Digital Signature

ഡിജിറ്റൽ സിഗ്നേച്ചർ

എന്തിന്?, ഉപയോഗിക്കുന്നതിനുള്ള രീതി, ലഭ്യമാകുന്ന രീതി,
ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ, കമ്പ്യൂട്ടറിൽ വിന്യസിക്കുന്ന രീതി,
കമ്പ്യൂട്ടറിൽ നിന്നും നീക്കം ചെയ്യുന്നതിനുള്ള രീതി.....

വെർഷൻ 1.0

ഇൻഫർമേഷൻ കേരള മിഷൻ

www.infokerala.org

ഡിജിറ്റൽ സിഗ്നേച്ചർ എന്തിനു?

- ഡിജിറ്റൽ ടാറ്റയുടെ പ്രാമാണ്യം തെളിയിക്കാൻ
- ഉത്തരവാദിത്തം തള്ളിക്കളയാൻസാധിക്കില്ല
- ഡിജിറ്റൽ രേഖകൾക്ക് അംഗീകാരം നൽകുന്നതിന്
- സോഫ്റ്റ്വെയർ ഉപയോഗിക്കുന്നതിന് പ്രവേശനാനുമതി നല്കാൻ (ലോഗിൻ ചെയ്യുന്നതിന്)
- കമ്പ്യൂട്ടർ ഉപയോഗിച്ചുള്ള സാമ്പത്തിക ഇടപാടുകൾ, മറ്റു പ്രമുഖ നടപടികൾ നിർവഹിക്കുന്ന സ്ഥലങ്ങളിൽ കള്ളയാധാരമുണ്ടാക്കൽ, ടാറ്റ ഹാനീവരുത്തൽ തുടങ്ങിയവ തടയാൻ ഈ സഗേതിക വിദ്യ സഹായിക്കുന്നു.
- ഇന്ത്യ തുടങ്ങിയ നിരവധി രാജ്യങ്ങളിൽ നിയമാനുസൃതമായി പ്രാധാന്യം നൽകിയിട്ടുണ്ട്.

The Information Technology Act 2000

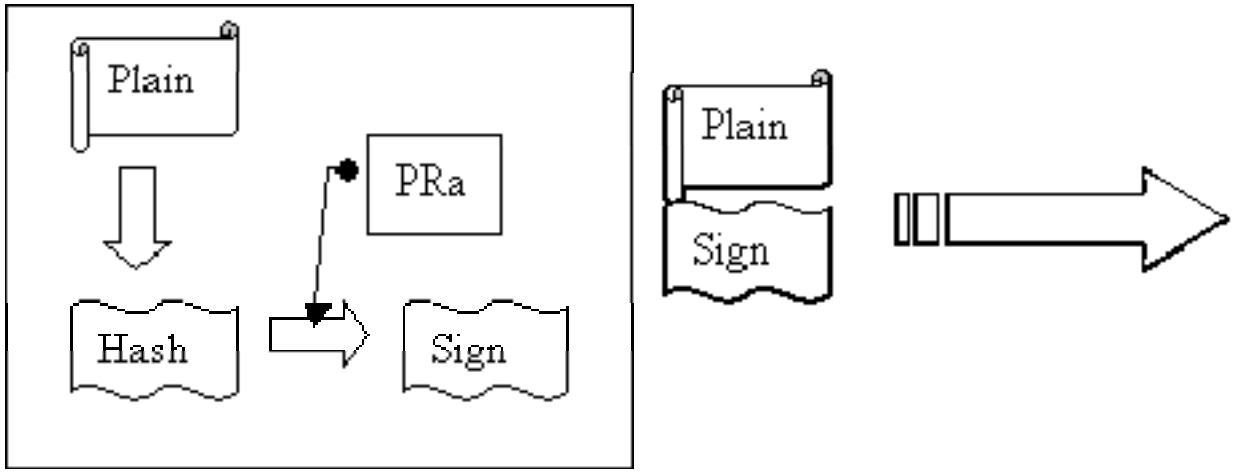
- Chapters II, VI, VII and VIII says about Digital Signature
- Chapters III and IV exclusively deal with electronic records.
- Chapter V introduces the concept of secure electronic records , secure digital signatures and its security procedure.
- Chapter IX and XI enumerates Offences and Penalties
- Chapter X – Cyber Regulations appellate Tribunal, its constitution, powers and functions.
- Chapter XIII – residuary matters like police powers, removal of difficulties, power to make rules and regulations, amendment to various enactments, etc.

ഡിജിറ്റൽ സിഗ്നേച്ചർ എന്നാൽ എന്ത്?

- ഗണിതശാസ്ത്രപരമായ ഒരു സമ്പ്രദായം ഉപയോഗിച്ചാണ് "ഡിജിറ്റൽ സിഗ്നേച്ചർ " പ്രാവർത്തിക മാക്കുന്നത്
- ഡിജിറ്റൽ രേഖകളുടെ ഗൂഢാക്ഷര ലേഖകൾ (Encrypted data) അസുരക്ഷിതമായ കമ്പ്യൂട്ടർ ശൃംഖലകളിലൂടെ അയച്ചാലും അവ ലഭിക്കുന്ന വ്യക്തിക്ക് അയച്ച വ്യക്തിയുടെ തിരിച്ചറിയൽ സാധ്യമാകുന്നതും പ്രാമാണ്യം ഉറപ്പിക്കുന്നതിനും സാധിക്കുന്നു.
- Asymmetric Cryptography എന്ന രീതിയിലാണ് പ്രധാനമായി "ഡിജിറ്റൽ സിഗ്നേച്ചർ " സമ്പ്രദായത്തിനായി ഉപയോഗിച്ച് പോരുന്നത്. അതായത് ഉടമസ്ഥന്റെ കൈവശം സുരക്ഷിതമായി സൂക്ഷിച്ചിട്ടുള്ള ഒരു "Private Key" യും മറ്റുള്ളവർക്ക് നൽകുന്ന ഒരു "Public Key" യും.
- ഉദാഹരണത്തിന് : സുരക്ഷിതമാക്കേണ്ട ടാറ്റ ഒരു "Private Key" ഉപയോഗിച്ച് മറ്റുള്ളവർക്ക് മനസ്സിലാകാത്ത വിധത്തിൽ രഹസ്യ കോഡിൽ എഴുതുന്നു. അവ ഉടമസ്ഥന്റെ തന്നെ "Public Key" ഉപയോഗിച്ച് തിരികെ പൂർവ സ്ഥിതിയിലേക്ക് കൊണ്ടുവരാൻ സാധിക്കുന്നു.

