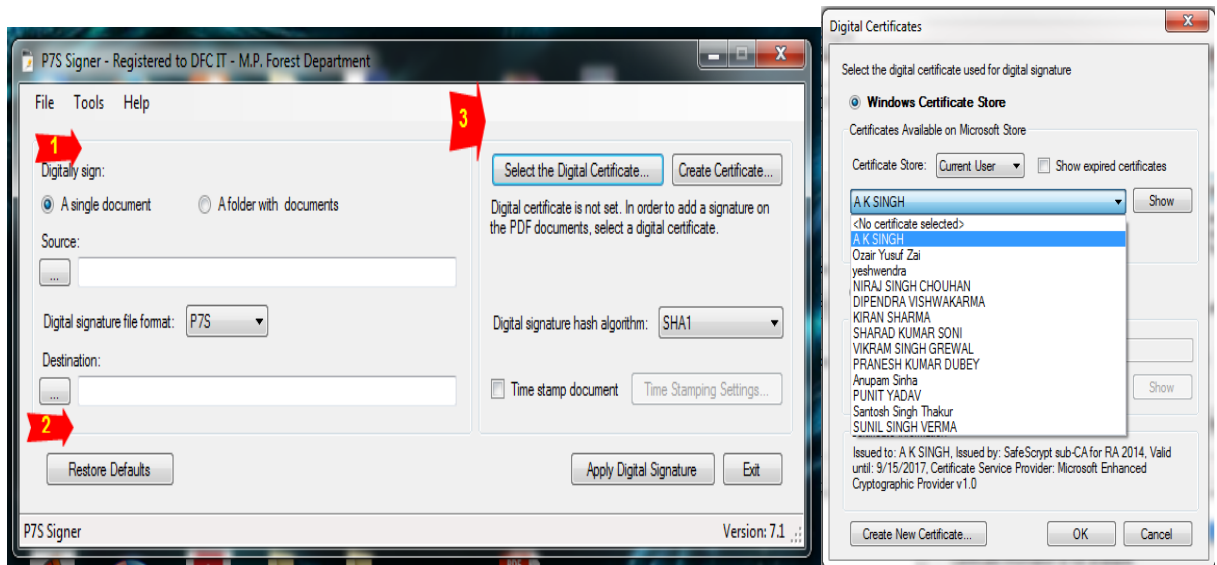
STEP 2 – OPEN DESKTOP SHORTCUT TO OPEN SW

डेस्टटाप पर बने हुए सॉटकर्ट से आप सॉफ्टवेयर खोले



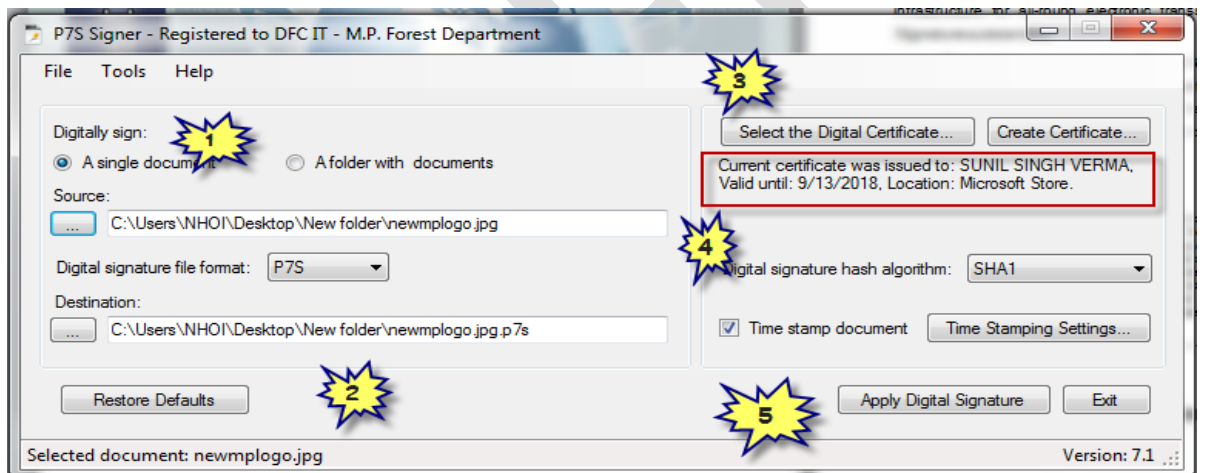
STEP 3 . आप इस सॉफ्टवेयर के द्वारा एक बार में एक इमेज अथवा स्कैन इमेज से भरा हुआ फोल्डर डिजिटल सत्यापित कर सकते हैं आप को सबसे पहले सादी इमेज का स्थान तथा डिजिटल साईन इमेज का स्थान चुनाना होगा आप को अपना ई-टोकन लगा कर डिजिटल टोकन चुनाना होगा।