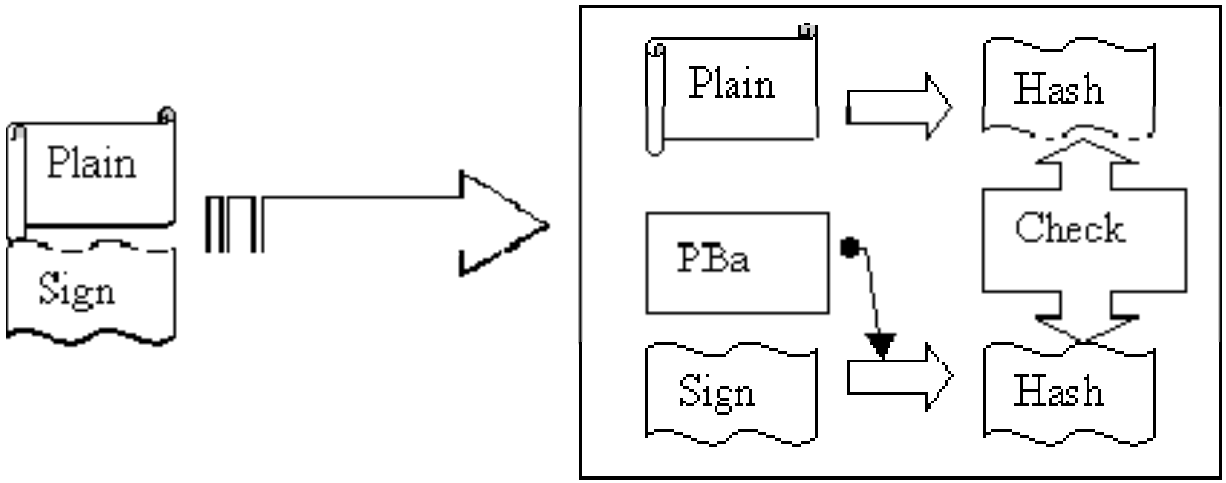
സാങ്കേതികമായി ഡിജിറ്റൽ സിഗ്നേച്ചർ ഉപയോഗിക്കുന്ന രീതി

- ഇതിനായി നാം ഇവിടെ ഉപയോഗിക്കുന്നത് RSA encryption algorithm (Rivest, Shamir, Adleman) മാണ്.
- സാങ്കേതികമായി സൈൻ ചെയ്യുന്ന പ്രക്രിയ:
  - സുരക്ഷിതമാക്കേണ്ട ഒരു ടാറ്റ യുടെ ഒരു "Hash" ഉണ്ടാക്കുന്നു.
  - *"ഹാഷ്" എന്നാൽ ഇതൊരു ടാറ്റ യുടെയും ഒരു സാരാംശം അഥവാ സത്ത്. പ്രസ്തുത സത്തിന്റെ വലിപ്പം ഇപ്പോഴും ഒന്നുതന്നെ ആയിരിക്കും. വ്യത്യസ്തമായ ടാറ്റ കൾക്ക് വ്യത്യസ്തമായ "ഹാഷ്" ആയിരിക്കും ലഭിക്കുക. അതുപോലെ തന്നെ, ഒരേ ടാറ്റ പലതവണയായി "ഹാഷ്" ചെയ്താലും ഒരേ "ഹാഷ്" തന്നെ ലഭിക്കുകയുള്ളൂ. എന്നാൽ ഒരു ഹാഷ് ഏതു രീതിയിൽ ശ്രമിച്ചാലും തിരികെ അതിന്റെ പൂർവ രൂപത്തിൽ എത്തിക്കുവാൻ സാധിക്കില്ല.*



- ശേഷം പ്രസ്തുത ഹാഷിനെ സൈൻ ചെയ്യുന്ന വ്യക്തിയുടെ "Private Key" ഉപയോഗിച്ച് ഋഡ്ഢാക്ഷരലേഖ ഉണ്ടാക്കുന്നു. ഇവയെയാണ് "Signature" എന്ന് പറയുക.
- ഇങ്ങനെ ലഭിക്കുന്ന "Signature" റും, യഥാർത്ഥ ടാറ്റയും സൈൻ ചെയ്ത വ്യക്തിയുടെ "Public Key" യും മറ്റുള്ളവർക്ക് കൈമാറാവുന്നതാണ്.

- സൈൻ ചെയ്ത വിവരം സാങ്കേതികമായി ശരിയാണോ എന്ന് പരിശോധിക്കുന്ന പ്രക്രിയ:
  - ആദ്യമായി, ലഭിക്കുന്ന ടാറ്റ യുടെ ഒരു ഹാഷ് തയ്യാറാക്കുക.
  - ശേഷം "Signature"-നെ സൈൻ ചെയ്ത വ്യതിയുടെ "Public Key" ഉപയോഗിച്ച് തിരികെ പൂർവ്വസ്ഥിതിയിൽ എത്തിക്കുക. ഇന്ങ്ങനെ ലഭിക്കുന്ന ഹാഷും യഥാർത്ഥ ടാറ്റയുടെ ഹഷും ഒന്നാണെങ്കിൽ അവ ഉപയോഗിക്കാവുന്നതാണ്. ഇല്ലെങ്ങിൽ പ്രസ്തുത ടാറ്റ ആരോ തിരുത്തി എന്ന് ബോത്യമാകും.