- 1 SELECT SINGLE OR FOLDER OF IMAGE आप को इमेज का सोर्स चुनना होगा
- 2 SELECT DESTINATION OF IMAGE SIGNED आप डिजिटल साईन करने के बाद उसे कहा रखना चाहते हैं चुने
- 3 SELECT THE DIGITAL SIGNING OFFICER TO APPLY अधिकारी का डिजिटल साईन चुनिए



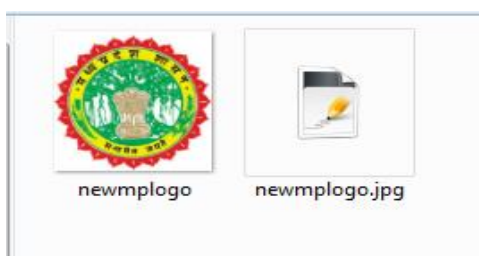
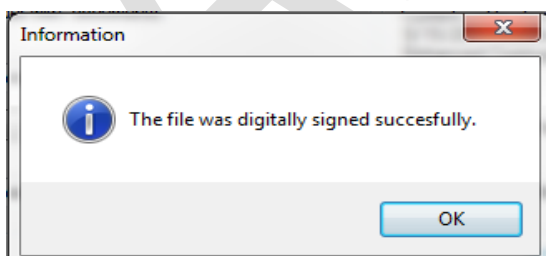
ONCE YOU HAVE SELECTED SIGNATURE YOU CAN SEE THE DETAILS AS IN POINT NO 4 जैसे ही आप डिजिटल साइन चुनते हैं अधिकारी के डिटेल में जानकारी 4 नंबर अनुसार दिखेगी

5. APPLY THE SIGNATURE AS IN POINT 5 आप हस्ताक्षर लगाइए



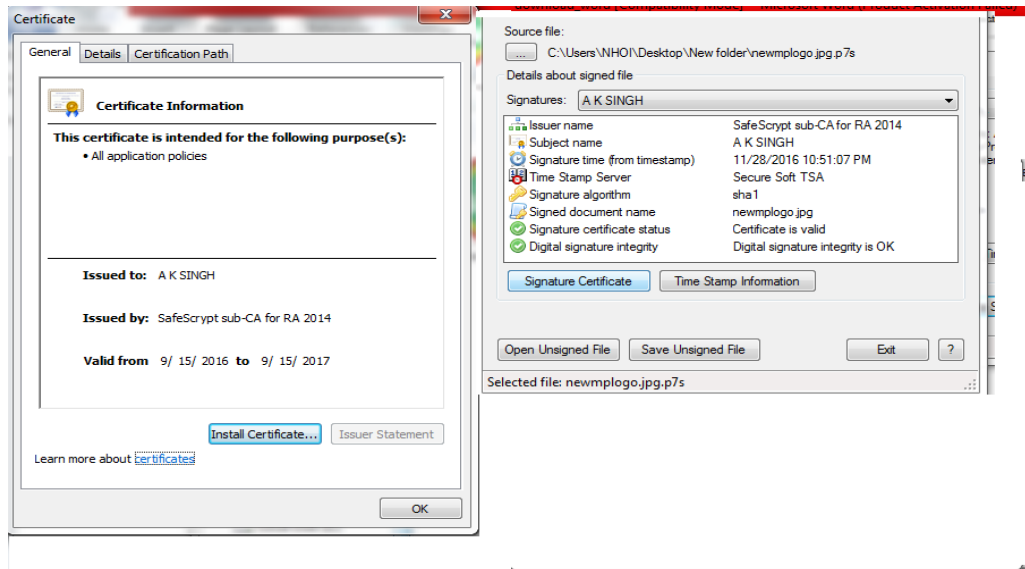
AFTER FEW SECOND THE FILE WILL BE SIGNED AND WILL BE SAVED IN DESIRED LOCATION AS HERE BELOW

आप डिजिटल सिग्नेचर जैसे ही एफालाई करते है थोडे समय बाद आप की इमेज डिजिटलसाइन हो जायेगी



आप डिजिटलसाइन को इमेज को ईमेल कर सकते है तथा आप उस इमेज को ओपन कर के डिजिटलसाइन हस्ताक्षर करने वाले का नाम देख सकते है तथा चाहे तो बिना डिजिटलसाइन के पोर्मट में सेव कर सकते है

YOU CAN CLICK SIGNATURE DETAILS BY DOUBLE CLICK THE FILE AND THEN SAVE THE UNSIGNED FILE AS YOU MAY NEED



PUBLIC KEY CRYPTOGRAPHY STANDARDS PKCS

IMAGE SIGNING FORMAT IS P7S P7M WHICH YOU MAY SELECT CUSTOM CONFIGURATION IN SOME CASES, YOU WILL NEED A DIFFERENT SIGNATURE CONFIGURATION (E.G. DIFFERENT SIGNATURE APPEARANCE AND DIGITAL CERTIFICATES) FOR DIFFERENT FILES/FOLDERS.

To save a specific configuration, go to File – Save Configuration As and save the configuration on a file. Later, you can use that file in batch mode to apply different signature configuration on your signed file. आप फ़ाइल → सेव कंफिगुर में अपनी सेटिंग्स इत्यादि सेट कर के रख सकते हैं

नोट्स बनाने के लिए स्पेस

4 DIGITAL SIGNING OF PDF DOCUMENTS –PDF SIGNER SOFTWARE

पी डी ऍफ़ साइनर साफ्टवेयर

पी डी ऍफ़ साइनर साफ्टवेयर जो की मध्यप्रदेश फारेस्ट विभाग के नाम से रजिस्टर्ड है से आप अपनी इमेज अथवा डाक्यूमेंट जो की पी डी ऍफ़ फार्मेट में है उन पर डिजिटल सिग्नेचर लगा सकते है पी डी ऍफ़ फार्मेट होने के कारण आपना सिग्नेचर नजर आता है तथा आनलाइन वेरीफाई भी हो सकता है

–This is registered to MP Forest and can be obtained from Forest Website by Contacting IT Department APCCFIT

- Portable Document Format (PDF) is best and suitable format to Sign Files Digitally as the Signature Details is Visible in the Documents and it can be validated also .

इमेज को पी डी ऍफ़ में बदलने के तरीके

STORED IMAGES MAPS DOCUMENTS LETTER CAN BE CONVERTED INTO PDF EASILY पी डी ऍफ़ में कैसे बदले

- Use GOOGLE CHROME ----Open Google Chrome DRAG n DROP Image into chrome → Click CTRL + P (File→ Print) . आप गूगल क्रोम में सीधे इमेज को ड्रेग कर के उसे पी डी ऍफ़ में सेव कर सकते है |
- In Print Option Choose Save AS PDF and the file is stored as PDF फ़ाइल→ प्रिंट→ सेव
- USE FREE PDF CONVERT SOFTWARE LIKE do pdf ,icecreampdf ,pdf maker etc गूगल में सर्च कर डाउनलोड करे
- Use Free Online PDF Converting Website Like <https://www.freepdfconvert.com/> <https://online2pdf.com> <https://www.wordtopdf.com> <https://www.convertonlinefree.com> etc etc आनलाइन भी आप फ्री कन्वर्ट कर सकते है |
- RECEIVE CONVERTED FILE IN YOUR EMAIL - Alternatively, you can forward the original email message to pdfconvert@pdfconvert.me and the service will send a PDF version of the message back to you in a second or two. आप सीधे इमेल कर सकते है और तुरंत आपको पी डी ऍफ़ फ़ाइल प्राप्त होगी
- If there are any **Word, Excel or Powerpoint attachments** inside the mail, you can forward the files to attachconvert@pdfconvert.me and they'll come back to you in PDF format. आप **Word, Excel or Powerpoint attachments** सीधे इमेल कर सकते है और तुरंत आपको पी डी ऍफ़ फ़ाइल प्राप्त होगी

-----नोट्स बनाने हेतु स्थान →

वन विभाग का पी डी ऍफ़ साइनर साफ्टवेयर



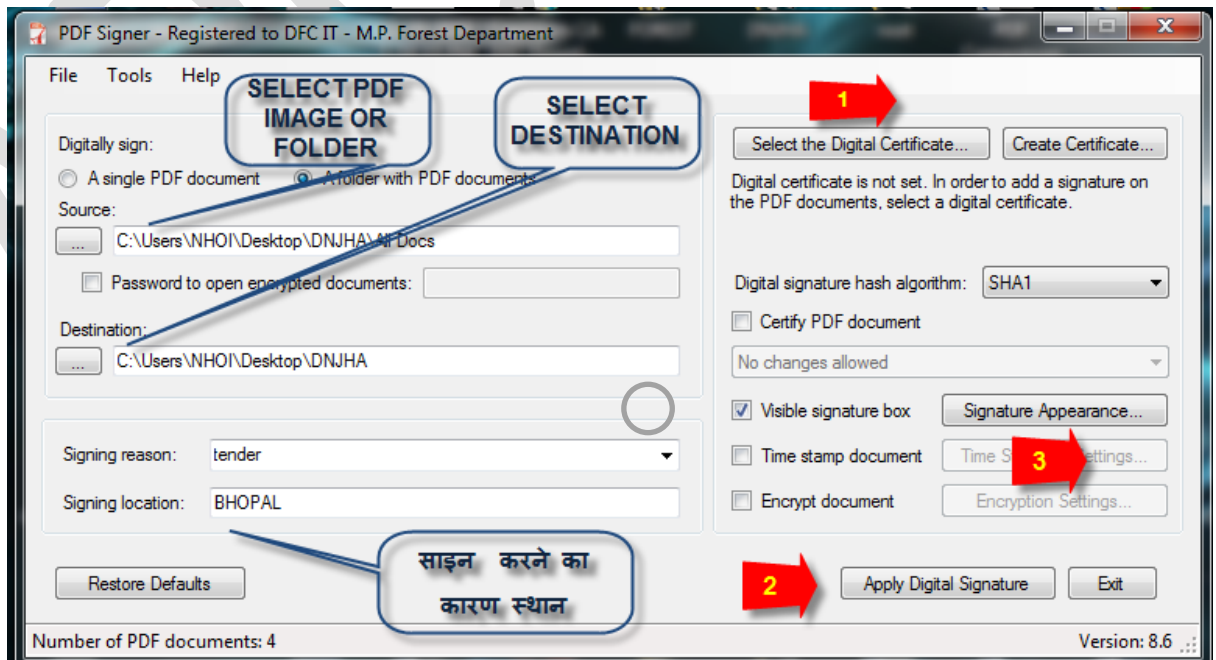
वन विभाग का पी डी ऍफ़ सेनर साफ्टवेयर इंस्टाल करिए डेस्कटाप शार्ट कट से खोलिए