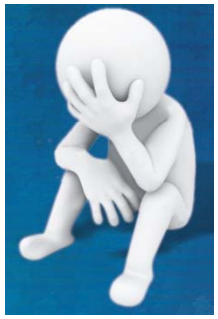


ഡിജിറ്റൽ സിഗ്നേച്ചർ ലഭിക്കാൻ

- പ്രധാനമായും ഇവയെ ക്ലാസ്സ് 2 എന്നും ക്ലാസ്സ് 3 എന്നും രണ്ടായി തരം തിരിക്കാം.
- സാധാരണ ആവശ്യങ്ങൾക്ക് ക്ലാസ്സ് 2 എന്ന തരവും, കൂടുതൽ സുരക്ഷിതമായ ആവശ്യങ്ങൾക്ക് ക്ലാസ്സ് 3 യും ഉപയോഗിക്കാം.
- ടാറ്റ സൈൻ ചെയ്യുന്നതിനായി ക്ലാസ്സ് 2 തരത്തിലുള്ള സിഗ്നേച്ചർ മതിയാകും
- ഡിജിറ്റൽ സിഗ്നേച്ചർ ലഭിക്കുന്നതിനുള്ള അപേക്ഷ പ്രസ്തുത ഫോർമാറ്റിൽ ഉയർന്ന ഉദ്യോഗസ്ഥൻറെ സാക്ഷ്യപെടുത്തലോടുകൂടി NIC യുടെ സംസ്ഥാന ഓഫീസിൽ നൽകുക. (ആവശ്യമായ തുകയുടെ DD യോടുകൂടി, നിലവിൽ Rs. 550/- ആണ്)
- അപേക്ഷയുടെ അവസ്ഥ ഇ-മെയിലിൽ യഥാസമയം അറിയിക്കും.
- അപേക്ഷ അന്ഗീകരിച്ചാൽ NIC യുടെ വെബ്സൈറ്റിലെ അപേക്ഷകന്റെ ഇ-മെയിലിൽ ലഭിച്ച ലോഗിൻ ഉപയോഗിച്ച് ഡിജിറ്റൽ സിഗ്നേച്ചർ ഡൌൺലോഡ് ചെയ്യാവുന്നതാണ്.
- പ്രസ്തുത ഡിജിറ്റൽ സിഗ്നേച്ചർ സൂക്ഷിക്കുന്നതിനായുള്ള പ്രത്യേക ടോക്കൻ ഇതോടൊപ്പം ലഭിക്കും
- (USB ഡ്രൈവിൽ ഉപയോഗിക്കാവുന്ന തരത്തിലുള്ള ഒരു സുരക്ഷിതമായ ഉപകരണമാണ് ഇവ)

ഡിജിറ്റൽ സിഗ്നേച്ചർ - ശ്രദ്ധിക്കേണ്ട കാര്യങ്ങൾ

- ലഭിക്കുന്ന "signature file" സ്വന്തം ആവശ്യത്തിനുള്ള കമ്പ്യൂട്ടറിൽ മാത്രം പരമാവധി ഇൻസ്റ്റോൾ ചെയ്യുക.
- ലഭിക്കുന്ന "signature file" പൊതുവായ കമ്പ്യൂട്ടറിൽ ഇൻസ്റ്റോൾ ചെയ്താൽ ഉപയോഗത്തിന് ശേഷം ഡിലീറ്റ് ചെയ്യാൻ മറക്കരുത്.
- പരമാവധി "signature token" ഉപയോഗിക്കാൻ ശ്രമിക്കുക. ഈരീതിയാണ് തികച്ചും സുരക്ഷിതമായിട്ടുള്ളത്.
- ലഭിക്കുന്ന "signature file" മറ്റുള്ളവർക്ക് അയച്ചു കൊടുക്കാൻ പാടില്ല. താങ്കളുടെ ATM Card ഉം, അവയുടെ രഹസ്യനാമവും പോലെതന്നെ ഇവയും സുരക്ഷിതമായി ഉപയോഗിക്കുക.
- Key ദുരുപയോഗപ്പെട്ടാൽ അതിന്റെ ഉടമസ്ഥനാണ് ബാധ്യത
- Key നഷ്ട്ടപ്പെട്ടുപോയാൽ ഉടൻ തന്നെ Certifying Authority (CA) യെ അറിയിക്കുക.



CONTROLLER OF CERTIFYING AUTHORITIES
CONTROLLER OF CERTIFYING AUTHORITIES
6, CGO Complex, Electronics Niketan
Lodhi Road, New Delhi - 110003
E-mail : info@cca.gov.in Website : http://cca.gov.in
Ministry of Communications & Information Technology
Government of India

ഡിജിറ്റൽ സിഗ്നേച്ചർ -
കമ്പ്യൂട്ടറിൽ വിന്യസിക്കുന്ന രീതി

- അപേക്ഷകന്റെ ഇ-മെയിലിൽ ലഭിച്ച ലോഗിൻ ഉപയോഗിച്ച് NIC യുടെ വെബ്സൈറ്റിലൂടെ ഡിജിറ്റൽ സിഗ്നേച്ചർ ഡൌൺലോഡ് ചെയ്യാവുന്നതാണ്.
- അതിനായി https://nicca.nic.in എന്നാ വെബ്സൈറ്റിൽ പ്രവേശിക്കുക (ചിത്രം കാണുക)
- *Token വിന്യസിക്കുന്നതിനുള്ള സെറ്റപ്പ് ഫയൽ, വിന്യസിക്കുന്നതിനുള്ള സഹായങ്ങൾ തുടങ്ങിയവയും ഈ വെബ്സൈറ്റിലൂടെ ലഭിക്കും*