Install the Software PDF Signer → Agree → Install → Shortcut is created @DT साफ्टवेयर इंस्टाल करे डेस्कटाप पर शार्टकट बन जाएगा उसे खोले

Select PDF Single Document or Folder Origin and Destination Both आप पी डी ऍफ़ फ़ाइल अथवा उनका फोल्डर चुने तथा उसे कहा रखना है वो स्थान भी तय करे

Select Reason and Place of Signing if needed आप किस कारण से डाक्यूमेंट साइन कर सहे है यदि हो तो लिखे तथा साइन करने का स्थान भी दे

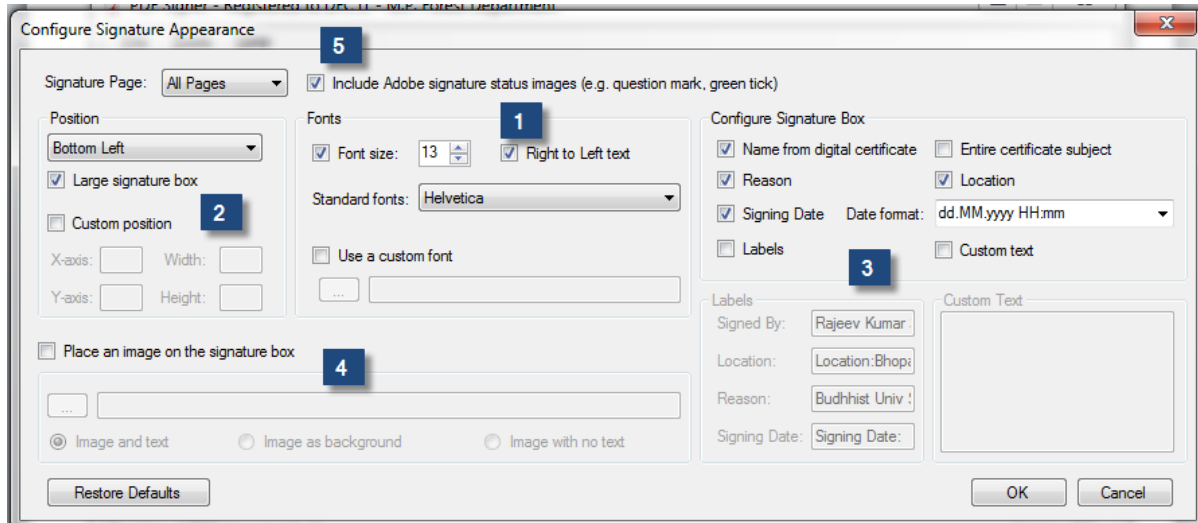
- 1 Select Digital Signature to sign the Documents आप अधिकारी का हस्ताक्षर चुने
- 2 आप अधिकारी के सिग्नेचर को लगा दे
- 3 You Can configure signature appearance by Checking into Visible Sign Box and include adobe Right Tick and Question mark Status for validation also आप अपने हस्ताक्षर में अन्य जानकारी कैसे दे सकते है इस सम्बन्ध में जानकारी इस प्रकार से है



DIGITAL SIGNATURE OPTIONS सिग्नेचर APPEARANCE पर क्लिक करने से ओपन होगा

DIGITAL SIGNATURE RECTANGLE

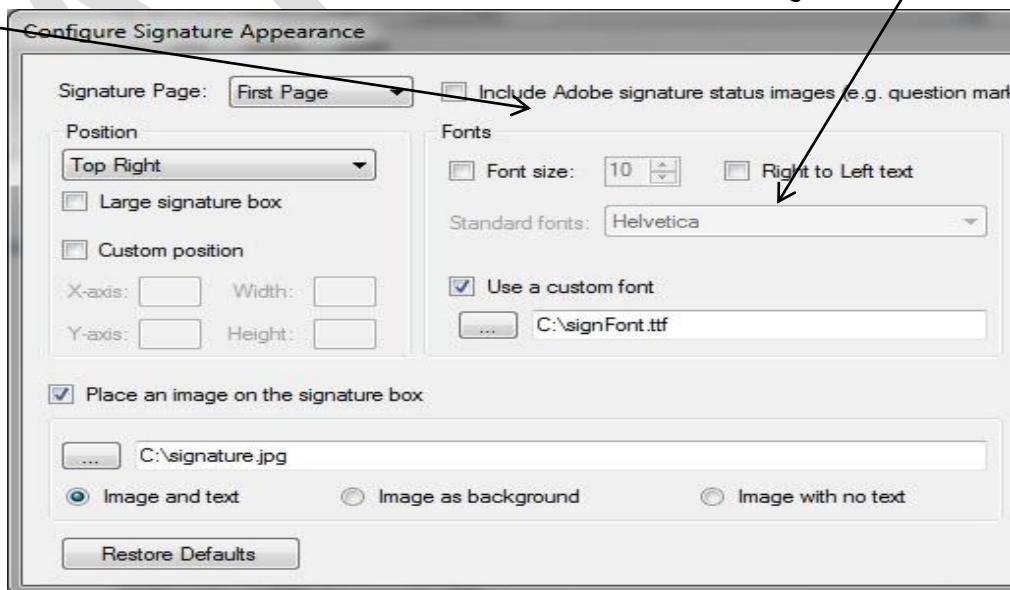
If the checkbox Visible signature box is checked, a signature rectangle will be inserted on the PDF document. The appearance of the digital signature can be customized from the Signature Appearance section. आप Visible signature box पर टिक कर दे तो आप के सिग्नेचर के आस पार एक आयत बन जाएगा



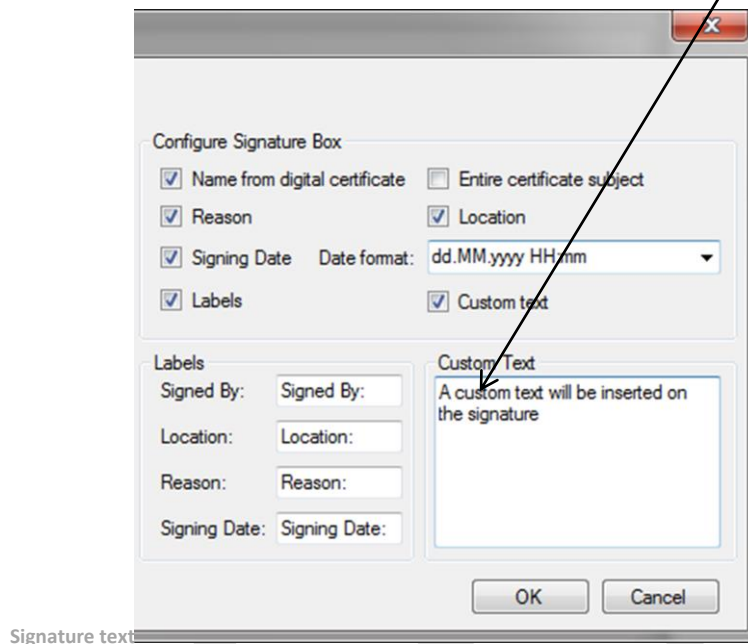
1 फॉन्ट साइज तथा डायरेक्शन आफ टेक्स्ट आप चुन सकते हैं The default text direction is left to right. To change the text direction to right to left (e.g. for Hebrew language) checkbox Right to Left text must be checked. The default font file for the digital signature rectangle is Helvetica. It is possible that this font to not include all necessary UNICODE characters like ä, à, â. On this case you will need to use an external font. The font size is calculated based on the signature rectangle size in order to fit on the signature rectangle (it not have a fixed size). If you want to use a specific font size, it can be specified on the Font size section.

Observation: If the custom position will be used, the corner (0,0) is on the bottom इन्क्लुड एडोबी सिग्नेचर मार्क left of the page. बाई डिफाल्ट उल्टे फाट तरफ निचे की सिग्नेचर आता है आप चाहे तो नया स्थान चुनचुन सकते हैं |

5 आप अपने सिग्नेचर में वेलिड का चिन्ह सही का हरा निशान प्रश्न चिन्ह इत्यादि इन्क्लुड एडोबी सिग्नेचर मार्क से ले सकते हैं