NIC Certifying Authority

Home Resources Support Repository Contact Us

The maximum time limit for DC suspension/revocation re

Pls read carefully Encryption Key Backup Procedure

View DSC Fee Structure Download DSC Request Form Download Smart Card/USB eToken Driver

Download Certificate chain

NOTICE:Implementation of Interoperability Guidelines for Digital Signature Certificates (DSC) issued under Information Technology Act. 2000

It is to bring to the notice of all concerned that NICCA would start issuing DSC as per new certificate profile as laid down in the Interoperability Guidelines,upon communication from CCA. All application vendors are requested to test their application with new certficates(DSC) which can be downloaded from here: SHA256 with 2048 Trust Chain

***** NOTICE *****

All CA/RA Administrators/Officers are required to get issued fresh DSC with SHA256/2048 bits for their ROLE CARDS on immediate basis because existing DSC cards with SHA1 will not work for DSC issuance. Pls send your request immediately to NICCA Delhi. Those who have already issued SHA256 card NEED NOT to request fresh DSC for their Role cards. (Pls update your client to JRE 6) Download JRE 6 (32 bit)

FAQs for DLL to select RAA & CAO card/token

Prerequisites for Token Installation

As per CCA directives:

From 1st January 2012, NICCA shall issue DSC with Signature Algorithm SHA256 with 2048 bits key strength only.

Login

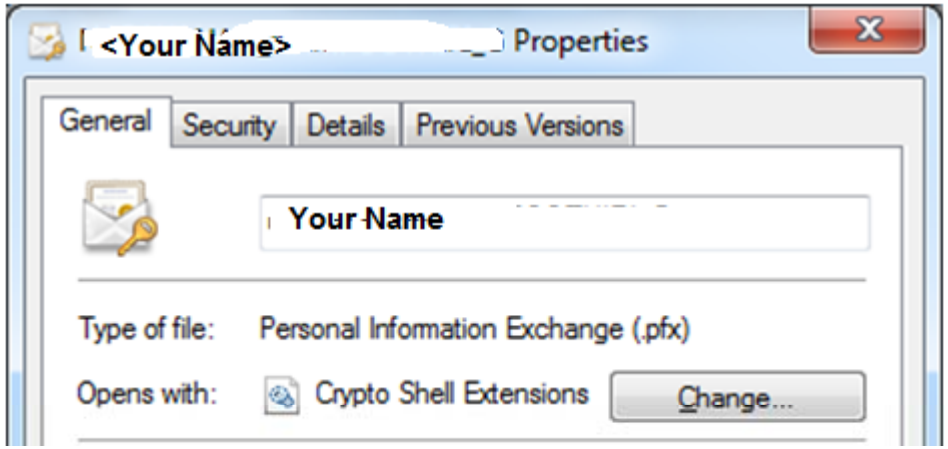
Member Login

Administrator Login

More

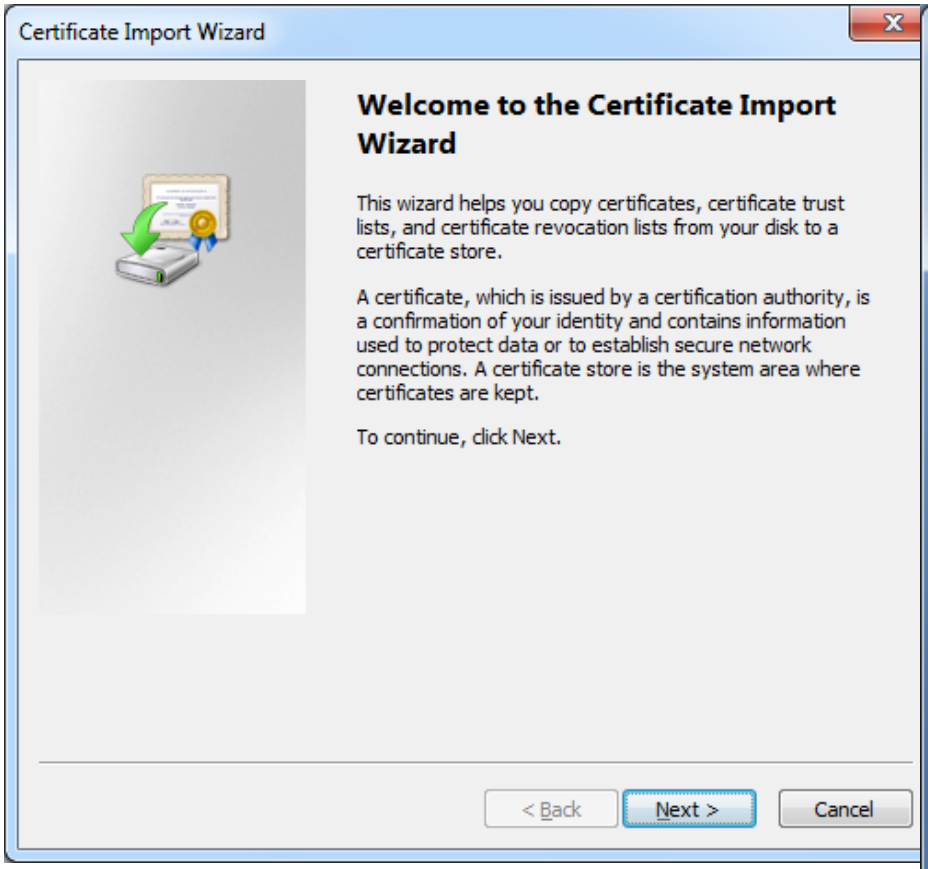
Instructions for Digital Certificate Enrolment:

- ശേഷം “Member login” എന്നാ ലിങ്ക് തെരഞ്ഞെടുത്ത ഈമെയിലിൽ ലഭിച്ച യുസർ നയിമും രഹസ്യകൊടും നൽകുക.
- ശേഷം “Download Certificate” എന്നാ ഭാഗത്തുനിന്നും താങ്കൾക്ക് അനുവദിച്ചിട്ടുള്ള “Digital Signature (DSC)” ഡൌൺലോഡ് ചെയ്യുക.
- ഇങ്ങനെ ഡൌൺലോഡ് ചെയ്ത ഫയലിന് (.pfx) എന്നായിരിക്കും എക്സ്റ്റൻഷൻ ഉണ്ടാവുക. (പ്രസ്തുത ഫയലിന്റെ Properties ശ്രദ്ധിക്കുക)

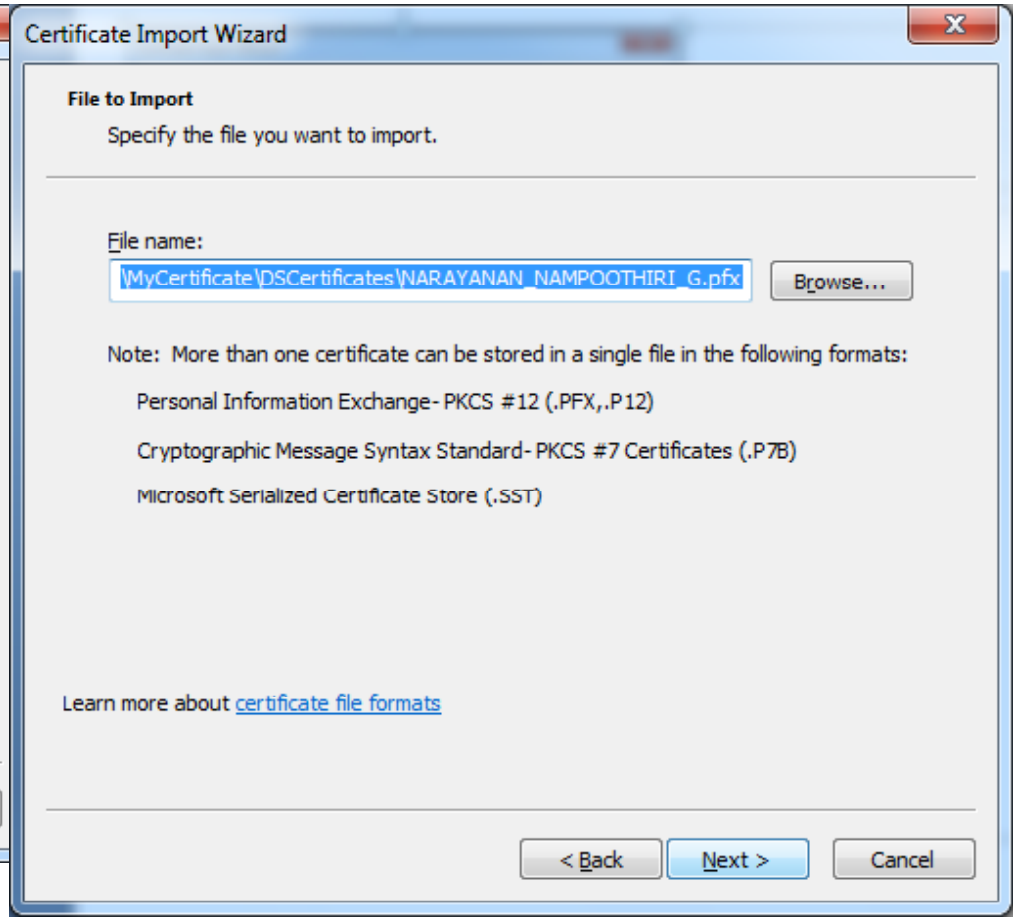


- അവ സുരക്ഷിതമായ ഒരു ഫോൾഡറിൽ സൂക്ഷിക്കുക

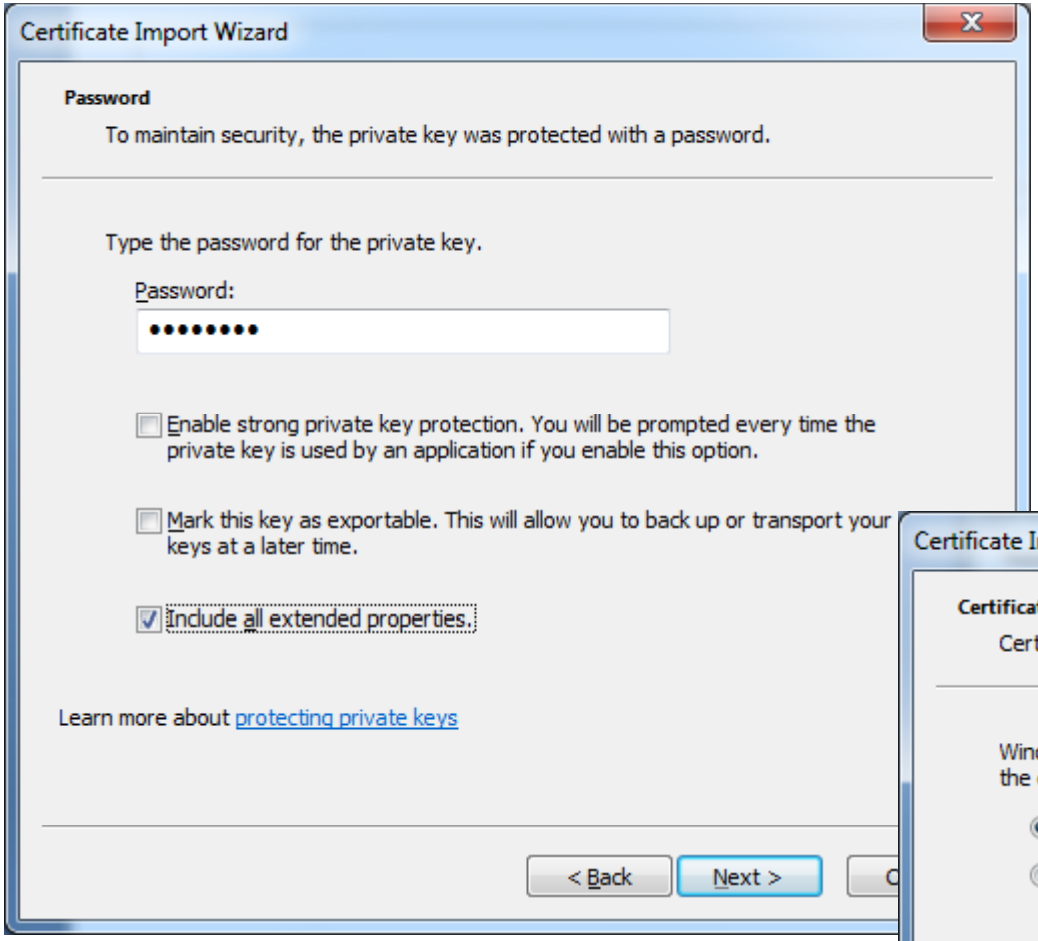
- അവ കമ്പ്യൂട്ടറിൽ വിന്യസിക്കുന്നതിനായി പ്രസ്തുത ഫയൽ ഡബിൾ ക്ലിക്ക് ചെയ്യുക.