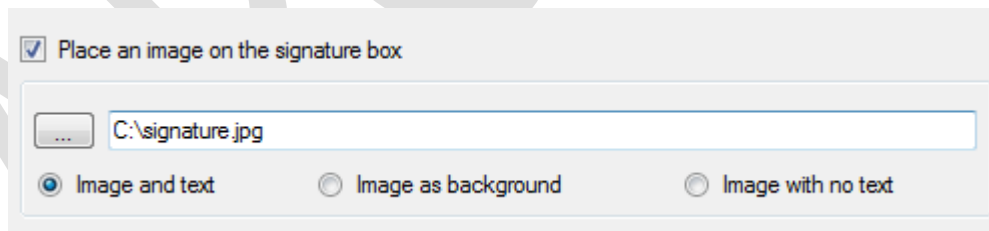
3 The default digital signature text contains information extracted from the signing certificate, signing date, signing reason and signing location but the digital signature text can be easily customized. सिग्नेचर में आपका नाम दिनांक कारण और स्थान आता है आप चाहे तो



LABELS तथा CUSTOM TEXT को टिक करके अन्य जानकारी दे सकते हैं

Set the Digital Signature Graphic सिग्नेचर के साथ में इमेज सिग्नेचर भी लगाना आप अपनी सिग्नेचर की इमेज ब्राउस कर के लगा सकते हैं

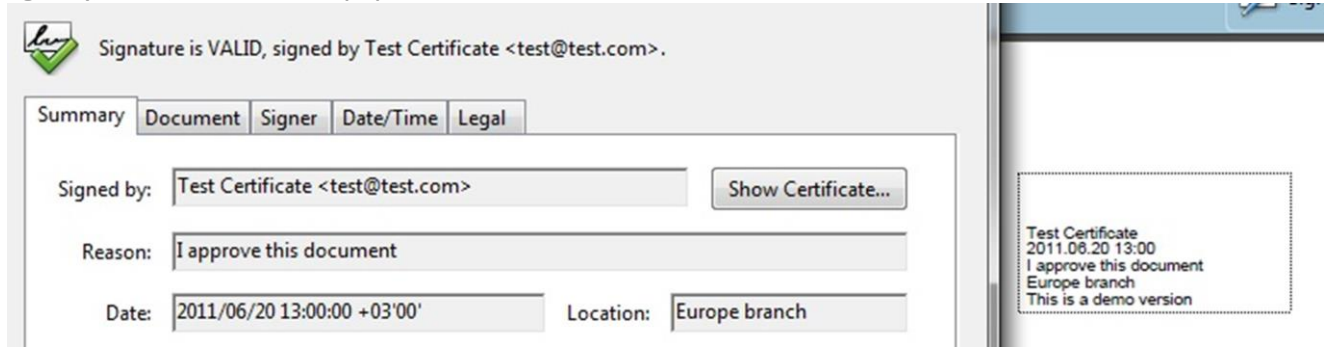
The digital signature rectangle can contains text, graphic or text with graphic. To add an image on the digital signature rectangle, you can do that from Place an image on the signature box section.



These types of signatures are shown below: इस तरह से इमेज नजर आएगी

1. Image and text, 2. Image as background, 3. Image with no text



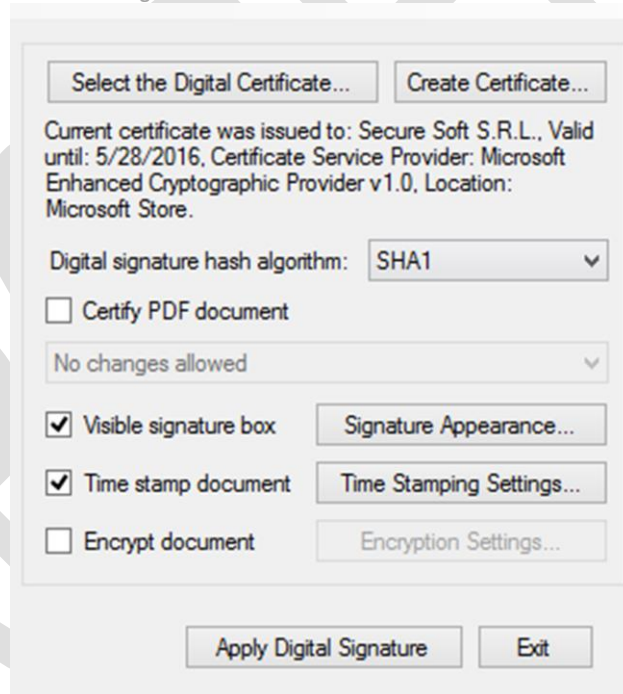


USING SHA256, SHA512 HASH ALGORITHMS

The default hash algorithm used by the library is SHA1 but in some cases, SHA256/384/512 must be used for the digital signature and the Time Stamp Request.

Attention: SHA-256 and SHA-512 hash algorithms are not supported by Windows XP. Note that some smart cards and USB tokens not support SHA-256 and SHA-512 hash algorithms.

Set the hash algorithm



BYPASSING THE SMART CARD PIN स्मार्ट कार्ड का पिन बाई पास करने की विधि आप । टोकन का पासवर्ड साफ़्ट्वर्ड में डाल देते हैं तो अबार बार आपको पासवर्ड नहीं डालना होता है

In case the digital signature must be made without user intervention and the certificate is stored on a smart card or USB token, the PIN dialog might be automatically bypassed for some models.