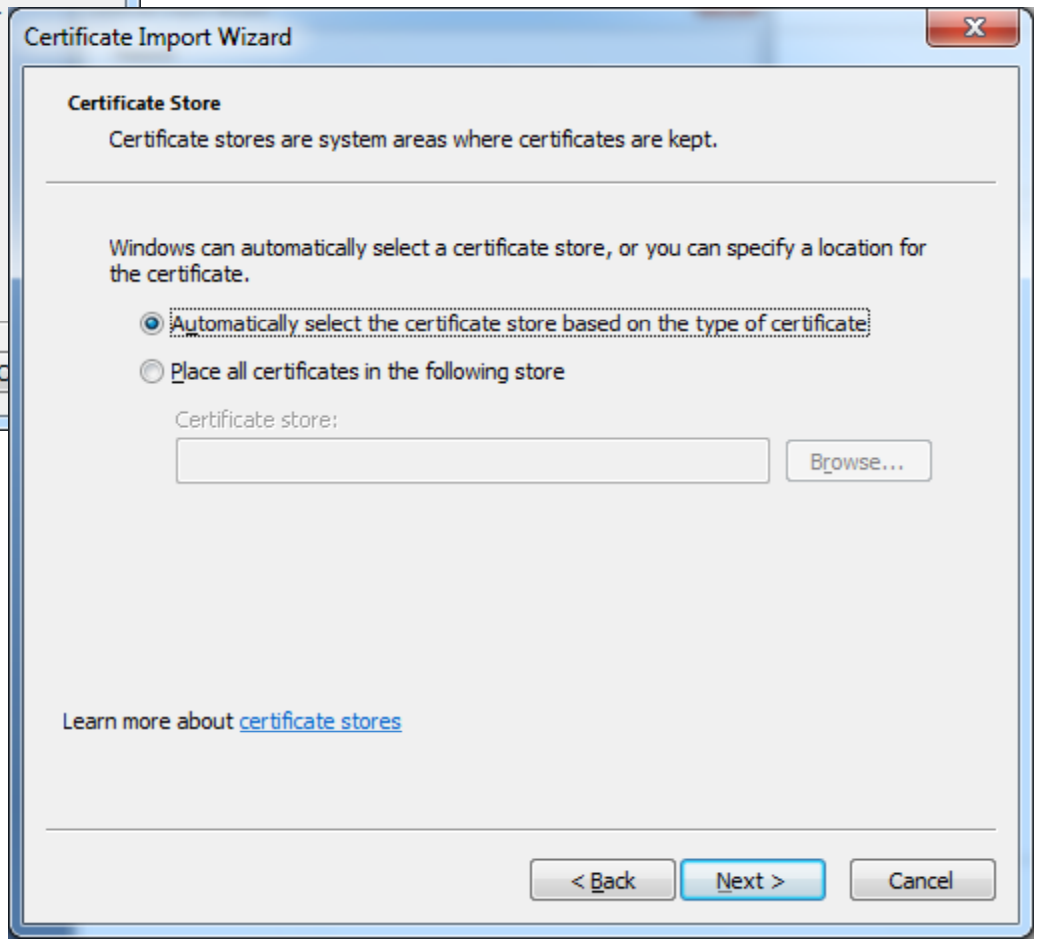
- ചിത്രം 1



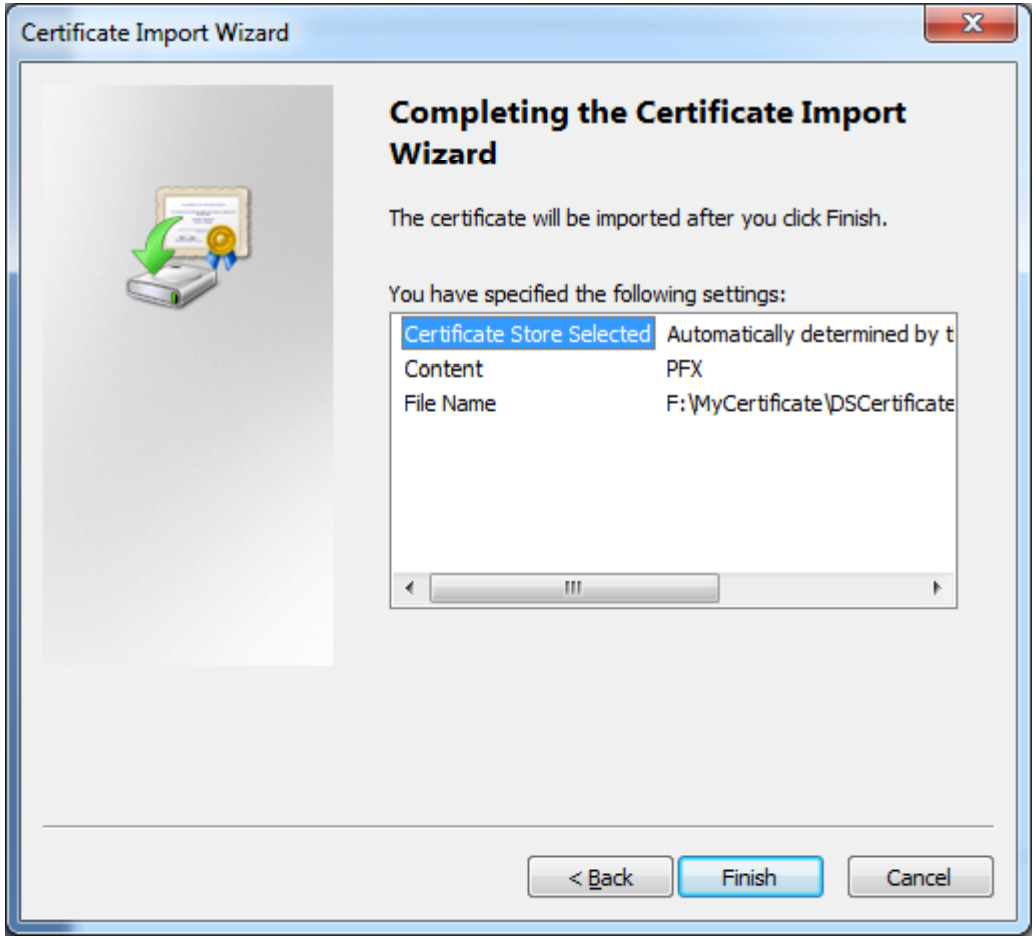
- ചിത്രം 2



• ചിത്രം 3 – സർട്ടിഫിക്കറ്റിന്റെ പാസ്സ്‌വേർഡ് നൽകുക

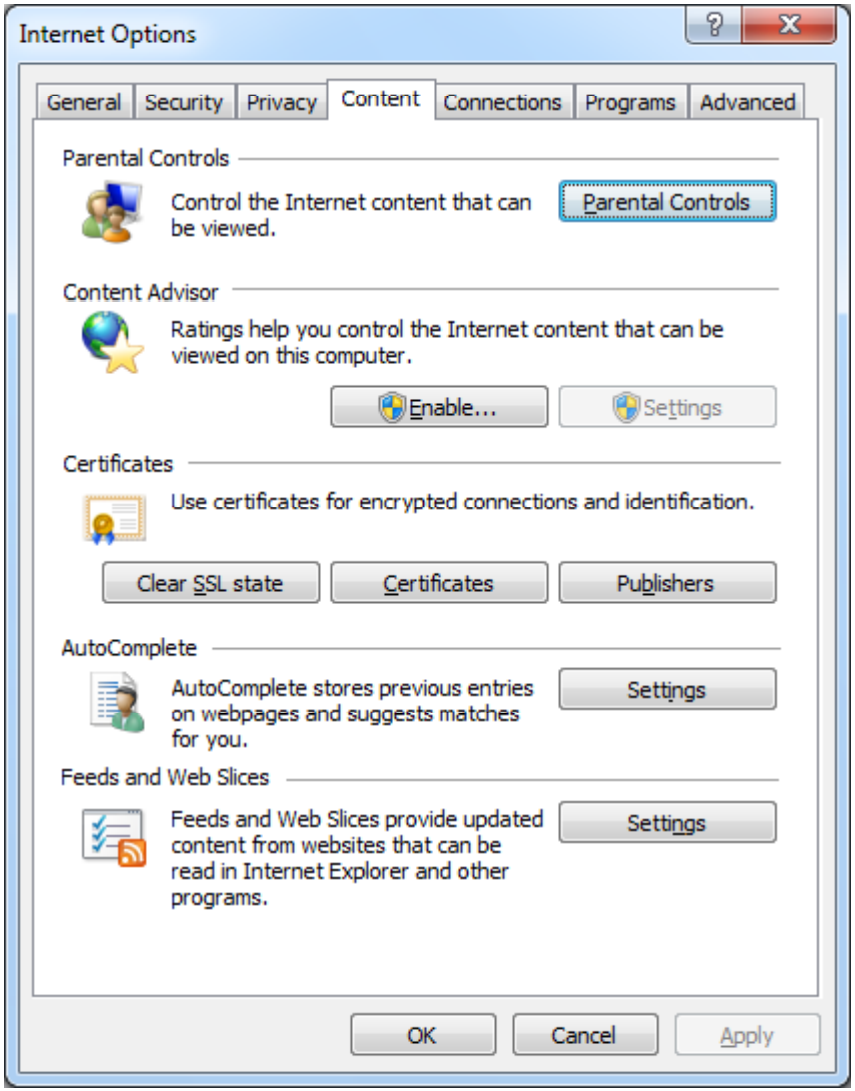


• ചിത്രം 4



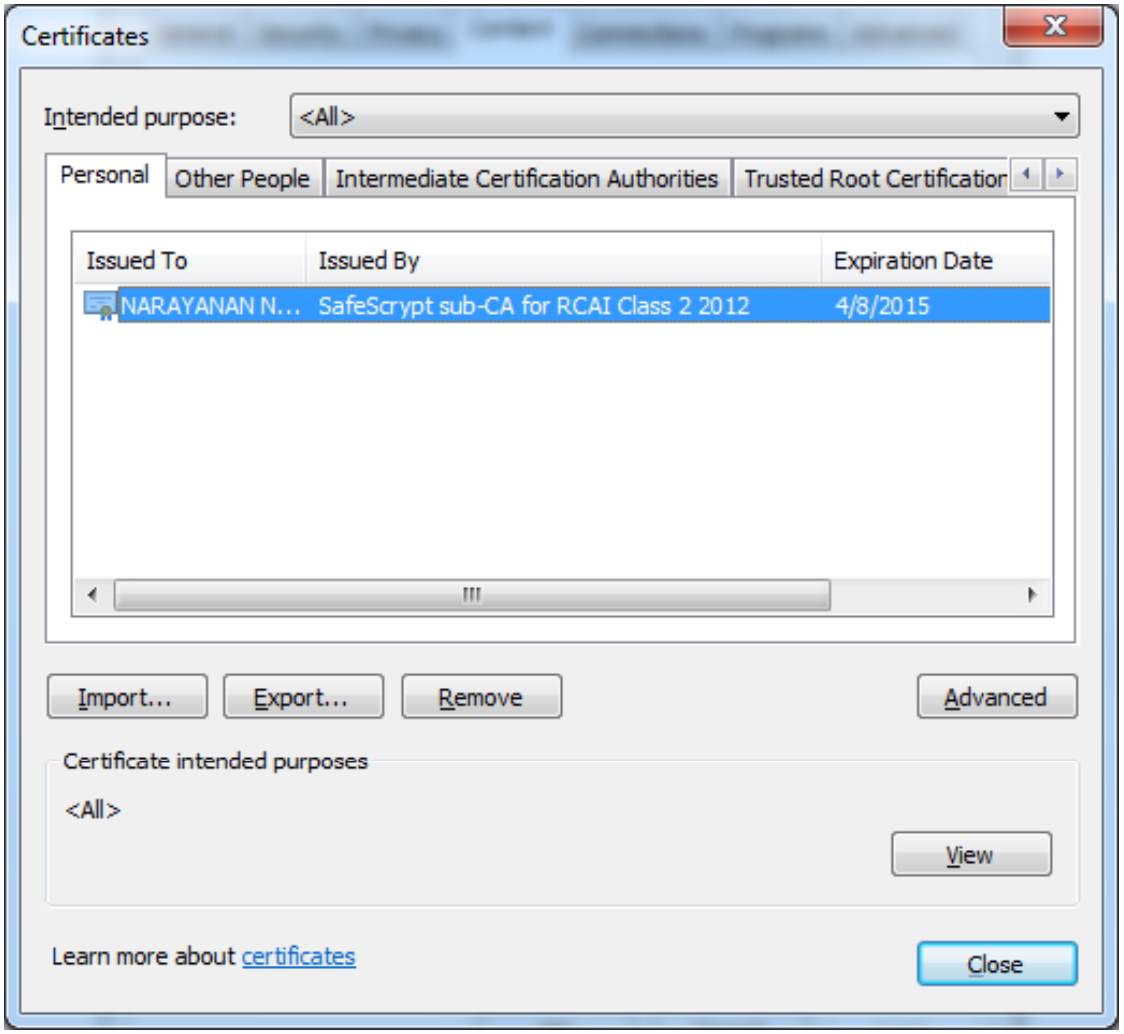
• ചിത്രം 5 – “Finish” ബട്ടൺ ചിക്ക് ചെയ്താൽ സർട്ടിഫിക്കറ്റ് കമ്പ്യൂട്ടറിൽ വിന്യസിക്കപ്പെടും

- സർട്ടിഫിക്കറ്റ് കമ്പ്യൂട്ടറിൽ വിന്യസിച്ചോ എന്നറിയാൻ.
- “Internet Explorer” എന്ന സോഫ്റ്റ്വെയർ തുറക്കുക
- ശേഷം “Tools” എന്ന മെനുവിൽ നിന്നും “Internet Option” എന്ന സബ് മെനു എടുക്കുക.



- അതിലെ “Content” എന്ന ടാബിലെ “Certificates” എന്ന ബട്ടൺ തെരഞ്ഞെടുക്കുക

- പ്രസ്തുത സ്ക്രീനിൽ സർട്ടിഫിക്കറ്റ് ലഭിച്ച വ്യക്തിയുടെ പേരും, സർട്ടിഫിക്കറ്റ് നൽകിയ സ്ഥാപനത്തിന്റെ വിവരങ്ങളും, സർട്ടിഫിക്കടിന്റെ കാലാവധി അവസാനിക്കുന്ന തീയതിയും കാണാം.



- *സർട്ടിഫിക്കറ്റിന്റെ ഉപയോഗം കഴിഞ്ഞാൽ "Remove" എന്നാ ബട്ടൺ തെരഞ്ഞെടുത്താൽ അവ കമ്പ്യൂട്ടറിൽ നിന്നും നീക്കം ചെയ്യാവുന്നതാണ്.*
- *വീണ്ടും ആവശ്യം വന്നാൽ, ആദ്യം ഡൌൺലോഡ് ചെയ്ത (.pfx) ഫയൽ വീണ്ടും വിന്യസിച്ചാൽ മതിയാകും.*

ഇൻഫർമേഷൻ കേരള മിഷൻ വികസിപ്പിച്ച അപ്ലികേഷൻ സോഫ്റ്റ്വെയറിൽ “Digital Signature” ഉപയോഗിക്കുന്നതിനായിട്ടുള്ള സഹായി പ്രസ്തുത സോഫ്റ്റ്വെയറിന്റെ കൂടെ ലഭിക്കുന്നതാണ്.

ഈ പ്രസന്റേഷനെ കുറിച്ചുള്ള അഭിപ്രായങ്ങളും നിർദേശങ്ങളും ദയവുചെയ്ത് narayanang@ikm.gov.in എന്ന ഇമെയിൽ വിലാസത്തിൽ അറിയിക്കുക. അല്ലെങ്കിൽ 0471-2595832 എന്ന ടെലെഫോൺ നമ്പറിലോ ബന്ധപ്പെടുക.