PIN dialog can be bypassed

Enter the Token Password.

Token Name:

Token Password:

Current Language: **EN**

In order to bypass the PIN dialog window, the Smart Card PIN checkbox must be checked and the right PIN to be entered. DigitalCertificate.SmartCardPin property must be set. This option bypass the PIN dialog and the file is automatically signed without any user intervention.

Bypassing the Smart Card PIN

Digital Certificates

Select the digital certificate used for digital signature

Windows Certificate Store

Certificates Available on Microsoft Store

Certificate Store: Show expired certificates


Smart Card PIN:

Attention: This feature will NOT work for all available smart card/USB tokens because of the drivers or other security measures. Use this property carefully.

6. ATTACHING DIGITAL SIGNATURE IN EMAIL BY USING OUTLOOK[™] USING OUTLOOK TO SEND DIGITALLY SIGNED EMAIL

Digitally sign a single message

In the message, on the Options tab, in the Permission group, click Sign Message.

- If you don't see the Sign Message button, do the following:
- In the message, click Options.
- In the More Options group, click the dialog box launcher  in the lower-right corner.
- Click Security Settings, and then select the Add digital signature to this message check box.
- Click OK, and then click Close.
- If you don't see the Sign Message button, you might not have a digital ID configured to digitally sign messages, and you need to do the following to install a digital signature.
- On the File menu, click Options > Trust Center.
- Under Microsoft Outlook Trust Center, click Trust Center Settings > Email Security
- Click Import/Export to import a digital ID from a file on your computer, or click Get digital IDs to find a list of services that issue digital IDs for your use.

Compose your message, and then send it.

DIGITALLY SIGN ALL MESSAGES

1. On the File tab, click Options > Trust Center.
2. Under Microsoft Outlook Trust Center, click Trust Center Settings.
3. On the Email Security tab, under Encrypted Mail, select the Add digital signature to outgoing messages check box.
4. If available, you can select one of the following options:
5. If you want recipients who don't have S/MIME security to be able to read the message, select the Send clear text signed message when sending signed messages check box. By default, this check box is selected.
6. To verify that your digitally signed message was received unaltered by the intended recipients, select the Request S/MIME receipt for all S/MIME signed messages check box. You can request notification telling you who opened the message and when it was opened, When you send a message that uses an S/MIME return receipt request, this verification information is returned as a message sent to your Inbox.
7. To change additional settings, such as choosing between multiple certificates to use, click Settings.
8. Click OK on each open dialog box.

-----नोट्स बनाने हेतु स्थान →

SOURCES AND REFERENCES

CCA website: <http://cca.gov.in>

NIC- CA website: <http://nicca.nic.in>

Interoperability Guidelines for Digital Signature Certificates:
<http://cca.gov.in/rw/pages/index.en.do>

IT ACT 2000 <http://www.mit.gov.in/content/information-technology-act>

Wikipedia <http://www.wikipedia.org>

Nemmadi <http://nemmadi.karnataka.gov.in/>

गूगल -GOOGLE

COMPILATIONS / टीम एवं सहयोग –

- **SUNIL SINGH VERMA (TECHNICAL INCHARGE BCSPL) BE.CS**
- **SUPPORTING STAFF – AMLESH SINGH (TECHNICAL ASSISTANT)BE.EC**
- **DEEPENDRA – BCOM KAJOL (BCOM PGDCA) बालाजी साल्युशंस / बालाजी कम्प्युसाफ्ट भोपाल**
- **GWALIOR - तोमर JABALPUR - हरिशी सिंह , इंदौर - प्रेम एरण**

TOLL FREE NUMBER FOR DIGITAL SIGNATURE HELP FOR FOREST DEPARTMENT

TOLL FREE 180030002448

LANDLINE 0755-4292405 | MOBILE - 9407532405 9407532411

EMAIL - dsc@digitalsignature.net.in | Website www.digitalsignature.net.in/forestit

**CORRESPONDENCE - BALAJI SOLUTIONS(BCSPL) 116 SUNNY PLACE MP NAGAR
ZONE 1 OPP DB MALL NEAR HOTEL SURENDRA VILAS BHOPAL MP PIN 462011**

-----*****Thank you Very Much *****-----

APPLICATION FORM - SIGNATURE / ENCRYPTION CERTIFICATE

FOR GOVERNMENT ORGANIZATION

 Application ID: (S) (E)

(For Office Use Only)

PLEASE FILL IN BLOCK LETTERS ONLY. ALL FIELDS ARE MANDATORYMore Instructions available at: <http://www.e-mudhra.com/instruction.html>**APPLICANT INFORMATION**

LASTNAME	FIRSTNAME	MIDDLE	NAME
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Date of Birth	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	Gender <input type="checkbox"/> Male <input type="checkbox"/> Female	Nationality <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Organisation Name	<input type="text"/>		
Department	<input type="text"/>		
Org Address	<input type="text"/>		
<input type="text"/>			
<input type="text"/>			
City	<input type="text"/>	Pin code	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
State	<input type="text"/>		
PAN of Applicant	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>	Mobile	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Email ID	<input type="text"/>		

Affix recent passport size photograph of the applicant **duly signed across**

CLASS:
 Class 1 Class 2 Class 3

TYPE:
 Signature Encryption Combo

VALIDITY:
 1 Year 2 Years

DOCUMENT PROOF (attested by Authorized Signatory of the Organization)

- Document required:**
- Copy of Applicant's Government ID Card / Letter from Organization / Pay Slip
 - Authorized Signatory Organisational ID Card / Self-Attested Letter of Organizational Identity
 - Copy of PAN Card of Applicant, if PAN provided

DECLARATION BY APPLICANT

I hereby agree that I have read and understood the provisions of e-Mudhra Certification Practice Statement (CPS) and the subscriber agreement and will abide by the same. The information provided in this form is true & correct to the best of my knowledge. I accept publishing my certificate information in e-Mudhra repository. I am aware of risks associated in case of Class 1 Certificate,when storing the private key on a device other than a FIPS 140-1/2 validated cryptographic module.

Date Place Signature of the applicant
(As in ID proof | Blue Ink Only)**AUTHORIZATION**

I hereby authorize this application on behalf of the organization. I hereby confirm the mobile number of Applicant given above. In case of class 3, I confirm the Physical Verification of Applicant.

Authorized Signatory (Sign and Seal)

TO BE FILLED BY RA OFFICE ONLY

I declare that the applicant has provided correct information in this application form. I have checked and verified the application form and supporting documents. **I hereby take full responsibility for any wrong verification made, or wrong documents submitted for the application.**

Date

RA Name, Code & Seal

Signature of RA

Digital Signature Certificate Subscription Form

Class of Certificate	Class 2	<input type="checkbox"/>	Individual	<input type="checkbox"/>	Signing	<input type="checkbox"/>	1 Year	<input type="checkbox"/>	Request Id:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
	Class 3	<input type="checkbox"/>	With Org Name	<input type="checkbox"/>	Encryption	<input type="checkbox"/>	2 Years	<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Section 1: Subscriber Details

Name*:

Designation :

Date of Birth*: Gender*: Male Female

Address (Residential address in case of Individual or Organization address in case of DSC with ORG)

Organisation Name * :

Door No/Building Name * :

Road/ Street/ Post Office * :

Town/ City/ District * :

State/ Union Territory * :

Country* : PIN Code*

Telephone Number* (with STD Code):

Mobile Number* :

Email id* :



* Self Attested Photo

- Use blue-ink only including signature.
- Ensure the Name, Designation, Address and Contact number of the attesting officer in at least one of the attestation document.

Section 2: Identity Proof Details

Photo Identity Proof *	Address Proof *
Identity Proof Name (Eg: Pan Card, DL, Passport, ...) <input type="text"/>	Address Proof Name (Eg: Passport, DL, Latest Telephone Bill, ...) <input type="text"/>
Identity Proof Number <input type="text"/>	

Note*: Subscriber's signature should appear on the Photo ID Proof.

Section 3: Declaration

I hereby declare that all the information provided in this Subscription form for the purpose of obtaining a digital certificate is true and correct to the best of my knowledge. I am aware, as a subscriber for the digital signature certificate, the duties and responsibilities which are applicable under the SafeScript CA CPS (<https://www.safescrypt.com/pdf/cps.pdf>) and also under the Section 71 of IT Act which stipulates that if anyone makes a misrepresentation or suppresses any material fact from the CCA or CA for obtaining any DSC such person shall be punishable with imprisonment up to 2 years or with fine up to one lakh rupees or with both.

Signature of the Subscriber*

Date*: Place*:

Note*: Subscriber has to sign before the Authorised LRA/Partner for Class3 DSC.

Section 4: Authorisation (only for ORG DSC)

I, _____ acknowledge by my signature, that the Subscriber information in this document is complete and accurate as per our office records. I fully understand that the Subscriber is responsible to transact on the Organisation's behalf and I will ensure timely revocation of Digital Signature Certificate in case the employee leaves the company in future.

Signature & Organisation seal*

For office use only

Attestation By Sify Authorised LRA/Partner* (For Class3DSC Only)

I hereby declare that the subscriber has personally appeared before me and submitted the original document copies.

Signature and Seal *

Date * Name *

Note*: Safescrypt at its discretion, will make a telephone call to verify the details of the Subscriber.

Partner Name:	<input type="text"/>
Sify RA:	<input type="text"/>
Date of Issuance:	<input type="text"/>

SafeScript CA Services brought to you by:

Sify Technologies Limited, 2nd Floor, Tidel Park, #4 Rajiv Gandhi Salai, Taramani, Chennai - 600 113. E-Mail: enquiries@safescrypt.com

